INDIA'S FRONTLINE IT MAGAZINE

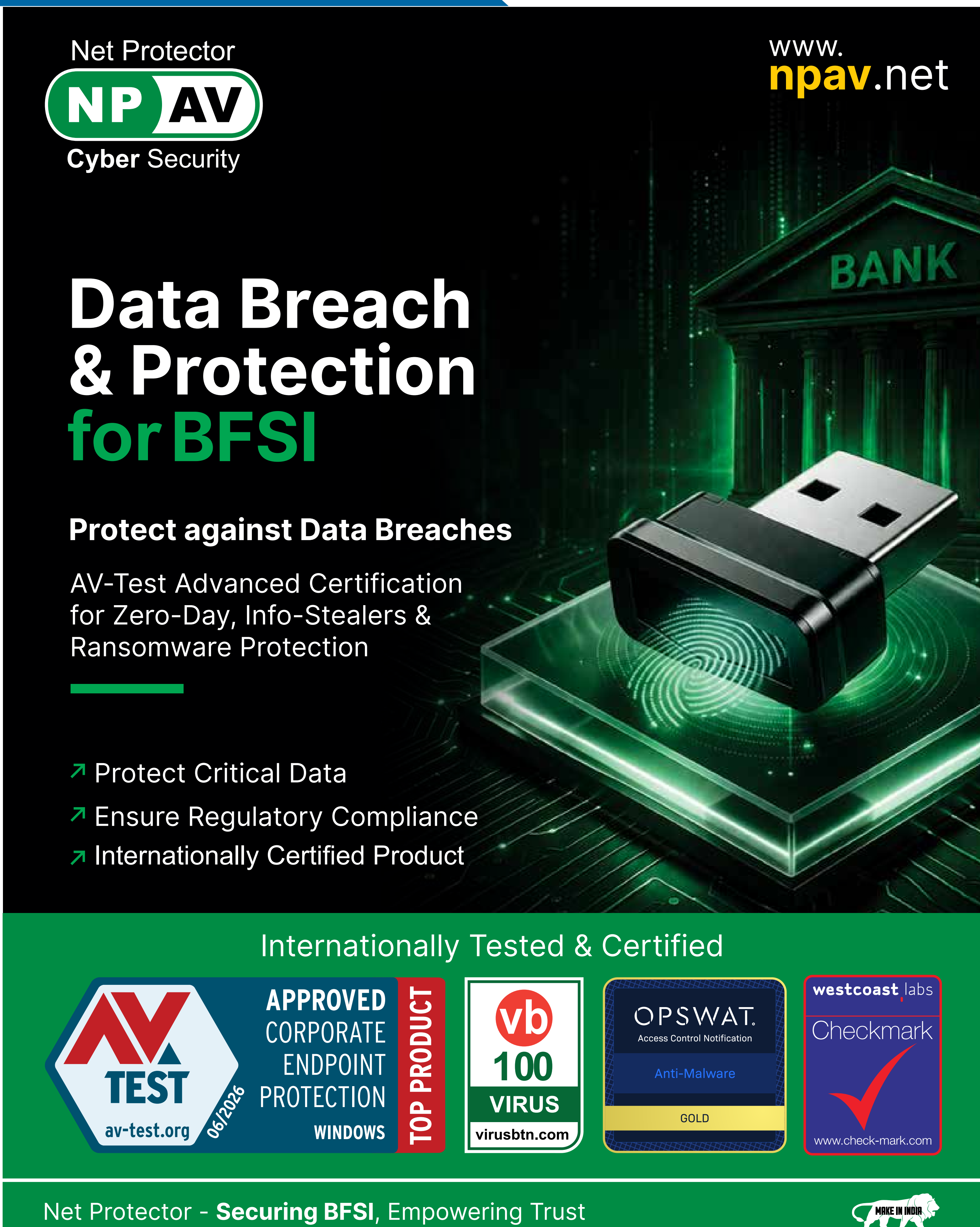
VARINDIA

THE ULTIMATE *Voice* OF INDIAN VALUE ADDED RESELLERS

VARINDIA 27 YEARS 1999-2026 ANNIVERSARY
COMING SOON SEPTEMBER 2026

SUBSCRIPTION COPY NOT FOR SALE

VOLUME XXVII | ISSUE 11 | JULY 2026 | PRICE RS. 50



INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

VOLUME XXVII ISSUE 11 JULY 2026 PRICE RS. 50 SUBSCRIPTION COPY NOT FOR SALE

AI, TRUST AND ALLIANCES: THE NEW ENTERPRISE IMPERATIVE

PAGE 46

India to set up first Telecom Manufacturing Zone in Gwalior

India will establish its first dedicated Telecom Manufacturing Zone in Gwalior to boost domestic telecom equipment manufacturing and attract semiconductor and data centre investments. Announcing the move ahead of the theme launch of the

10th edition of the India Mobile Congress (IMC), Communications Minister Jyotiraditya Scindia said the initiative aims to position India as a global telecom technology hub. He also highlighted the success of the telecom PLI scheme and reaffirmed the government's ambition to lead the world in 6G technology through innovation and manufacturing.

Microsoft expands MAI AI models across enterprise applications

Microsoft is expanding its in-house MAI artificial intelligence models across products such as GitHub Copilot, Excel, Outlook and other Microsoft 365 applications to improve enterprise performance while reducing AI operating costs. Microsoft CEO Satya Nadella said the company will use a combination of proprietary and partner AI models, selecting the best model for each task rather than relying on a single system. Microsoft said the approach has delivered encouraging results and will also power enterprise AI development through Microsoft Foundry.

THE AI INVESTMENT TEST: CAN BIG TECH TURN BILLIONS INTO PROFITS?

Artificial intelligence has entered a defining phase. The race has evolved beyond chatbots to autonomous AI agents capable of reasoning, planning, and executing complex tasks with minimal human intervention. Industry leaders such as OpenAI, Google DeepMind, Anthropic, Microsoft, NVIDIA, AWS, Meta, Salesforce, IBM, Oracle, SAP, ServiceNow, UiPath, Perplexity AI, xAI, and others are investing billions to lead this transformation. As innovation accelerates, concerns around AI safety, governance, transparency, cybersecurity, ethics, and regulatory compliance are becoming equally critical.

Following Google's earnings, investors are now turning their attention to Meta, Microsoft, Amazon, Apple, and PayPal. Their quarterly results will reveal whether unprecedented AI investments are translating into stronger revenue growth, cloud adoption, enterprise demand, and long-term profitability. Beyond financial performance, management commentary will provide important clues about the future direction of AI commercialization.

Meta faces perhaps the greatest pressure. CEO Mark Zuckerberg has committed enormous resources to AI infrastructure, foundation models, and data centres, yet investors continue to question the path to monetization. Analysts will look for updates on Meta's AI strategy, commercial opportunities, and whether the company plans to generate additional revenue by offering spare computing capacity to external customers.

Microsoft will be watched for proof that AI drives enterprise growth, with Azure's cloud growth and Microsoft 365 Copilot adoption as key metrics validating its OpenAI partnership. Amazon faces similar scrutiny, as investors seek evidence that its heavy AI infrastructure spending is accelerating AWS growth with sustainable returns. Apple, taking a more measured AI approach, is benefiting from renewed iPhone demand—though rising memory chip costs and expected hardware price hikes could pressure margins and consumer spending ahead.

Beyond earnings, this reporting season highlights a larger shift in the AI industry. Competition is increasingly centered on autonomous AI agents capable of transforming software development, customer service, cybersecurity, business operations, and scientific research. At the same time, responsible AI has become a strategic priority, with enterprises demanding explainable AI, stronger security, privacy protection, regulatory compliance, and trustworthy governance.

The companies that successfully balance innovation with responsible AI and strong commercial execution will shape the next era of digital transformation and define the future of the global AI economy.

AI's compute demands are the direct engine behind this data center boom. AI didn't just create demand for a new app category — it created demand for a fundamentally different, much more resource-intensive physical infrastructure layer, which is driving this segment's outsized growth. This is 1.7 trillion in Data Center IT spending needed by 2026 to build out AI infrastructure.

India's innovation ecosystem is entering a transformative phase, redefining its global technology leadership. From startup-led rocket launches and a 16-year-old capturing striking high-resolution Moon images that drew international attention, to quantum communication networks spanning over 1,000 kilometers with ambitions to reach 20,000, the country is rapidly pushing the frontiers of science and technology.

Other major innovations driving India's technology boom include:

- Indigenous semiconductor design under Semicon 2.0
- Sovereign AI and large language model (LLM) development
- Post-Quantum Cryptography (PQC) and quantum-safe cybersecurity
- AI-powered digital public infrastructure and governance
- Gaganyaan human spaceflight mission and reusable space technologies
- Green hydrogen, battery storage, and clean energy technologies
- Precision healthcare, genomics, and AI-driven drug discovery
- Advanced defense technologies, including hypersonic and directed-energy systems

Together, these innovations are positioning India not merely as a technology adopter, but as a global innovation powerhouse shaping the future of science, AI, quantum computing, space, cybersecurity, and deep-tech industries.

Security infrastructure has shifted from an IT necessity to a strategic business enabler as cyber threats grow more sophisticated. Modern enterprises need platforms that combine performance, intelligent automation, and real-time threat detection to protect their expanding digital ecosystems. AI-powered security, cloud-native architectures, zero-trust frameworks, and post-quantum readiness are now redefining how organizations defend critical assets.

The ability to detect, analyze, and respond to attacks at machine speed is now essential for maintaining operational resilience and business continuity. Enterprises that invest in scalable, innovative, and resilient security infrastructure will not only reduce cyber risk but also accelerate digital transformation, strengthen customer trust, ensure regulatory compliance, and gain a sustainable competitive advantage in an increasingly connected world.

Finally, the RBI's Draft Guidance on Data Governance requires Regulated Entities to treat data as a strategic asset by strengthening governance, lifecycle management, security, accountability, resilience, and third-party data oversight for better regulatory compliance.

Mohini

S. Mohini Ratna
Editor, VARINDIA
mohini@varindia.com

CADYCE

Life Aasaan Banaao
www.cadyce.com

USB HDMI KVM Switch

Multiple Systems. One Console.

Simplify operations and manage multiple systems through a single point of control.

4K	Quick	Multi-OS
4K Ultra HD @60Hz	Switching	Compatible

Available Models:

- CA-HDK200
- CA-UHDK220
- CA-UHDK440

Warranty : rma@cadyce.com | **Online Chat :** www.cadyce.com | **Email Support :** support@cadyce.com | **Sales :** sales@cadyce.com

Pune: +91 9226783571, 9322153959 | **Mumbai:** +91 9769726552, 9307742595 | **Maharashtra:** +91 9890227701 | **Gujarat:** +91 9974800847 | **Delhi:** +91 9999071626 | **Bangalore:** +91 9972534115, 9880660912 | **AP & TS:** +91 8882212998 | **Tamil Nadu:** +91 9840894013 | **Other Territories:** +91 9699375712.

Toll Free :
1800 266 9910
Tech Support :
+91 91722 12959

PICKUP · FREE · DELIVERY

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS
Website: www.varindia.com

Publisher: Dr. Deepak Kumar Sahu
Editor: S Mohini Ratna
Executive Editor: Dr. Vijay Anand
Consulting Editor: Gyana Swain
Associate Editor: Samrita Baruah
Assistant Editor: Ramesh Kumar Raja
Sub. Editor: Aparna Mullick
Art Director: Rakesh Kumar
Network Administrator: Ashok Kumar Singh
Visualizer: Ravinder Barthwal
Manager-IT: Subhash Mohanta
Manager-SEO: Santosh Kumar
Web Developer: Shivangi Mishra
SEO-Executive: Karan Arora

BUSINESS:
Commercial Manager: Amit Kumar Jha
Circulation Executive: Manish Kumar

CORPORATE OFFICE:
VAR House, A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030
Tel: 011-41656383, 43306464
Email: edit@varindia.com

Bangalore: Bureau office
Marketing Manager: S. Kamala kar
D-103 G.F., Ashish JK Apartments
Thubarahalli Extended Road
Bangaluru- 560066
Tel: 080-49530399 | Mobile:09886280836
E-mail: kamlakar@varindia.com

Mumbai: Bureau office
Regional Manager (West): Anil Kumar Sahu
Radha Krishna Complex, B/202, Plot no 24, Sector-25, Kamothe, Navi Mumbai - 410206, Maharashtra
Tel: 022-65561292, Mobile: 08108017479
E-mail: anil@varindia.com, mamta@varindia.com

Chennai: Bureau office
Branch Manager: K. Parthiban
F1, Meadows Green Apartments, 64, Chetty Street
1st Cross, Mel Ayanambakkam, Chennai - 600 095

Hyderabad: Bureau office
Branch Manager: Sunil Kumar Sahu
32-161/3, 202 Neha Paradise, Nr. Maissamma Temple, Venketeswara colony
Ramakrishna Puram, Hyderabad - 500056
Telangana, Tel: 040-32989844/ Cell No. 08100298033
E-mail: sunil@varindia.com

Kolkata: Bureau office
Marketing Officer: Sunil Kumar
Correspondent: B Kiran Dutta
Haritasa Electronics Solutions Pvt Ltd
204 Tower- 2, PS Srijan Corporate Park, Block EP-GP, Salt Lake, Sector - V, Kolkata - 700091
Mobile: 08100298033, E-mail: sunil@varindia.com
Mobile: 09903088480, E-mail: kiran@varindia.com

Bhubaneswar: Bureau office
Jagannath Warrior Residency, Suit No.A5/501, Kaimatia Bhubaneswar-752054 | Cell No. 8100298033

Printed and Published by **Deepak Kumar Sahu** on behalf of M/s. Kalinga Digital Media Pvt. Ltd. and Printed at Pushpak Press Pvt. Ltd. Shed No. 203 - 204, DSIDC Complex, Okhla Industrial Area, Phase-I, New Delhi-110020 and Published at A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030, Editor - S Mohini Ratna.

For Subscription queries contact: info@varindia.com
Subscription: Rs. 500(12 issues)Rs. 1000 (24 issues)

All payments favouring:
KALINGA DIGITAL MEDIA PVT LTD

CONTENTS

COVER STORY / 30pg

INFOTECH FORUM 2026
FORGING ALLIANCES, FUELING GROWTH

Cloud Migration in the AI Era:
Insights from Across the Industry

LEAD STORY
55pg

DELL Technologies

Stay Ahead with

Dell Pro Essential Micro

AMD

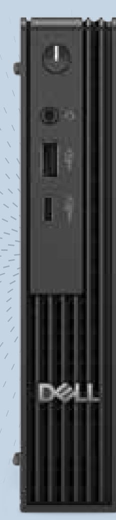
Dell Pro Essential Micro PVM1265: Big power. Ultracompact. Exception Security.

Performance for day-to-day demands

Boost productivity with AMD Ryzen™ processors performance and up to DDR5 memory[1] for seamless multitasking.

Easy to access

Tool-less entry and an easily removable panel allow for quick access to upgrade or service your desktop's internal components.



Hardware TPM

Protect your data with Trusted Platform Module (TPM), a security technology designed to secure hardware with integrated cryptographic keys.

Ultracompact

This ultra-compact desktop saves valuable space and is compatible with a wide range of mounts and stands, giving you flexible setup options to suit your business needs.

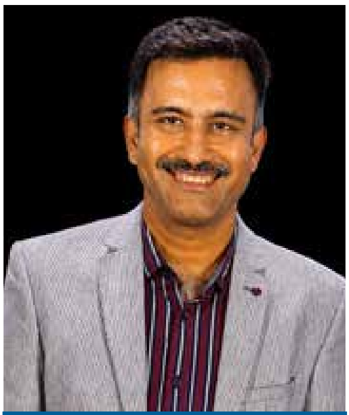
Meet the demands of your busy workdays with AMD Ryzen™ 5 150 processor, MS Windows Pro OS, 1X16GB DDR5, 512 GB SSD. Wired KB and Mouse, Internal Wifi, Bluetooth, and 3 Yrs Onsite Warranty.

Contact Us to Know More:

Name: Pooja Chavan | Email ID: dell.amd@rptechindia.com
Mobile Number: +91 86579 78028

[1]Up to 64GB, regional availability may vary.
[2]WiFi 6 module is optional.

Made in India, Powering India's cyber resilience



Sumeet Kela
Founder - Director
Net Protector cybersecurity

NPAV's cybersecurity philosophy is centered on developing indigenous security solutions tailored to India's unique digital ecosystem. Designed and developed entirely in India, its solutions are built to address the specific needs of Indian businesses—especially MSMEs—by delivering robust, lightweight, affordable, and easy-to-deploy protection without compromising performance.

Leveraging a deep understanding of the local market, Sanjiv Kela, Founder - MD & Sumeet Kela, Founder - Director – Net Protector Anti Virus (NPAV) tells VARINDIA of how the brand differentiates itself through solutions, backed by round-the-clock customer support and an extensive partner network.

Sanjiv Kela
Founder & MD
Net Protector cybersecurity

NPAV has emerged as a trusted "Made in India" cybersecurity brand. What has been the key philosophy behind building indigenous security solutions that address India's unique cyber challenges?

NPAV's philosophy has always been rooted in the belief that India's digital landscape requires cybersecurity solutions built specifically for its unique scale, diversity, and rapidly evolving digital ecosystem. India's IT environment differs significantly from global markets, and so do its cybersecurity challenges. From the beginning, we recognized that Indian businesses—particularly MSMEs—as well as individual users need security solutions that are powerful, lightweight, affordable, and easy to deploy. At NPAV, our guiding principle has always been to deliver maximum protection without compromising system performance. By designing and developing our core technologies entirely in Pune, India, we maintain complete control over innovation and can respond quickly to emerging threats. This enables us to build security solutions that effectively counter localized cyber threats while meeting global cybersecurity standards.

How does NPAV differentiate itself from global cybersecurity vendors while strengthening customer trust and contributing to India's vision of digital sovereignty?

What differentiates NPAV from global cybersecurity vendors is our deep understanding of the Indian market and our close proximity to our customers. While many international solutions are designed primarily for Western markets, our products are engineered specifically to perform efficiently across India's diverse infrastructure, internet conditions, and hardware environments. Customer trust is built on reliability, transparency, and accessibility. We provide dedicated 24×7 technical and commercial support through our extensive partner network across India, ensuring customers receive prompt assistance whenever they need it. As an indigenous cybersecurity company, we strongly support India's vision of digital sovereignty. By developing cybersecurity solutions within India, we help ensure that sensitive data, threat intelligence, and security telemetry remain under Indian control, which is increasingly important for national security and strategic digital independence.

How is NPAV innovating its products to safeguard Indian enterprises, government organizations, and critical infrastructure?

The cyber threat landscape has evolved dramatically, with attackers increasingly leveraging artificial intelligence to launch sophisticated ransomware, zero-day exploits, and advanced persistent threats.

To stay ahead, NPAV has integrated advanced Artificial Intelligence and Machine Learning into its security architecture through our proprietary ZeroV DeepLearn AI technology. Rather than relying solely on traditional signature-based detection, our solutions use real-time behavioral analysis, heuristic detection, and AI-driven threat intelligence to proactively identify and block previously unknown threats before they can execute.

Our enterprise solutions—including Endpoint Security and Z Security—provide multi-layered protection with capabilities such as ransomware defense, data loss prevention, secure cloud backup, device control, vulnerability management, and centralized security management.

How does NPAV's "Made in India" approach support national cybersecurity, data sovereignty, and the vision of Atmanirbhar Bharat?

Cybersecurity has become an essential pillar of national security. Dependence on foreign technologies to protect critical digital infrastructure can introduce strategic risks. NPAV embodies the vision of Atmanirbhar Bharat by demonstrating that world-class cybersecurity solutions can be researched, developed, and continuously enhanced entirely in India. By building our own proprietary security technologies, threat intelligence, and detection algorithms, we reduce dependence on external platforms while ensuring greater control over cybersecurity operations. This approach strengthens data sovereignty, supports the growth of India's cybersecurity ecosystem, creates high-value technology jobs, and contributes to building a resilient digital future for the nation.

As the CEO of NPAV, what is your vision for the company's next phase of growth, and how do you see NPAV shaping the future of cybersecurity in India while expanding its global footprint?

Our long-term vision, inspired by our Founder and Managing Director, Mr. Sanjiv Kela, is to transform NPAV from a leading endpoint security provider into a globally recognized cybersecurity and digital trust company. In India, we are making significant investments in next-generation technologies, including Zero Trust Security, AI-powered threat detection, cloud security, Extended Detection and Response (XDR), and advanced endpoint protection to support the country's rapidly growing digital economy.

Internationally, we see tremendous opportunities across emerging markets in Asia, the Middle East, Africa, Australia, and New Zealand. Our goal is to deliver scalable, affordable, and enterprise-grade "Made in India" cybersecurity solutions worldwide while demonstrating that Indian cybersecurity innovation can compete with the world's best.

Cybersecurity Suite for BFSI

Net Protector (NPAV) offers an integrated cybersecurity suite to help BFSI organizations strengthen cyber resilience, protect critical data, ensure regulatory compliance, and maintain business continuity.

The portfolio includes Krypton Enterprise Backup, Krypton Firewall Log & Access BFSI Audit, Krypton Enterprise AI Insight, and Krypton Encryption Manager, delivering backup, audit, AI-driven security insights, and encryption.

Together, these solutions provide a strong foundation for data protection, compliance, and operational resilience, while organizations should complement them with capabilities for AI-driven identity fraud, deepfake detection, and privacy governance to address emerging cyber threats.

COMPROMISED CREDENTIALS:

Net Protector (NPAV) addresses identity-based threats through a layered approach combining Krypton Enterprise AI Insight (KEAI)and Krypton Firewall Log & Access BFSI Audit (KFLA). KEAI uses AI-driven behavioral analytics to establish normal user activity and detect anomalies such as unusual login times, devices, locations, or access patterns. KFLA centralizes and monitors firewall and access logs for real-time visibility across the enterprise. Additionally, NPAV's AV-Test Advanced Certified endpoint protection helps prevent credential theft by blocking keyloggers and infostealer malware before credentials can be compromised.

ON DATA EXFILTRATION DETECTION

Krypton Firewall Log & Access (KFLA) and Krypton Enterprise AI Insight (KEAI) work together to detect abnormal data access and movement in real time. KFLA provides continuous monitoring and audit-ready logging, while KEAI applies behavioral analytics and predictive intelligence to identify unusual activities—such as large data transfers—and trigger automated responses like alerts or session isolation. Together, they enhance threat detection, incident response, and forensic readiness for BFSI organizations.

ON AI-DRIVEN / AUTONOMOUS ATTACKS

NPAV's Krypton Enterprise AI Insight (KEAI) combines AI-driven threat detection, behavioral analytics, predictive intelligence, and automated response to identify adaptive cyber threats beyond traditional signature-based methods. Complementing this, Krypton Encryption Manager (KEM) enforces policy-based encryption across endpoints, servers, and removable devices, ensuring data remains protected even if attackers bypass initial defenses. Together, they provide a layered security approach against evolving AI-driven attacks, although the underlying machine learning techniques are not detailed in the presentation.

ON DETECTION SPEED AND RESPONSE

This is the one area the presentation materials don't quantify. The deck references "real-time monitoring" and "automated response" as design goals across KFLA and KEAI, but it doesn't publish specific MTTD (mean-time-to-detect) or MTTR (mean-time-to-respond) benchmarks for an account-takeover scenario. Given the earlier questions we discussed around the Bank of Baroda breach, this is actually the most important number to press NPAV on directly — ideally with reference to independent testing (similar to how their endpoint protection carries AV-Test, VB100, OPSWAT, and West Coast Labs certifications) rather than vendor-stated figures alone.

ON REGULATORY AND SECTOR-SPECIFIC FIT

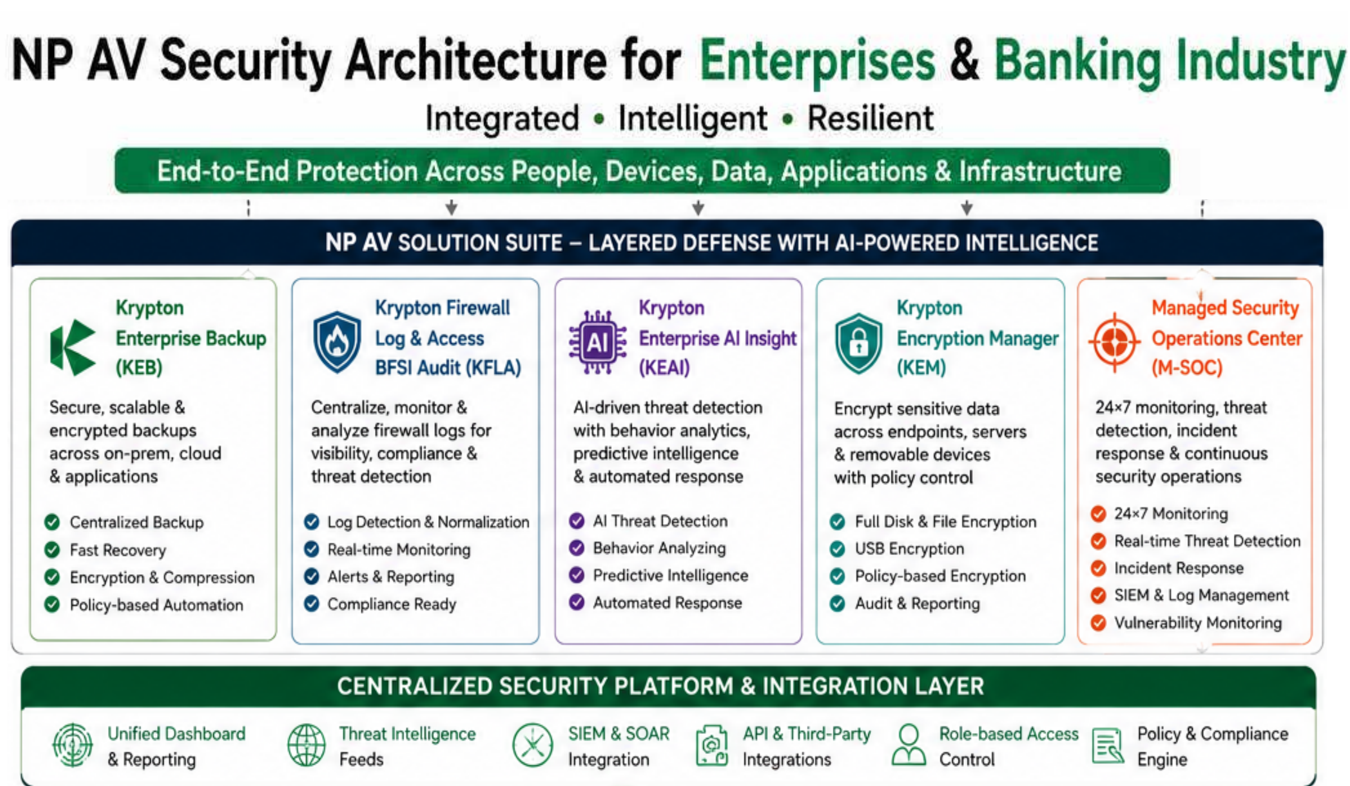
Net Protector (NPAV)'s Krypton Firewall Log & Access (KFLA) is purpose-built for the BFSI sector, offering compliance-ready log management, monitoring, and audit reporting aligned with RBI cybersecurity expectations. Krypton Encryption Manager (KEM) strengthens data protection through encryption and audit capabilities. Supported by certifications such as AV-

Our long-term strategy centers heavily on the BFSI market. To support this vision, we are increasing our investment in enterprise offerings tailored to financial institutions, ensuring we remain a trusted partner in their digital transformation journey over the coming years.

Ms. Shaila Kela
Director & CFO

To stay ahead in the current AI landscape, we are constantly upgrading our capabilities to address the stringent security needs of the financial sector. We are committed to achieving zero-day trust and providing next-generation cyber defense for our clients."

Ms. Preeti Kela
Director & Head Of Ai / Cybersecurity Lab



Football, Technology, and the Changing World: More Than Just a Game

DR. ASOKE K. LAHA
Chairman-Emeritus and Founder, InterraIT

The FIFA Worls Cup had gripped the imagination of billions across the globe. In India too, millions sacrificed sleep to cheer their favourite teams and players. For several weeks, normal routines were disrupted as football fever spread across homes, workplaces, and social media. I could not resist making football the central theme of this month's column.

At first glance, readers may wonder what football has to do with a column that usually focuses on information technology and the digital economy. Surprisingly, the connection is deeper than it appears.

As I watched match after match—both live broadcasts and highlights—I was struck by how remarkably unchanged the essence of football has remained over the decades. Ever since I began watching and playing the game in my childhood, its fundamental character has stayed intact. Whether played in a grand stadium before eighty thousand spectators or in a small backyard with makeshift goalposts, football remains the same beautiful game.

Although the game's essence has remained unchanged, it has evolved in important ways. New rules have been introduced to improve fairness, reduce dangerous play, and protect players from serious injuries. The use of yellow and red cards has significantly discouraged reckless tackles and deliberate fouls. Interpretations of offside, handball, and more recently, technological interventions such as the Video Assistant Referee (VAR), have enhanced the accuracy of officiating. Modern tournaments also provide world-class medical facilities and emergency response systems, ensuring injured players receive immediate treatment—something unimaginable in earlier decades.

Yet the fundamentals remain constant. A football team still fields eleven players. Victory continues to depend on discipline, teamwork, strategy, stamina, agility, dribbling skills, and finishing ability. Individual brilliance may win admiration, but championships are won by cohesive teams. One weak link in the chain can undermine the collective effort, much like a fragile component disrupting an otherwise efficient business supply chain.

History has celebrated extraordinary footballers whose individual genius inspired generations. Pelé transformed football into a global spectacle. Later came Diego Maradona, Cristiano Ronaldo, Lionel Messi, and many others whose names became synonymous with excellence. However, even these icons depended on teammates. Football remains the ultimate team sport, where collaboration outweighs individual talent.

While the game itself has changed little, everything surrounding it has undergone a remarkable transformation. Football today is no longer merely a sport; it is one of the world's largest entertainment industries. Technology has revolutionised how football is produced, consumed, and commercialised.

I vividly remember waiting eagerly for the morning newspaper to read match reports or tuning in to All India Radio for live commentary. Those experiences carried their own excitement. Today, the situation is dramatically different. High-definition television, satellite broadcasting, smartphones, streaming platforms, and social media allow fans to watch every match live from virtually anywhere in the world. Instant replays, real-time statistics, multilingual commentary, and interactive fan engagement have transformed viewing into a highly immersive digital experience.

This technological revolution has reshaped football's economics. Broadcasting rights, sponsorships, merchandising, advertising, digital subscriptions, and global branding now generate enormous revenues. According to Deloitte's Football Money League reports, Europe's leading clubs earn billions of dollars annually through commercial activities, media rights, and matchday revenues. When one includes clubs across continents, the global football economy comfortably exceeds tens of billions of dollars every year and continues to expand rapidly.

Players have benefited enormously from this commercial boom. The world's elite footballers are no longer merely athletes; they are global brands. Endorsement contracts, image rights, business ventures, and investments have created extraordinary wealth. Cristiano Ronaldo, for instance, has built a business empire extending well beyond football through sponsorships, hospitality, fashion, and media ventures.

The contrast with earlier generations, particularly in India, is striking. Many talented footballers who represented the country with distinction struggled financially after retirement. One poignant example is Olympian Antony, who reportedly spent his later years doing modest jobs to support himself before dying in relative obscurity. Such stories reflect the limited recognition and financial security historically available to Indian footballers, despite their contributions to the sport.

Football enjoys passionate support in several parts of India. States such as Kerala and West Bengal have long nurtured vibrant football cultures where the sport rivals, and sometimes surpasses, cricket in popularity. Tamil Nadu, Karnataka, Goa, and parts of the Northeast also possess strong football traditions. Nevertheless, despite widespread enthusiasm, India has not translated this passion into sustained international success.

India's football history contains moments of genuine achievement. The national team participated in the Olympic Games beginning in 1948, famously playing barefoot in some matches. Under the legendary coach Syed Abdul Rahim, India reached the semi-finals of the 1956 Melbourne Olympics—still regarded as one of the country's finest football achievements. However, after the 1960s, Indian football gradually lost its competitive edge and failed to qualify consistently for major international tournaments.

This decline invites serious reflection. Why has India excelled in sports such as cricket and made notable recoveries in hockey while football has remained on the margins? Infrastructure, grassroots development, coaching standards, sports administration, and long-term investment all deserve closer examination. The popularity of football among fans has never been in doubt; what remains uncertain is whether institutional commitment has matched public enthusiasm.

Football also reveals broader social and political contradictions. Many European nations and the United States, despite celebrating football's diversity, continue to adopt increasingly restrictive immigration policies, particularly towards migrants from poorer African countries. Yet some of their strongest football teams rely heavily on players of African origin or heritage. Their sporting success often reflects the contributions of immigrant communities they otherwise seek to restrict.

Football, however, offers a powerful counter-narrative. On the field, talent transcends race, nationality, religion, and economic status. Success is determined by skill, discipline, teamwork, and determination rather than birthplace or social background. In many ways, football represents one of humanity's greatest levellers.

The digital revolution has transformed how football is watched, marketed, and monetised, but it has not changed the spirit of the game itself. Teamwork, perseverance, discipline, and collective effort remain as relevant today as they were generations ago.

Apple briefly tops $5 trillion market value milestone

Apple briefly became only the second publicly listed company to surpass a $5 trillion market capitalisation after its shares climbed to an intraday high of $342.89. The rally lifted the company's valuation to about $5.036 trillion, although the stock later closed at $340.08, leaving its market value at approximately $4.99 trillion, just below the historic milestone.

The achievement followed Apple's return as the world's most valuable listed company, overtaking Nvidia. Investor optimism surrounding Apple's expanding services business, integrated hardware ecosystem and artificial intelligence strategy has driven its shares nearly 25% higher this year.

Attention is now focused on Apple's upcoming quarterly earnings, with investors seeking updates on revenue growth, AI initiatives and future product strategy. Nvidia, the first company to cross the $5 trillion valuation mark, has a market capitalisation of about $4.77 trillion, keeping the race for global technology market leadership closely contested.

NVIDIA, Microsoft, IBM join Open Secure AI Alliance to strengthen AI security

A coalition of more than 60 technology companies, cybersecurity vendors and open-source organisations has launched the Open Secure AI Alliance (OSAA) to develop open technologies, tools and frameworks for securing AI systems. Founding members include NVIDIA, Microsoft, IBM, Cisco, CrowdStrike, Palo Alto Networks, Fortinet, Red Hat, Hugging Face, Salesforce, SAP, Dell Technologies, HPE, GitHub, Nokia, ServiceNow and the Linux Foundation.

Building on the Linux Foundation's Akrites initiative and the Open Source Security Foundation, the alliance aims to accelerate development of open AI models, security tools, agent frameworks and vulnerability remediation technologies. Members will collaborate on AI agent identity, model isolation, secure coding, vulnerability scanning and evaluation frameworks.

The alliance also urged governments to recognise open AI models as defensive cybersecurity assets. Among the first contributions, NVIDIA released its NOOA research framework on GitHub, while Microsoft, IBM, Red Hat, HPE and Hugging Face contributed technologies to strengthen AI security, software supply chains and enterprise cyber resilience.

HCLTech, Sarvam partner to build sovereign AI data centre in Odisha

HCLTech will invest Rs. 14,257 crore to establish its first AI data centre in Odisha in partnership with Sarvam AI and the state government. The facility, to be located at the upcoming Odisha Sovereign AI Park in Bhubaneswar, will leverage HCLTech's full-stack AI capabilities and Sarvam's foundation models to deliver sector-specific AI applications for public and private enterprises.

The project aims to strengthen India's sovereign AI ecosystem by supporting multilingual AI services, local developer innovation and enterprise adoption. It is also expected to enhance the country's AI infrastructure while addressing data sovereignty requirements and accelerating AI-led digital transformation.

Roshni Nadar Malhotra, Chairperson, HCLTech, said the initiative aligns with the Digital India and Atmanirbhar Bharat vision by advancing India's sovereign AI ecosystem. C. Vijayakumar, CEO & Managing Director, HCLTech, said the investment will help meet growing demand for sovereign AI solutions while expanding the company's strategic partnership with Sarvam AI.

Redington posts record quarterly revenue as cloud, AI drive 34% growth

Technology solutions provider Redington reported its highest-ever quarterly revenue and profit for the first quarter of FY27, driven by strong demand for cloud, cybersecurity, AI infrastructure and enterprise technology solutions. Consolidated revenue rose 34% year-on-year to Rs. 34,966 crore, while profit after tax (excluding exceptional items) increased 77% to Rs. 486 crore, with the PAT margin improving to 1.4%.

India emerged as the company's fastest-growing market, with revenue rising 63% and profit after tax increasing 60%. Growth was supported by enterprise technology projects, higher PC realisations, premium smartphone demand and continued adoption of cloud and cybersecurity solutions. The Software Solutions Group recorded the strongest growth, followed by the Technology Solutions and Endpoint Solutions businesses.

V. S. Hariharan, Managing Director and Group CEO, Redington, said the company delivered its strongest quarterly performance and expects sustained growth opportunities as enterprises continue investing in cloud computing, AI, cybersecurity and digital transformation initiatives.

Uttar Pradesh cements position as India's largest electronics manufacturing hub

Uttar Pradesh has reinforced its position as India's leading electronics and mobile manufacturing hub, accounting for nearly 65% of the country's mobile phone production and about 55% of electronics component manufacturing. The Noida-Greater Noida industrial belt has attracted global brands such as Samsung, Oppo, Vivo and LG, alongside leading manufacturers including Dixon Technologies, Optiemus and Padget Electronics.

The state's electronics ecosystem has expanded beyond smartphone assembly to include printed circuit boards, display modules and other key components. According to the state government, industry-focused policies have attracted investments exceeding ₹28,000 crore from more than 75 companies, while approved semiconductor projects worth ₹32,146 crore are expected to strengthen domestic chip manufacturing.

Uttar Pradesh has also recorded strong export growth, with smartphone exports reaching $17.5 billion in 2024-25. The state is now promoting investments in artificial intelligence, robotics, automation and Industry 4.0 technologies to further strengthen its role in India's global electronics manufacturing ambitions.

Anthropic expands India enterprise AI ecosystem with LTTS, LTM partnerships

Anthropic has expanded its enterprise services ecosystem in India through strategic partnerships with L&T Technology Services (LTTS) and LTM to accelerate adoption of its Claude AI models. The collaborations aim to help enterprises move generative AI initiatives from pilot projects to large-scale deployments across engineering, software development and application modernisation.

LTTS will integrate Claude models into its AI-powered engineering platforms to support product engineering, software development, testing and lifecycle management. Meanwhile, LTM will embed Claude, Claude Code and Claude Cowork into its BlueVerse AI Delivery Fabric while establishing a Claude Center of Excellence and expanding its AI1000 talent initiative to train Claude-certified professionals.

Amit Chadha, CEO and Managing Director, LTTS, said the partnership will embed AI across engineering workflows to accelerate innovation. Venu Lambu, CEO and Managing Director, LTM, said combining Claude with BlueVerse and skilled talent will help enterprises modernise applications and achieve measurable business outcomes through AI-led transformation.

DELL Technologies

Windows 11

Transform Your Productivity

Work smarter with Dell Pro Essential

Streamline IT and simplify your business

Security
Encrypt credentials with **TPM 2.0,** enable quick sign-in with an optional **fingerprint reader**, and secure devices with a lock slot.

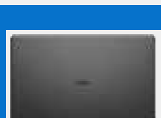
Manageability
Autopilot and Intune streamline setup and configuration, while **Dell Management Portal** simplifies cloud-based PC management. Support

Support
Support Assist resolves issues proactively, and **ProSupport** offers 24/7 expert assistance with extended warranty options.

Built for Business
Enterprise-grade productivity unlocked with optimized thermals, enhanced display, and extended battery life.

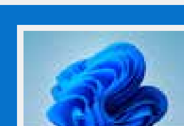
Intelligent Software
Dell BIOS, Dell Optimizer's AI, and **Excalibur OS** improve performance, security, and system recovery.

Recycled Materials
Dell Pro Essential devices are built with durability and use responsibly sourced, **recycled materials** to reduce environmental impact.



Always choose Genuine pre-installed Windows 11 Pro devices
Ensure a secure, trusted foundation from day one.

Secure and reliable
Built to withstand everyday business use with features like FHD IR camera, fingerprint reader, and AI-powered noise reduction.



Gain more than just a secure OS
Genuine Windows 11 Pro reduces overall cyber-risk and helps lower security costs.

Seamless views for smarter work
Enjoy crisp visuals on a 14-inch screen with a 16:10 aspect ratio and 300 nits brightness.

92% of successful ransomware attacks originated from unmanaged devices, underscoring the need for built-in OS-level security and device control.

Professional Designs in Various Shades

Dell Pro Essential laptops are available with optional chassis materials and colors; crafted to meet military-grade standards (MIL-STD) for proven reliability.

Carbon Black

Platinum Silver

Midnight Blue (Aluminum)

Contact Us to Know More
Email ID: EnquiryDell@kestoneglobal.biz

Satcom Infotech partners with halofort to expand endpoint management in India

Satcom Infotech has announced a strategic distribution partnership with halofort to expand the reach of the halofort.uemx platform across India. The collaboration aims to help enterprises simplify endpoint management while strengthening identity governance, compliance and Zero Trust security. The platform integrates Unified Endpoint Management (UEM), Identity and Access Management (IAM), Mobile Device Management (MDM) and security capabilities within a single architecture. The partnership combines Satcom Infotech's cybersecurity distribution network with halofort's endpoint management platform, enabling channel partners and system integrators to address rising demand for secure, cloud-ready and identity-centric IT environments.

Pratap Mondal, Chief Growth Officer, Satcom Infotech, said the partnership expands the company's cybersecurity portfolio while enabling partners to deliver integrated endpoint management and security solutions. As part of the alliance, Satcom Infotech will drive halofort's market expansion through partner recruitment, technical enablement, certification programmes, solution demonstrations and joint marketing initiatives across India, targeting key enterprise sectors.

Sectigo, eCAPS partner to automate certificate lifecycle management

Sectigo has entered into a strategic partnership with eCAPS Computers India to expand automated Certificate Lifecycle Management (CLM) solutions across India. The collaboration aims to help enterprises and managed security service providers address the industry's transition to 47-day digital certificate lifecycles through automation, ensuring continuous uptime, stronger cryptographic security and improved operational efficiency.

The partnership combines Sectigo's CLM platform with eCAPS' value-added distribution network to provide end-to-end certificate visibility, deployment and automated renewal. According to the companies, the solution will help organisations manage digital certificates efficiently while adapting to evolving industry standards.

Sarabjeet Khurana, Country Manager for India & ASEAN, Sectigo, said automation is essential as certificate validity periods continue to shrink. Gunasegharan K, Director, eCAPS Computers India, said the partnership strengthens the company's cybersecurity portfolio by delivering scalable certificate lifecycle management capabilities to customers and channel partners across India.

ESDS unveils sovereign cybersecurity platforms to strengthen digital resilience

ESDS Software Solution Limited has launched Swaraj Nandi and Swaraj Hansa, two indigenous enterprise security platforms developed in India to strengthen cyber resilience and support digital sovereignty. The platforms expand the company's portfolio of homegrown cybersecurity solutions and are designed to help organisations secure critical infrastructure while meeting evolving regulatory and compliance requirements.

Swaraj Nandi is a Privileged Access Management (PAM) platform built on Zero Trust principles, while Swaraj Hansa is an AI-powered Security Information and Event Management (SIEM) platform that automates threat detection, investigation and response. Both solutions address growing enterprise security challenges, including privileged access risks, alert fatigue and compliance monitoring.

Piyush Somani, Promoter, Managing Director and Chairman, ESDS, said the platforms combine Zero Trust security with AI-driven operations to protect critical infrastructure. The solutions are available through on-premises, private cloud and as-a-service deployment models for enterprises across banking, government, healthcare and other regulated sectors.

Tata Communications, TTBS partner to accelerate AI adoption among SMBs

Tata Communications and Tata Tele Business Services (TTBS) have announced a strategic collaboration to accelerate AI adoption among India's small and medium businesses through a unified AI platform stack. The partnership combines Tata Communications' AI and communications capabilities with TTBS' extensive SMB reach to deliver enterprise-grade AI solutions that are easier to deploy and manage.

The companies showcased an AI-powered Voice Agent capable of handling customer enquiries, scheduling appointments, processing orders and delivering multilingual support. Powered by Tata Communications' Commotion conversational AI platform and Vayu AI Cloud, the solution is supported by TTBS' voice infrastructure for secure and scalable deployment.

Ganesh Lakshminarayanan, MD & CEO, Tata Communications, said the collaboration will help SMBs adopt AI with confidence. Harjit Singh, MD, Tata Teleservices, said the partnership builds on TTBS' digital capabilities to create a comprehensive AI ecosystem that enhances productivity, improves customer experiences and supports business growth across India's SMB sector.

ManageEngine launches marketplace to expand enterprise IT ecosystem

ManageEngine has launched the ManageEngine Marketplace, introducing a partner-developer ecosystem that enables enterprises to discover and deploy extensions, integrations, plugins and AI agents across its platforms. The marketplace is designed to expand the capabilities of ManageEngine solutions by allowing customers to access specialised tools developed by partners and independent developers.

The platform also serves as a gateway for Zia Agents, ManageEngine's AI-powered autonomous agents for enterprise IT environments. According to the company, the marketplace combines its core platform capabilities with ecosystem-driven innovation, helping organisations customise deployments and address specific business requirements.

Rajesh Ganesan, CEO, ManageEngine, said the marketplace enables developers to extend platform capabilities while maintaining the security, governance and quality standards expected by enterprise customers. Every submission will undergo validation for functionality, security and compliance before publication, ensuring organisations can adopt partner-built solutions with confidence while accelerating enterprise innovation.

HPE expands supercomputing portfolio for AI and HPC workloads

HPE has introduced new supercomputing software and infrastructure enhancements to simplify high-performance computing (HPC) and AI deployments. The company has extended its Supercomputing Programming Software to HPE ProLiant Compute servers, enabling a consistent programming experience across platforms while reducing deployment complexity for AI and HPC workloads.

HPE has also added multi-tenant networking and storage capabilities to support sovereign AI research. The enhancements strengthen data isolation and security across HPE Slingshot 400 software and HPE Cray Supercomputing Storage Systems E2000, helping research institutions manage multiple users and workloads more efficiently.

Fumiki Negishi, VP and GM, HPC & AI APJ GTM Division, HPE, said the innovations simplify AI ecosystems while providing secure, sovereign infrastructure. HPE Financial Services has also introduced new end-of-life services to help organisations securely retire HPC and AI systems while ensuring data protection and regulatory compliance.

Acer, Intel and Infinity Learn launch India's first NEET-ready laptop for CBT transition

As the National Eligibility cum Entrance Test (NEET) prepares to transition to a Computer-Based Test (CBT) format from 2027, Acer, Intel and Infinity Learn have partnered to launch what they describe as India's first integrated NEET Ready Ecosystem. As part of the collaboration, the companies have unveiled the country's first NEET Ready Laptop, designed to equip medical aspirants with both digital skills and academic resources required for the new examination format. The initiative combines Acer's Aspire series laptops, Intel's computing technologies and Infinity Learn's AI-powered NEET preparation platform to help students adapt to the evolving digital examination landscape.

Every year, more than 22 lakh students appear for NEET, making it India's largest undergraduate medical entrance examination. The partnership aims to bridge this gap, particularly for students from Tier II, Tier III and rural regions, where access to personal computing devices remains limited. Nearly 70% of NEET aspirants come from these regions, making digital preparedness an important aspect of exam readiness.

F5 advances frontier AI cyber resilience with new fleet management capabilities

F5 has announced new fleet management capabilities for F5 Insight for ADSP that help enterprises reduce risk exposure across F5 BIG-IP environments as frontier AI compresses vulnerability response timelines. The new F5 Insight workflows give security and operations teams fleet-wide visibility, guided update management, enterprise authentication, role-based access controls, and a tamper-evident AI audit trail. This enables customers to move from identifying risk to taking accountable action across large, distributed application delivery and security fleets.

The new capabilities build on F5's move to monthly hardened software releases and reflect a broader shift in how F5 helps customers respond to AI-accelerated threats. As vulnerability response timelines shrink, enterprises need more than faster fixes. They need the operational control to understand what is exposed, prioritize updates, execute changes safely, and maintain a clear record of action across complex environments.

Fortinet expands FortiEndpoint with new capabilities for the AI era

Fortinet has announced new capabilities for its unified endpoint platform, FortiEndpoint, designed to help organizations securely adopt AI, protect sensitive data, and reduce risk. By bringing AI visibility and control, native data security, endpoint risk scoring, and FortiAI-assisted operations into FortiEndpoint, Fortinet enables security teams to better govern AI usage, reduce sensitive data

FORTINET®

exposure, enforce risk-aware access, and simplify security operations across distributed environments.

"Organizations need a simpler and more effective way to manage security as their environments become more complex and AI-enabled. The Fortinet Security Fabric is designed to converge critical security and networking functions across the enterprise, helping customers reduce complexity, improve visibility, and strengthen protection. With FortiEndpoint, we are extending that strategy by consolidating security, secure access, data security, AI visibility, and assisted operations in a unified endpoint platform, delivered through one agent, one console, and one license," said Michael Xie, Founder, President, and Chief Technology Officer, Fortinet.

Acrobat rolls out PDF workflows to WhatsApp

Adobe and WhatsApp are bringing Acrobat-powered PDF experiences directly into WhatsApp Web and Windows, so that users can open, review and act on documents right in the chat without needing to download files or switch tools. Many of WhatsApp's three billion users already use the platform to share files and move work forward. Adobe Acrobat has long delivered trusted PDF viewing, collaboration and AI-powered productivity in the places where people work with documents. Integrating Acrobat into WhatsApp extends that value, so you can stay in the flow whether you're reviewing an invoice, checking a contract, looking over a design or confirming details.

"Acrobat is built to power document workflows wherever they happen," said Abhigyan Modi, senior vice president, Creativity & Productivity Business. "Bringing PDF capabilities into WhatsApp Web and Windows extends that vision into one of the world's most important communication platforms."

Dell launches AI-ready Pro Precision workstations, introduces Deskside Agentic AI in India

Dell Technologies has expanded its workstation portfolio in India with the launch of the new Dell Pro Precision lineup, introducing a range of AI-ready mobile and tower workstations designed for professionals handling compute-intensive workloads. Alongside the hardware launch, the company unveiled Dell Deskside Agentic AI, a solution that enables organizations to deploy, manage and scale agentic AI workloads locally rather than relying solely on cloud infrastructure.

The new portfolio comprises the Dell Pro Precision 5 Series (14S, 16S), Dell Pro Precision 5 Series (14, 16), Dell Pro Precision 7 Series (14, 16) and the Dell Pro Precision 7 T1. The systems target engineers, architects, designers, creators and other professional users requiring high-performance computing for AI applications, simulations, visualization and rendering. According to Dell, increasing investments in AI applications, engineering software and data-intensive workflows are driving demand for dedicated workstation platforms.

Lenovo expands gaming and entertainment portfolio in India

Lenovo has expanded its consumer device portfolio in India with the launch of the Lenovo LOQ monitor series and the Lenovo Tab Plus Gen 2, strengthening its presence in the gaming and entertainment segments. The new products are designed for users who switch between gaming, streaming, content consumption and multitasking, while offering high-performance features across different usage scenarios. The launch includes the Lenovo LOQ gaming monitor lineup, built for fast-paced gaming, alongside the Tab Plus Gen 2, a tablet that combines premium audio, AI-powered features and portability for entertainment and productivity on the go.

Speaking on the launch, Kaman Chawla, Director, Consumer Business, Lenovo India, said, "Consumers today expect seamless experiences across devices, whether they are gaming at their desks or consuming content on the move. With the Lenovo LOQ monitor series, we are delivering high-performance displays engineered for speed, precision, and immersive gameplay."

Tenable expands Exposure Management Platform to contextualize and prioritize application security risk

Tenable Holdings has announced the expansion of the Tenable One Exposure Management Platform, unifying application security risks with all other exposure data. By integrating static code vulnerability data, Tenable One delivers complete, code-to-runtime visibility across the entire attack surface.

Tenable One ingests, analyzes and normalizes data from relevant application development and security sources, including AI application security tools, such as Claude Security. Tenable One then connects all ingested exposure data – unifying Tenable telemetry with data from other security tools, including endpoint protection, cloud security, vulnerability management, operational technology security and more, and vital business context from repositories like configuration management databases – designed to deliver the most complete view of enterprise risk, and accelerate remediation prioritization and action. With this platform expansion, Tenable One shifts organizations from reactive application scanning to proactive risk prioritization, connecting code risks to the runtime systems, cloud workloads, identities and attack paths they put at risk.

Oracle announces AI-native builder experience for Oracle AI Agent Studio

Oracle has announced a new AI-native builder experience for Oracle AI Agent Studio for Fusion Applications that enables customers and partners to create and run Fusion Agentic Applications natively within Oracle Fusion Cloud Applications. Fusion Agentic Applications represent a new class of enterprise application: outcome-driven systems backed by teams of specialized AI agents that reason, coordinate, and decide, then execute work through Fusion business objects, workflows, tools, policies, approvals, and logged actions.

Unlike standalone agents, copilots, or disconnected AI automation tools, Fusion Agentic Applications are designed to operate inside the enterprise system where the work already happens. They run natively in Oracle Fusion Applications, inherit Fusion security and governance controls, act against Fusion business objects and workflows, and provide the auditability required for enterprise execution. The new builder experience brings no-code, low-code, and pro-code development into one Fusion-native framework.

Coforge launches Nuuron AI OS for the autonomous enterprise

Coforge has announced the launch of Coforge Nuuron, an AI Operating System (AI-OS) designed to help enterprises move beyond isolated AI initiatives and industrialize AI-driven outcomes across the business. Built on years of investment in AI-native platforms including Coforge Forge-X, Coforge evolveOps.AI, Coforge CodeInsight.AI, Coforge Data Cosmos, Coforge Quasar, and BLUESWAN— this AI-OS creates a unified operational layer that connects enterprise knowledge, workflows, decisions, and actions. It enables organizations to deploy agentic AI at scale while maintaining the governance, transparency, and control required for enterprise adoption.

As AI adoption accelerates, organizations face a new challenge: transforming fragmented knowledge, business context, and decision logic into consistent execution. Coforge Nuuron addresses this challenge by converting enterprise intelligence into operational intelligence, enabling AI agents, systems, and people to work together toward measurable business outcomes.

GoDaddy launches AI-ready Developer Platform to simplify domain management

GoDaddy has launched its new Developer Platform, a solution designed to simplify domain management for developers working alongside AI coding assistants, automated workflows and intelligent software agents. The platform integrates domain-related services directly into developer environments, eliminating the need to switch between coding tools and web browsers for essential domain tasks. The launch reflects the growing role of artificial intelligence in software development, where developers increasingly rely on AI-powered assistants to build websites and applications. However, domain registration and configuration have largely remained manual processes requiring users to navigate registrar websites separately.

With the new platform, GoDaddy aims to unify the complete domain lifecycle within the tools developers already use, including terminals, AI chat interfaces and coding assistants. The integrated workflow allows users to search for domains, complete registrations, configure DNS settings and manage domains without leaving their development environment.

Zoho announces Zoho Classes 2.0 for teaching, learning, and student success

Zoho has announced the launch of Zoho Classes 2.0, an AI-powered academic LMS built in India and designed for educational institutions worldwide. The platform is launching first in India, with roll-outs across global markets to follow in the coming months, each with regional capabilities tailored to local educational requirements.

In India, Zoho is making Zoho Classes 2.0 available at no product licensing cost to all Central and State Government schools, colleges, and universities, in a move to democratize access to educational technology. Additionally, any teacher with up to 100 students can use the platform free of charge. Zoho believes education is a critical pillar of nation-building, and that quality learning tools should reach every student and teacher regardless of an institution's budget. Zoho Classes 2.0 brings teaching, learning, student success, and institutional administration together on a unified AI-powered platform.

Salesforce launches SMB Growth Kit to simplify growth for small businesses in India

Salesforce has announced SMB Growth Kit, a connected offering for India's small and medium businesses (SMBs) that brings Agentforce Sales, Slack, and Tableau into one platform designed to meet the needs of fast-growing Indian businesses. This powerful platform helps SMBs replace disconnected tools and apps with a simpler, smarter way to run their business—improving visibility, accelerating collaboration, supporting revenue growth, and going live in four - six weeks.

Agentforce Sales brings structure and visibility to the revenue engine. Instead of relying on spreadsheets, manual updates or one individual to maintain customer records, businesses get a real-time view of every lead, opportunity and pipeline. Automated lead assignment, workflow automation and mobile access help sales teams move faster, while built-in AI capabilities—including opportunity scoring, forecasting and intelligent recommendations—help teams focus on the opportunities that matter most without requiring specialist expertise.

TRAI discusses plans to build unified anti-spam network in with Meta and Google

The Telecom Regulatory Authority of India (TRAI) is in discussions with Meta and Google to create a unified system for tackling spam and scam communications. This will be done by integrating user-reported spam data from WhatsApp and Android phone dialers with telecom operators' complaint platforms. The proposed framework would connect reports from these digital platforms with telecom companies' Distributed Ledger Technology (DLT) systems and TRAI's Do Not Disturb (DND) portal, enabling faster identification and action against repeat offenders.

The initiative is part of India's broader effort to strengthen consumer protection.

If implemented, it would represent one of the country's most comprehensive anti-spam collaborations involving telecom operators, messaging platforms, and smartphone ecosystem providers.

The telecom regulator wants spam complaints made on digital platforms to feed into telecom operators' enforcement systems.

The proposal is currently under discussion with Meta and Google, and no final implementation timeline has been announced.

Bharti Airtel Shifts Growth Focus to Financial Services, Cloud and Data Centres

Following an investment of Rs. 3.3 lakh crore in digital infrastructure over the past decade, Bharti Airtel is now shifting its focus toward financial services, data centres and cloud as its next growth drivers, Chairman Sunil Bharti Mittal said in the telecom operator's FY2026 annual report.

He also committed Rs. 20,000 crore to strengthen its NBFC arm, Airtel Money, while its data centre subsidiary, Nxtra, recently secured $1 billion (approximately Rs. 9,500 crore) in funding to expand its infrastructure to 1 gigawatt (GW) of capacity.

"Over the last few years, we took a calibrated approach to build new growth engines for Airtel. These bold bets yielded strong outcomes and have grown our conviction in three adjacencies where we believe Airtel has a clear right to win -- financial services, data centres and Airtel Cloud," Mittal said.

Mittal announced that Airtel Money has received approval from the Reserve Bank of India to operate as a non-deposit-taking Non-Banking Financial Company (NBFC).

Smaller UPI apps raise competition concerns over NPCI's proposed UPI Meta framework

Several smaller Unified Payments Interface (UPI) applications have urged the National Payments Corporation of India (NPCI) to revisit its proposed UPI Meta framework, expressing concerns that the initiative could disproportionately benefit dominant payment platforms while making it more difficult for emerging players to compete.

According to reports, multiple UPI service providers have jointly submitted a representation to NPCI, questioning both the necessity and the potential impact of the proposed framework. The companies contend that the existing UPI payment flow already offers a smooth user experience and that the new mechanism may alter the platform's open and interoperable design without delivering significant benefits to consumers.

The report, which reviewed a copy of the representation, said the payment firms have called for broader stakeholder consultations before the framework is introduced. The proposed UPI Meta framework would allow customers to select and save a preferred UPI application on merchant platforms such as Amazon, Blinkit and Swiggy. Once configured, users could complete future transactions directly through PIN or biometric authentication without being redirected to their chosen payment application.

Delhi set to roll out Smart-PDS to digitise ration distribution

The Delhi government is preparing to modernise its Public Distribution System (PDS) with the introduction of the Smart Public Distribution System (Smart-PDS), a digital platform designed to streamline ration-card services and improve the delivery of subsidised foodgrains across the national capital.

The initiative aims to shift several key services online, reducing the need for beneficiaries to visit government offices while offering greater visibility into the ration distribution process. Once implemented, eligible households will be able to check the status of their ration allocation, track when supplies reach Fair Price Shops, and receive updates on the expected distribution schedule through digital channels.

The proposed system is also intended to strengthen oversight of the ration distribution network by addressing issues such as fake ration cards, duplicate records, black marketing and diversion of subsidised foodgrains.

Under the Smart-PDS framework, ration-card holders will be able to complete a range of services online. These include adding or deleting family members from ration cards, uploading supporting documents and tracking the status of applications without repeated visits to government offices.

Paytm seeks RBI approval to revive digital wallet business

One97 Communications has approached the Reserve Bank of India (RBI) for a Prepaid Payment Instrument (PPI) licence, marking a significant step in its efforts to revive Paytm's digital wallet business after the closure of its payments bank operations. If approved, the licence would enable the company to independently offer prepaid wallet services and expand its digital payments portfolio beyond Unified Payments Interface (UPI)-based transactions.

The application comes as Paytm continues to reshape its payments strategy following regulatory action against Paytm Payments Bank. While the company has maintained uninterrupted UPI services through partnerships with multiple banks, its wallet business has remained inactive since the banking arm ceased operations.

A PPI licence authorises eligible entities to issue digital wallets and other prepaid payment products that allow users to load money in advance for transactions. Such wallets can be used for merchant payments, utility bill settlements, online purchases and fund transfers within regulatory limits, providing an alternative payment option alongside bank accounts and UPI.

Vodafone Idea teams up with Meta to Deliver Safer, Faster & Seamless Verification for its Users Across Meta Platforms

Vodafone Idea (Vi) announced the launch of Silent Mobile Verification (SMV) capabilities across Meta Platforms WhatsApp, Facebook and Instagram for Vi users enabling safer, seamless and password-less digital experiences for millions of users.

SMV is a secure, network-based authentication technology that verifies a user's mobile number in the background without requiring manual entry of verification credentials, switching between apps, or waiting for verification messages. When a Vi user accesses WhatsApp, Facebook and Instagram on the Vi mobile network, the verification request is validated through the telecom network itself, delivering a faster and frictionless experience.

Vi users may experience SMV-supported journeys across scenarios such as new user registration, mobile number verification, login and re-login, account recovery, and authentication during security checks. This translates into faster onboarding, fewer manual steps, and enhanced protection against phishing and digital identity risks.

TP-Link India concludes JAS 2025 incentive scheme with Vietnam recognition tour

TP-Link India recently concluded its JAS 2025 Incentive Scheme by rewarding its top-performing channel partners with an incentive trip to Phu Quoc, Vietnam. The initiative recognised outstanding sales performance across the company's FTTH, SOHO and VIGI product portfolios while reinforcing its commitment to strengthening long-term channel partnerships. A total of 33 partner organisations, represented by 48 participants, qualified for the programme based on their sales achievements during the incentive period.

The recognition programme also enabled partners to interact with TP-Link India's leadership team and gain insights into the company's strategic vision and future roadmap. According to the company, the initiative reflects its continued investment in the partner ecosystem, recognising the critical role channel partners play in driving business growth and expanding its networking and surveillance solutions across India. It also provided an opportunity to strengthen collaboration and reinforce long-term business relationships.

Bijoy Alaylo, Director & COO, TP-Link India, said, "At TP-Link, we remain committed to instilling confidence in our partners, especially during challenging times. Our channel partners have been instrumental in our success, and initiatives like the JAS 2025 Incentive Scheme are our way of recognising their unwavering commitment and exceptional performance."

TAIT's 'Kya Lagta Hai?' Market Adda spotlights IT channel trends

The Technology Association of Information Technology (TAIT) hosted another edition of its flagship Market Adda in Mumbai recently, bringing together members, technology leaders, distributors and industry experts for discussions on emerging trends and business

opportunities. Held at the Ginget Hotel, the session was themed "Kya Lagta Hai?" and encouraged participants to exchange perspectives on the evolving IT channel landscape through an interactive discussion format instead of a conventional seminar.

Moderated by Rushabh Shah, the panel featured Gaurav Jaitley (HP Consumer), Vijay Goel (Miracle Tech Distributors), Chetan Timbadia (DC Infotech and Communication), Atul Gaur (Savex Technologies) and Abhishek Jain (Arihant Infosolutions). Discussions focused on channel growth, cybersecurity opportunities, enterprise AI adoption, enterprise storage and data centre investments. Members actively participated by sharing experiences and raising questions on current market developments. The event also featured a networking activity for members, while event partner NPAV showcased its latest solutions and partner initiatives. TAIT directors felicitated the panellists, reaffirming the association's focus on knowledge sharing, collaboration and helping members stay updated on emerging technologies, evolving market trends and new business opportunities.

ISODA relaunches Hyderabad Chapter to strengthen channel collaboration

The Infotech Software Dealers Association (ISODA) successfully relaunched its Hyderabad Chapter, bringing together system integrators, value-added resellers, distributors, ISVs and SaaS companies for an evening focused on collaboration, business growth and networking. The event also saw participation from ISODA's national leadership and members. Designed as an interactive gathering, the programme encouraged discussions and peer engagement across the IT channel community.

ISODA Chairman Vinod Kumar highlighted the challenges facing the IT channel ecosystem and stressed the need for stronger collaboration, knowledge sharing and trusted business relationships.

Vice Chairman Vimesh Avlani and Membership Drive Lead Yogesh Chordia outlined ISODA's member ecosystem, chapter initiatives and business benefits. Hyderabad-based members also shared how the association has supported growth through referrals, partnerships and knowledge exchange.

Speaking on the occasion, Vimesh Avlani, Vice Chairman, ISODA, said, "Strong industry associations are built on participation, trust and collaboration. Hyderabad has always been an important technology market and we are delighted to see such encouraging interest as we strengthen ISODA's presence in the city." ISODA represents over 200 member companies across 25 cities, generating more than Rs. 15,000 crore in annual business.

Iris Global evolves into a business transformation enabler with IRIS 2.0

Iris Global Services has unveiled IRIS 2.0, marking its transition from a technology distributor to a future-focused business transformation enabler. The announcement was made during its customer and partner summit in Jaipur, attended by more than 75 customers, channel partners and technology leaders. The company also introduced Persistent Systems' SASVA enterprise AI platform, which Iris Global will distribute across India, the Middle East and Asia Pacific under its strategic partnership with Persistent Systems.

SASVA is designed to help enterprises accelerate AI adoption, strengthen cybersecurity, modernise IT infrastructure and advance cloud transformation. The event also featured keynote sessions on AI-ready infrastructure, cyber resilience and enterprise innovation, alongside solution demonstrations, partner interactions and networking opportunities. According to the company, the SASVA launch marks the first strategic milestone under its partnership with Persistent Systems and reinforces its long-term enterprise AI strategy.

Speaking on the occasion, Sanjiv Krishen, Founder-CMD, Iris Global, said, "Technology is evolving at an unprecedented pace, and businesses today require much more than products—they need trusted partners capable of guiding them through continuous transformation. IRIS 2.0 reflects our commitment to building stronger capabilities, deeper technology alliances and a future-ready partner ecosystem."

CADYCE Launches CA-HXKVM HDMI KVM Extender for Enterprise AV Deployments

CADYCE has introduced the CA-HXKVM, a USB HDMI KVM Extender Over Ethernet designed to support long-distance HDMI and USB signal transmission for enterprise and commercial AV environments. The solution enables 4K Ultra HD video, along with USB keyboard and mouse connectivity, to be extended over a single Ethernet cable for distances of up to 80 metres.

Aimed at professional deployments, the extender is suited for control rooms, corporate offices, security monitoring centres, digital signage, educational institutions, command centres and industrial environments where reliable remote system access and high-quality video transmission are critical.

DESIGNED FOR ENTERPRISE AV INFRASTRUCTURE

The CA-HXKVM supports HDMI 2.0 and HDCP 2.2, ensuring compatibility with modern 4K displays and protected digital content. It also enables users to control remotely located computers through USB keyboard and mouse connectivity, eliminating the need for direct physical access to systems.

A key feature is its Power-over-Cable (PoC) technology, which requires power at only one end—either the transmitter or receiver. This simplifies installation, reduces cabling requirements and offers greater flexibility for enterprise AV deployments.

The extender supports CAT5e, CAT6, CAT6A and CAT7 Ethernet cables, delivering stable signal transmission while preserving video quality and USB performance across distances of up to 80 metres.

STRENGTHENING ENTERPRISE CONNECTIVITY PORTFOLIO

The compact and durable device supports USB 2.0 and is compatible with Windows, macOS, Linux and other operating systems, allowing integration into diverse enterprise IT environments. It is also certified for CE, FCC, RoHS, UKCA and BIS compliance.

Each package includes a transmitter, receiver, 12V DC power adapter, 1.8-metre HDMI and USB KVM cable, and a user manual for deployment.

With the launch of the CA-HXKVM, CADYCE is expanding its portfolio of connectivity, networking and professional AV solutions for enterprise customers.

The new extender is positioned to address the growing demand for dependable long-distance HDMI and USB signal extension, offering system integrators, AV consultants, enterprise IT teams and channel partners a solution for deploying scalable AV infrastructure across commercial and industrial environments.

Hikvision Unveils Latest Active LED Display Portfolio for Enterprise AV Market

Hikvision India has expanded its commercial display offerings with the launch of its Active LED display portfolio, strengthening its presence in the professional AV (Pro AV) market. Leveraging its expertise in image processing, artificial intelligence (AI) and AIoT-enabled manufacturing, the company has introduced a range of indoor, outdoor, creative and modular LED display solutions for commercial applications.

The portfolio is designed for deployments across control rooms, retail, corporate offices, educational institutions, advertising and public infrastructure. Hikvision said the displays combine energy-efficient operation, high refresh rates and proprietary control technologies to deliver reliable visual performance across diverse enterprise environments.

BROAD RANGE OF DISPLAY SOLUTIONS

The portfolio includes regular LED modules supporting indoor pixel pitches from P1.2 to P3.0 and outdoor options from P2.5 to P8. It also features soft LED modules for curved and cylindrical installations, alongside cut-edge modules for customised display designs without compromising image continuity.

For indoor deployments, Hikvision offers cabinets based on COB (Chip-on-Board), HOB (Glue-on-Board) and SMD (Surface Mounted Device) technologies. The displays feature ultra-slim cabinets, a 16:9 aspect ratio for Full HD and Ultra HD applications, seamless splicing and single-cabinet calibration for colour consistency. Outdoor cabinets provide brightness of up to 6,500 nits with IP67 front and IP66 rear protection for demanding environments.

INTEGRATED MANAGEMENT PLATFORM

The portfolio is supported by LED controllers offering integrated video wall management, wireless projection from laptops and mobile devices, and support for flexible display layouts, including irregular screen configurations. Hikvision's self-developed software platform enables centralised device monitoring, content creation and scheduling, signal source management, remote content distribution, cloud-based deployment and third-party integration.

The company said its integrated ecosystem—covering controllers, receiving cards and software developed in-house—simplifies deployment while improving compatibility, scalability and long-term system reliability. The Active LED display portfolio is targeted at Smart City and traffic control rooms, transport hubs, retail, quick-service restaurants, corporate facilities, educational institutions, religious venues and other commercial applications, further expanding Hikvision India's enterprise AV and commercial display portfolio.

AI, Trust and Alliances: The New Enterprise Imperative

VARINDIA captures exclusive perspectives from senior technology leaders on AI, cybersecurity, partnerships and the future of digital transformation.

Artificial Intelligence has moved beyond experimentation to become a strategic priority for enterprises across industries. As organisations transition from Generative AI to Agentic AI, the focus is increasingly shifting towards practical adoption, stronger governance and measurable business outcomes. Technology leaders recognise that AI is no longer a standalone capability but part of a broader digital ecosystem encompassing cloud, cybersecurity, automation, data governance and trusted partnerships. Success will depend not only on adopting emerging technologies but also on aligning them with business objectives, building secure digital foundations and preparing organisations for long-term transformation.

Against this backdrop, VARINDIA sat down with CIOs, CISOs, CTOs and other senior technology leaders on the sidelines of the 24th INFOTECH FORUM 2026 to gather their exclusive perspectives on the technologies, priorities and partnerships shaping the future of enterprise IT. Across industries, the conversations reflected a shared emphasis on responsible AI adoption, cybersecurity resilience, data privacy, enterprise-wide collaboration and practical AI use cases that deliver measurable business value. They also highlighted the growing importance of strong partner ecosystems and industry alliances in accelerating digital transformation. Collectively, these insights provide a comprehensive view of how enterprise leaders are preparing for an AI-driven future while ensuring technology adoption remains secure, trusted and aligned with evolving business priorities.

Agentic AI will transform the way IT operations are managed

Agentic AI is expected to create significant opportunities by automating end-to-end business processes, particularly across IT operations. One of the biggest areas of impact will be the automation of routine operational activities, including Level 1 and Level 2 support functions, enabling organisations to improve operational efficiency and reduce manual effort. As AI agents continue to evolve, they are expected to play an increasingly important role in managing enterprise IT operations. Over the next 20 to 30 months, Agentic AI has the potential to bring meaningful changes to the way organisations deliver and manage technology services.

AI, cloud and cybersecurity are all critical and should be viewed as complementary technologies. AI can help automate business processes, while cloud provides the platform required to build and operate digital environments. At the same time, cybersecurity remains essential for protecting enterprise infrastructure. Organisations should therefore strengthen all three capabilities together to support secure, scalable and effective digital transformation across the enterprise.

AI is increasingly becoming an integral part of modern business operations and is expected to remain a core component of enterprise technology strategies. As organisations implement AI, strong processes and appropriate guardrails become essential for using these technologies effectively and at enterprise scale. Platforms such as INFOTECH FORUM provide valuable opportunities to exchange insights on AI, cybersecurity and emerging technologies while reinforcing the importance of combining technology adoption with robust processes, governance and operational discipline.

SANJEEV JAIN, CIO, INTEGREON MANAGED SOLUTIONS INDIA PVT. LTD.

AI is redefining the way organisations do business

Artificial Intelligence is changing the way organisations think, innovate and build products. While India may still be developing its own large language models, enterprises already have opportunities to leverage globally available AI models to accelerate business transformation. Organisations should redefine the way they operate, compete and develop products because AI is reshaping business models across industries. Enterprises that effectively adopt AI use cases will be better positioned to remain competitive, while those that fail to adapt risk falling behind as AI becomes increasingly integral to business.

Technology alliances are becoming increasingly important because no single organisation can independently develop every capability or innovation required for future growth. Collaboration enables enterprises to learn from new ideas, emerging technologies and the expertise of others across the industry. As innovation continues to accelerate, partnerships help organisations strengthen product strategies, identify new opportunities and create greater business value by bringing together complementary capabilities and shared knowledge.

AI also creates important business opportunities by helping organisations connect with the right customers, improve products and strengthen business strategies. It can support cost optimisation through improved efficiency, better resource utilisation and more effective decision-making, contributing to stronger business performance and improved profitability. Platforms such as INFOTECH FORUM provide valuable opportunities to learn from emerging technology use cases, exchange innovative ideas and strengthen collaboration across the technology ecosystem, helping organisations accelerate innovation and business growth.

VV JACOB, CHIEF GENERAL MANAGER – SYSTEMS/IT, MALAYALA MANORAMA CO. LTD.

Scaling AI requires data readiness, secure infrastructure and strong partnerships

As organisations work towards scaling AI from proof-of-concepts to enterprise deployments, the biggest challenge lies in data readiness, governance and security rather than the AI model itself. While many enterprises have initiated AI pilots, only a small percentage have successfully moved them into production because inference environments introduce new complexities around data management, compliance and security. With the Digital Personal Data Protection (DPDP) framework becoming increasingly important, organisations must ensure that AI-driven outcomes remain secure, compliant and supported by appropriate governance and human oversight wherever required.

Building a successful AI ecosystem also requires a strong digital infrastructure. AI workloads can no longer rely on retrofitted legacy data centres, making purpose-built, high-performance infrastructure essential for supporting advanced analytics, AI-driven decision-making and future-ready enterprise workloads. Looking ahead, Agentic AI is expected to be among the most influential technologies over the next two years, as organisations across industries increasingly explore intelligent systems to enhance business operations, improve efficiency and drive innovation.

A strong partner ecosystem is equally critical in helping organisations navigate an increasingly diverse technology landscape. While OEMs provide the underlying technologies, partners play a vital role in identifying and bringing the right solutions to customers. Events such as INFOTECH FORUM 2026 also provide valuable opportunities to exchange insights on AI, cybersecurity and emerging solutions, enabling organisations to stay aligned with evolving technology trends and make more informed technology decisions.

AVANEESH VATS, VP (DIGITAL INFRA & INNOVATION) & CIO, TECHNO ELECTRIC & ENGINEERING CO. LTD.

Responsible AI and data will shape the next phase of digital transformation

Over the past three decades, technology has transformed not only the way organisations operate but also the way individuals live and interact with the world. Digital technologies have become an integral part of everyday life, making connectivity, digital payments and online services indispensable. India has led this transformation through initiatives such as Digital India, Aadhaar, Jan Dhan Yojana and UPI, demonstrating technology adoption at an unprecedented scale. As AI continues to evolve, data has become a critical asset, creating an opportunity for India to develop indigenous AI models and strengthen its digital capabilities.

Responsible AI should be viewed as a shared responsibility rather than the obligation of any single stakeholder. Consumers must use AI responsibly, technology and data providers should implement appropriate governance mechanisms, governments need to establish balanced policy frameworks, and enterprises must foster ethical practices while deploying AI across their organisations. A collaborative and federated approach is essential, ensuring accountability while enabling innovation to progress responsibly.

Platforms such as VARINDIA's INFOTECH FORUM play an important role in bringing together industry leaders to exchange ideas on emerging technologies and future challenges. While AI can generate answers with increasing sophistication, real intelligence lies in asking the right questions and identifying the most relevant issues for discussion. Curating such conversations requires extensive research and sustained effort, making these forums valuable for encouraging knowledge sharing, industry collaboration and informed technology leadership.

BHARAT B ANAND, GROUP CITO, CONTEC GLOBAL

Privacy and responsible AI are reshaping enterprise cybersecurity

Privacy and data protection have become central to the cybersecurity agenda as organisations face increasingly stringent regulatory requirements and the potential for significant penalties in the event of non-compliance. At the same time, emerging technologies such as quantum computing are creating new security challenges by reshaping the future of encryption. These developments require enterprises to strengthen their security posture while preparing for evolving cyber risks.

As organisations move from AI pilots to enterprise adoption, it is equally important to understand both the opportunities and the risks associated with AI. Enterprises need clear guidance on what information can be shared with AI models, how these systems learn from organisational data, and the safeguards required to protect sensitive information. AI is a double-edged sword—it can significantly improve productivity, but without proper governance, user awareness and well-defined boundaries, it can also expose confidential data and create serious business risks. Building awareness around AI threats and responsible AI usage is therefore essential for secure adoption.

Our focus is on helping organisations strengthen cyber resilience through cybersecurity audits, forensic investigations and proactive identification of anomalies that could lead to sensitive data exposure or financial loss. By providing actionable insights into security gaps, we help enterprises mitigate risks before they escalate. Platforms such as INFOTECH FORUM also provide valuable opportunities for cybersecurity experts, industry leaders and technology providers to exchange knowledge and collaborate on emerging security challenges.

DR. HARSHA THENNARASU, FOUNDER & CISO, HKIT SECURITY SOLUTIONS

Security by design is essential in the age of AI

Cybersecurity is evolving rapidly as AI transforms both the threat landscape and the way organisations defend their digital assets. Since 2022, our focus has expanded to helping enterprises, government agencies, defence personnel and law enforcement understand AI-driven cyber threats while strengthening capabilities in cybercrime investigation and digital forensics. AI has accelerated threats such as deepfakes, voice cloning, synthetic content and advanced malware, but it also offers powerful opportunities to strengthen cyber defence. The priority should be to develop more AI-driven security solutions that help defenders stay ahead of evolving threats while strengthening resilience against emerging cyber risks.

As organisations accelerate AI adoption, security must become an organisational culture rather than being limited to periodic awareness programmes. Strengthening digital infrastructure, conducting regular security audits and adopting security-by-design principles are essential for reducing cyber risks. The Digital Personal Data Protection (DPDP) Act is a welcome step as it places greater emphasis on data privacy, user consent and organisational accountability, encouraging enterprises to take data protection more seriously while strengthening their security posture.

Collaboration is equally critical in building a stronger cybersecurity ecosystem. Organisations, technology providers and security partners must combine their expertise to address emerging challenges and accelerate innovation. Platforms such as INFOTECH FORUM provide valuable opportunities for knowledge sharing, networking and meaningful collaboration, helping organisations discover practical solutions while strengthening India's cybersecurity ecosystem through continuous awareness, innovation and collective action.

DR. RAKSHIT TANDON, FOUNDER & DIRECTOR, RT CYBER ACADEMY

Embedding AI across business processes to drive transformation

AI is at the core of our vision to transform the co-living industry by delivering a more seamless, convenient and digitally enabled experience for residents. As a digital-first organisation, we have built an in-house technology platform that serves as the operating system for our business, integrating functions across operations, finance, compliance and other critical processes. Through digitalisation, automation and sustainable practices, we are focused on improving operational efficiency, optimising costs and creating long-term value while enhancing the overall resident experience.

We view Agentic AI as far more than a tool for isolated use cases. Its real potential lies in augmenting people and transforming the way organisations operate across functions. Whether it is sales, business development, operations, finance or technology, AI can act as an intelligent assistant that enhances productivity, supports decision-making and enables more efficient workflows. Embedding AI across business processes will help organisations unlock meaningful enterprise-wide transformation and maximise its value across the business.

As AI adoption accelerates, governance, compliance and robust security frameworks will become increasingly important, alongside evolving zero-trust approaches for AI-enabled environments. Building secure and trusted AI ecosystems will be critical to sustaining long-term innovation. Industry platforms such as INFOTECH FORUM provide valuable opportunities for technology leaders to exchange practical use cases, learn from cross-industry experiences and evaluate how proven innovations can be adapted within their own organisations to deliver stronger business outcomes and measurable returns on investment.

GAURAV VIJ, FOUNDER & CIO, HOOLIV

AI, cloud and data security will shape the next phase of digital transformation

Artificial Intelligence, cloud computing, and data security and privacy will be among the most influential technologies shaping the next phase of digital transformation. Whether organisations are delivering government services, developing enterprise solutions or building digital platforms, these three pillars will play a defining role. AI, in particular, presents significant opportunities to derive insights from large datasets, identify meaningful patterns and drive innovation at scale, creating new possibilities for improving services and operational efficiency.

Realising AI's full potential, however, requires a balanced approach that combines innovation with responsible governance. Organisations must address challenges such as AI bias, explainability, security by design and continuous risk monitoring as integral elements of their AI governance framework. Enterprises that successfully embed these principles while responsibly scaling AI adoption will be better positioned to create sustainable value and build greater trust in AI-driven systems.

A strong ecosystem comprising industry, government, academia, research institutions and startups is equally essential for accelerating innovation and large-scale digital transformation. While governments provide policy direction, industry contributes products and solutions, academia advances research, and startups bring speed and disruptive thinking. The success of large public digital initiatives demonstrates the value of such collaboration in delivering better citizen services. Platforms such as INFOTECH FORUM further strengthen this ecosystem by bringing together diverse experts to exchange ideas, nurture AI talent and identify priorities that can help shape the future of India's technology landscape.

GOLOK KUMAR SIMLI, PRESIDENT - TECHNOLOGY & INNOVATION, BLS INTERNATIONAL

AI is evolving into an enterprise-wide capability

AI is rapidly evolving from an individual productivity tool into an enterprise-wide capability that can enhance organisational intelligence and improve business outcomes. Enterprises are increasingly exploring how AI can be integrated into their existing technology landscape with appropriate guardrails, enabling it to support decision-making, streamline operations and improve key performance indicators across the organisation. The real opportunity lies in embedding AI with appropriate guardrails so that it delivers measurable value while aligning with organisational objectives.

As AI adoption accelerates, organisations must recognise that it also expands the cybersecurity threat landscape. Establishing clear boundaries around what information can be shared with AI systems and implementing appropriate governance controls are essential for secure adoption. The emergence of 'shadow AI' highlights the need for greater visibility, user awareness and robust safeguards to prevent sensitive organisational information from being inadvertently exposed. When combined with cybersecurity and automation, AI has the potential to become a powerful enabler of business transformation over the coming years.

A strong partner ecosystem is equally critical to successful technology adoption. Organisations cannot build every capability internally and therefore benefit from working with knowledgeable partners who understand their operational landscape and recommend the most appropriate solutions rather than simply offering products. Events such as INFOTECH FORUM provide valuable opportunities to identify trusted technology partners, exchange practical insights and build long-term collaborations that support secure, effective and sustainable digital transformation.

KAMAL MATTA, CIO & CISO, SONIC BIOCHEM EXTRACTIONS

AI as a human assistant is driving secure and practical enterprise adoption

Artificial Intelligence is becoming an important enabler for enterprise operations, but its adoption must be approached with appropriate caution and governance. Rather than replacing human expertise, AI should serve as an intelligent assistant that improves efficiency while keeping people at the centre of decision-making. In our organisation, AI is already being used across service operations, including maintenance and insurance services, as well as document processing to automate information extraction from PDFs. We are also applying AI to analyse customers' financial statements to support informed credit-related assessments, while ensuring deployment remains measured, controlled and aligned with business requirements instead of pursuing an all-in approach to AI adoption.

As AI adoption expands, organisations must remain equally focused on managing associated risks. For enterprises handling sensitive financial and customer information, compliance with the Digital Personal Data Protection Act (DPDPA) is a key priority. Building a strong privacy framework through recognised standards such as ISO 27701 helps organisations strengthen preparedness for evolving regulatory requirements while reinforcing trust in digital operations.

A strong partner ecosystem is equally important for delivering secure and reliable technology services. Technology and business partners extend an organisation's capabilities, making collaboration essential for addressing emerging challenges and delivering better outcomes. Platforms such as INFOTECH FORUM provide valuable opportunities to exchange experiences with industry peers, understand evolving technology trends and help organisations prepare more effectively for future risks and opportunities across the industry.

RAJESH K THANUA, GM - TECHNOLOGY & CISO, SMAS AUTO LEASING INDIA PVT. LTD.

AI adoption depends as much on people as technology

Artificial Intelligence has evolved beyond being a productivity tool and is becoming an important driver of enterprise transformation. As AI progresses from executing tasks to making recommendations and collaborating across applications and business environments, organisations must focus not only on adopting the technology but also on preparing people to use it effectively. Successful AI adoption requires a balanced approach that considers AI governance, risk management, model oversight and business outcomes together. The real challenge is not simply creating AI-ready environments, but enabling people to understand, adopt and utilise AI responsibly across the organisation while maximising its long-term business value.

While AI is reshaping cybersecurity, people remain the most common target for cyberattacks. AI has made phishing, identity-based attacks and other threats faster, more relevant and increasingly sophisticated. As attackers leverage AI, defenders must also integrate AI into their security strategies. However, technology alone is not enough. Effective cyber resilience depends on the right combination of people, processes and technology, with organisations adopting AI in line with their business priorities and operational requirements.

Technology partnerships and industry collaboration are essential for navigating an evolving threat landscape. Organisations must prioritise technologies that best address their business needs while delivering measurable value. Platforms such as INFOTECH FORUM provide valuable opportunities to understand cross-industry security challenges, explore emerging technologies and exchange practical insights, helping organisations strengthen resilience and prepare more effectively for future risks.

RAJVEER SINGH, SENIOR RISK OFFICER - TECHNOLOGY SECURITY FOUNDATION, SAXO BANK

Monitoring AI, data flows and governance will define the next phase of cybersecurity

ROHIT PONNAPALLI,
CISO, ENVOY GLOBAL

AI is reshaping cybersecurity priorities by expanding the scope of security beyond traditional infrastructure to include AI models, data flows and interactions across enterprise environments. As organisations adopt GenAI and Agentic AI, it becomes increasingly important to understand how different business functions use AI, what data is accessed, and how appropriate security controls can prevent data leakage while enabling innovation. At the same time, enterprises should look beyond point-in-time compliance towards a more continuous approach to security posture and compliance management that evolves alongside new applications, infrastructure and business requirements.

AI also presents significant opportunities to strengthen cybersecurity operations. While organisations must ensure employees use authorised AI platforms and protect sensitive data from unintended exposure, AI can also improve security efficiency through faster incident detection, investigation and response. As cyberattacks become increasingly automated and faster to execute, leveraging AI-driven security capabilities can help organisations respond more effectively while supporting stronger business resilience. Security today is not just a support function but an important business enabler that builds trust and enables growth.

Strong industry alliances remain fundamental to advancing cybersecurity maturity. Collaboration with technology partners, security communities and industry peers helps organisations understand emerging threats, evaluate new capabilities and prepare for future challenges. Platforms such as INFOTECH FORUM create valuable opportunities to exchange practical insights, discover innovative security solutions and strengthen long-term security planning through continuous learning and collaboration.

Agentic AI is driving practical enterprise transformation

SANDEEP PANDITA,
AVP - IT, AGI GROWTHX
PVT. LTD.

Agentic AI is beginning to deliver tangible business value by enabling enterprise-scale automation and operational transformation. Our recent deployment of multilingual Agentic AI within customer care has demonstrated how intelligent automation can improve operational efficiency while reducing dependence on manual processes and optimising costs. As organisations continue to explore practical AI use cases, the focus will increasingly shift towards embedding AI across business functions in ways that enhance customer experience, improve service delivery and generate measurable business outcomes.

Alongside AI, cloud, cybersecurity and automation will remain fundamental drivers of enterprise transformation. These technologies are closely interconnected and together provide the foundation for secure, scalable and efficient digital operations. As organisations accelerate digital adoption, protecting customer information and maintaining strong control over enterprise data become even more important. With data privacy regulations such as the Digital Personal Data Protection (DPDP) framework gaining prominence, enterprises must strengthen data governance and implement appropriate security controls to safeguard sensitive information while supporting business growth.

Technology partnerships and industry collaboration play an important role in helping organisations adopt emerging technologies securely and effectively. Platforms such as INFOTECH FORUM create valuable opportunities to exchange ideas, understand evolving cyber threats and learn about new technology innovations. Such interactions enable organisations to evaluate practical solutions, strengthen their security posture and make more informed technology decisions while delivering a seamless and secure experience for customers and the business.

AI, quantum computing and industry alliances will shape enterprise growth

SARITA PADMINI,
SR. DIRECTOR,
PROTIVITI INDIA

Indian enterprises have a significant opportunity to accelerate growth by investing in emerging technologies and future-ready business models. Artificial Intelligence is among the most important opportunities today, enabling organisations to drive innovation and create new business value. At the same time, the continued expansion of GCCs presents a strong avenue for growth, while quantum computing represents a strategic area that organisations should begin preparing for now. Investing early while evaluating long-term returns will help enterprises build the capabilities needed for the next phase of digital transformation.

Industry alliances are equally critical in helping organisations navigate an evolving business and technology landscape. Collaboration enables enterprises to better understand market trends, emerging risks and growth opportunities while supporting more informed investment decisions. Alliances also provide valuable insights into technology adoption, digital transformation strategies and risk-based approaches, helping organisations strengthen resilience and plan their future roadmap with greater confidence. Building a strong collaborative ecosystem is therefore essential for driving sustainable growth and innovation.

Platforms such as INFOTECH FORUM play an important role in bringing together industry leaders to exchange ideas and discuss the technologies shaping the future. As conversations increasingly extend beyond AI to the long-term potential of quantum computing, such forums help organisations better understand future technology priorities. They provide valuable insights into emerging trends, encourage strategic thinking and support more informed decisions as enterprises plan their long-term technology and business transformation journeys.

Define the business problem before adopting AI

SONAM MALLIK,
HEAD - IT, INTERARCH BUILDING SOLUTIONS

Artificial Intelligence, whether Generative AI or Agentic AI, is emerging as a powerful enabler of enterprise transformation by improving efficiency, productivity and enabling new business models. However, organisations should avoid adopting AI simply because it is gaining momentum. The first priority should be to clearly identify and define the business problem that needs to be solved. Once that foundation is in place, selecting the right AI solution becomes far more effective and aligned with organisational objectives. Enterprises that adopt this problem-first approach will be better positioned to derive meaningful value from AI investments while supporting long-term business transformation.

Beyond AI, technologies such as machine learning, augmented reality, virtual reality and the Internet of Things will also play an important role in shaping enterprise innovation. For manufacturing organisations, technology partnerships are essential because their primary focus remains manufacturing excellence. Successful digital transformation increasingly depends on co-creating, co-designing and co-building technology solutions with trusted partners who bring complementary expertise and implementation capabilities.

Partnerships deliver the best outcomes only when organisations first establish clear business goals and understand the specific challenges they want to address. Different partners may contribute to solution design and implementation, making ecosystem collaboration essential. Platforms such as INFOTECH FORUM provide valuable opportunities to learn from industry use cases, evaluate relevant technologies and gain practical insights into engaging leadership teams while advancing technology-driven business transformation.

Agentic AI can be a game changer for enterprise transformation

SUJOY BRAHMACHARI,
CIO & CISO, ROSMERTA TECHNOLOGIES LTD.

Agentic AI has the potential to become a digital workforce within enterprises by improving productivity, enhancing accuracy and supporting business processes. However, its effectiveness depends on being properly trained so that it performs reliably and minimises errors. When implemented with the right data models and appropriate oversight, Agentic AI can become a significant enabler of enterprise transformation, helping organisations improve operational efficiency, strengthen process execution and deliver better business outcomes across different functions.

The greatest business value will come from the combined adoption of AI, cloud, cybersecurity and automation rather than from any single technology. AI has the potential to strengthen each of these areas through its capabilities, provided it is configured appropriately. Equally important is ensuring that the data models used for AI are accurate and transparent, as a strong data foundation is essential for enabling reliable outcomes, improving trust in AI-driven initiatives and supporting sustainable technology adoption across the enterprise.

Technology partnerships remain critical for successful digital transformation. Enterprises and technology vendors must work together closely, with partners bringing the right implementation skills and expertise to deliver sophisticated technology solutions effectively. Such collaboration enables organisations to maximise the value of technology investments. Platforms such as INFOTECH FORUM continue to provide valuable opportunities to explore emerging technology trends, learn from expert discussions, exchange practical insights and strengthen collaboration across the technology ecosystem while encouraging innovation across the industry.

AI will augment healthcare, not replace human expertise

SURJEET THAKUR,
CIO, RAJAGIRI HOSPITAL, KOCHI

Artificial Intelligence is creating significant opportunities across healthcare by supporting precision medicine, advancing drug discovery and improving patient care. AI is becoming an important enabler across the healthcare ecosystem, helping clinicians make more informed decisions and improving the quality of care. However, AI should be viewed as an assistive technology rather than a replacement for doctors or nurses. Its real value lies in augmenting healthcare professionals, enabling better clinical outcomes while preserving the central role of human expertise in patient care.

Beyond AI, robotic process automation (RPA) and cybersecurity will remain key priorities for healthcare organisations. As healthcare becomes increasingly digital, safeguarding sensitive patient information is more important than ever, with cybersecurity also receiving greater emphasis in evolving healthcare standards. At the same time, awareness continues to be one of the biggest cybersecurity challenges. As cyber threats become more sophisticated, organisations must strengthen user awareness and encourage responsible digital practices, as even a single click on a malicious email or message can lead to serious consequences.

Technology will continue to play a critical role in meeting growing expectations for faster, more accessible services while ensuring continuity during unforeseen situations. Platforms such as INFOTECH FORUM provide valuable opportunities to learn from peers across industries, explore emerging technology solutions, understand evolving challenges and engage with technology partners, helping organisations make better-informed decisions as they advance their digital transformation initiatives.

Agentic AI will drive the next phase of enterprise productivity

Agentic AI is emerging as a significant opportunity for enterprises by improving productivity and reducing errors associated with manual processes. As organisations increasingly combine Generative AI with Agentic AI, they can automate routine tasks more effectively while enhancing operational efficiency and accuracy. However, AI cannot deliver its full potential in isolation. Its success depends on a strong foundation comprising cloud infrastructure, cybersecurity and automation, with each technology complementing the others. Together, these capabilities have the potential to significantly transform the way organisations operate over the next 12 to 18 months.

Technology alliances have become essential for accelerating enterprise transformation. No organisation can succeed in isolation, and collaboration must extend beyond technology companies to include academia, startups and the broader innovation ecosystem. Enterprises should increasingly focus on working together, sharing knowledge and co-creating solutions rather than relying solely on competition. Such partnerships help organisations access diverse expertise, encourage innovation and strengthen their ability to respond to changing business and technology requirements.

Platforms such as INFOTECH FORUM continue to evolve by reflecting the changing priorities of the technology industry. As discussions increasingly focus on areas such as cybersecurity, quantum computing, Generative AI and Agentic AI, these forums provide valuable opportunities for technology leaders to exchange ideas, understand emerging trends and learn from peers. By adapting to the evolving needs of CIOs and IT leaders, they help organisations prepare more effectively for the future.

VIJAY SETHI, CHAIRMAN & CHIEF MENTOR, MENTORKART

Technology teams will become more efficient with Agentic AI

Agentic AI represents the next stage in enterprise AI adoption by addressing more specialised technology and operational challenges. While Generative AI has become widely accessible across different user groups, Agentic AI offers greater value from a technical perspective by helping technology teams resolve issues more efficiently and reduce the time spent on routine problem-solving. When implemented effectively, it can improve productivity and enable IT professionals to focus on higher-value activities. As organisations continue to adopt AI, Agentic AI has the potential to simplify technology operations and make the work of technology teams more efficient.

Technology alliances are essential because no single organisation possesses expertise across every technology domain or can independently deliver every capability required by enterprises. Organisations can achieve better outcomes by bringing together partners with complementary strengths and leveraging their respective areas of expertise. Such collaboration enables businesses to deliver more comprehensive technology solutions while addressing evolving business and technology requirements more effectively. A strong partner ecosystem therefore remains an important enabler of enterprise transformation and innovation.

Platforms such as INFOTECH FORUM provide valuable opportunities to gain insights into emerging technology trends and industry developments. By bringing together technology leaders, government representatives and industry experts, these forums help participants better understand the evolving landscape and make more informed decisions. The exchange of knowledge and practical perspectives supports stronger technology strategies and continuous learning across the industry.

VIVEKANANDA NASKAR, DIRECTOR - IT, PROTEGRITY INDIA PVT. LTD.

AI and automation must be aligned with business growth

Artificial Intelligence and automation will continue to be important drivers of business value, provided their adoption is aligned with business objectives and practical use cases. Technology investments should always be guided by business requirements and measurable outcomes that contribute directly to business growth rather than technology alone. AI and Generative AI can help organisations make faster and better-informed decisions that support business growth. We have implemented AI-driven use cases, including real-time inventory management integrated with enterprise systems, which have delivered measurable business benefits. The success of any AI initiative ultimately depends on its ability to create tangible business value while delivering a clear return on investment.

Cybersecurity is another critical priority as organisations increasingly require real-time visibility across their operations. AI and Generative AI can support a more proactive approach to threat detection and strengthen security capabilities. Technology also enables faster and more effective business decision-making. Strong partner ecosystems are equally important because they help organisations build integrated platforms that improve collaboration, streamline operations and support business growth through connected enterprise systems.

Platforms such as INFOTECH FORUM provide valuable opportunities for CIOs and technology leaders to exchange practical experiences, discuss emerging use cases and explore new technologies showcased by OEM partners. Such interactions help organisations understand evolving technology trends, evaluate relevant solutions and make more informed decisions while planning future technology initiatives aligned with changing business requirements and industry needs.

YOGENDRA SINGH, CIO/ CTO/HEAD - IT/SAP, BARISTA COFFEE CO. LTD.

AI is an evolving journey for enterprise transformation

Artificial Intelligence, whether Generative AI or Agentic AI, is an evolving journey that is reshaping industries rather than a technology confined to any single domain. Organisations across sectors are exploring practical AI use cases that address their business and operational requirements. At the same time, the rapid pace of AI innovation makes the next 18 to 24 months particularly significant as enterprises evaluate how these technologies evolve and can be adopted responsibly. The long-term impact will depend on how organisations utilise AI effectively while adapting to an evolving technology landscape.

Cloud, cybersecurity and AI should not be viewed as competing priorities but as complementary capabilities that together support enterprise transformation. Cloud has become an essential requirement for modern organisations, cybersecurity remains integral to protecting digital infrastructure, and AI is increasingly enhancing technology platforms and business processes. As technology continues to evolve rapidly, enterprises should adopt an integrated approach that enables these capabilities to work together while remaining adaptable to changing business and technology requirements.

Technology alliances play a vital role in strengthening enterprise architectures by bringing together multiple technologies and areas of expertise. Rather than relying on a single technology provider, organisations benefit from complementary solutions that work together effectively. Platforms such as INFOTECH FORUM enable vendors, partners, consultants and customers to exchange knowledge, understand emerging trends and strengthen collaboration, helping organisations make better-informed technology decisions while strengthening the broader technology ecosystem.

GAURAV RANADE, CTO, TECHNOCENTRIC ADVISORY

Trust and governance are essential for responsible AI adoption

Enterprise-scale AI adoption should begin with a structured pilot phase that helps organisations understand both the capabilities and limitations of AI. Training employees is an important first step, alongside preparing AI models and establishing clear governance around how information is processed and used. As organisations move from pilot projects to production environments, transparency with customers becomes equally important. Clear contractual agreements, appropriate data handling practices and well-defined data retention policies help customers understand how their information will be used and managed. Such an approach enables organisations to scale AI responsibly while building trust and confidence across the enterprise.

AI and quantum computing are among the emerging technologies that have the potential to reshape enterprise innovation over the coming years. While AI continues to evolve rapidly, organisations should adopt it with a balanced perspective and realistic expectations. The combination of AI and quantum computing could unlock significant new possibilities, but its long-term impact will depend on how these technologies are managed, governed and integrated into enterprise environments.

Trust should remain at the centre of every AI initiative. Organisations need to maintain an appropriate balance between innovation, cybersecurity, infrastructure and responsible technology adoption while understanding both the opportunities and the potential risks associated with emerging technologies. Platforms such as INFOTECH FORUM provide valuable opportunities to exchange perspectives on AI governance, trust and emerging technologies, helping organisations foster responsible innovation and strengthen confidence in the adoption of emerging technologies.

NARESH GURU GM - IT SERVICE DELIVERY, IBM

Responsible AI adoption requires awareness, guardrails and governance

Enterprise AI adoption is progressing steadily, although many organisations are still moving cautiously from proof-of-concept initiatives to production-scale deployments. CIOs and CISOs are carefully evaluating how AI pilots can transition into enterprise environments while addressing emerging AI risks and establishing appropriate guardrails. Sandbox environments, risk awareness, evaluation of different AI platforms and rollback planning are important steps in helping organisations understand potential challenges before wider deployment. Building organisational awareness and preparedness will therefore remain essential as enterprises gradually scale AI adoption in a responsible and controlled manner.

Artificial Intelligence will continue to evolve, but its long-term success will depend on maintaining the right balance between AI, security and privacy. Organisations should adopt a holistic approach that also considers people, processes and financial priorities rather than focusing only on technology. A balanced framework enables enterprises to strengthen governance, manage evolving risks and create a stronger foundation for sustainable AI adoption.

Strong partner ecosystems have become increasingly important as organisations operate across interconnected digital environments. Enterprises should carefully evaluate technology partners, establish appropriate contractual safeguards and strengthen third-party risk management as supply chain risks continue to evolve. Choosing the right partners and understanding how closely technology ecosystems are connected are essential for building resilient digital operations. Platforms such as INFOTECH FORUM bring together relevant stakeholders to exchange perspectives on emerging technologies and support collaboration across the evolving technology ecosystem.

PANKAJ MITTAL, FOUNDER & CEO, DIGIZEN CONSULTING

The New Email Battlefield: How AI Is Rewriting Phishing, BEC and Enterprise Email Security

Microsoft's latest threat intelligence shows that email attacks are becoming smarter, more personalized and increasingly powered by artificial intelligence.

For nearly three decades, email has been the preferred gateway for cybercriminals. From the "ILOVEYOU" worm and Nigerian prince scams to ransomware-laden attachments and credential-stealing phishing campaigns, attackers have consistently exploited the one business application every employee uses every day.

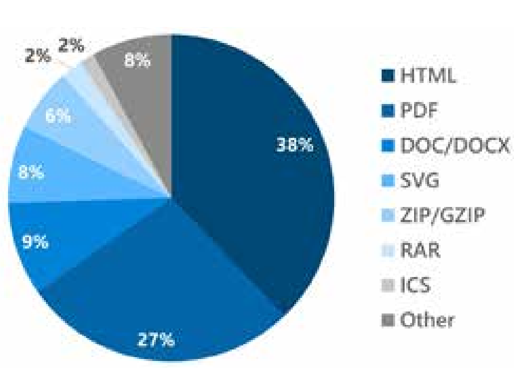
Yet despite billions of dollars invested in secure email gateways, spam filters, endpoint protection and employee awareness training, email continues to be the most effective route into enterprise networks.

The reason is simple: attackers have changed faster than enterprise defenses.

According to Microsoft's Email Threat Landscape Q2 2026 report, cybercriminals are no longer relying on poorly written phishing emails or malicious attachments to compromise organisations. Instead, they are combining artificial intelligence, legitimate cloud services, trusted identities and sophisticated social engineering to bypass traditional security controls. The inbox is no longer merely a place to deliver malware—it has become the starting point for attacks that target identities, cloud applications and business processes.

The report arrives at a time when enterprises worldwide are accelerating AI adoption while simultaneously facing an unprecedented rise in identity-based attacks. Security teams are discovering that technologies designed to stop yesterday's email threats often struggle against campaigns that use AI to mimic executives, hijack business conversations and exploit trusted cloud platforms.

For Indian enterprises, where hybrid work, cloud migration and digital transformation have become strategic priorities, the findings serve as another reminder that email security can no longer be viewed as a standalone technology. It has become a critical component of enterprise identity security.



PHISHING GROWS UP IN THE AGE OF AI

Phishing has long been considered cybersecurity's oldest trick. Traditionally, it relied on volume rather than sophistication—millions of generic emails promising lottery winnings, fake invoices or banking alerts, hoping that a small percentage of recipients would take the bait.

Artificial intelligence has dramatically changed that equation.

Microsoft's threat intelligence indicates that attackers are increasingly using AI to create convincing emails that mirror corporate writing styles, adopt flawless grammar and tailor messages for specific industries, regions and even individual employees. Instead of broadcasting identical messages to thousands of users, attackers can now generate highly personalised lures in seconds.

This has lowered both the cost and the skill required to launch sophisticated phishing campaigns.

Security researchers say AI-generated content is making it harder for employees to distinguish fraudulent messages from legitimate business communications. Emails impersonating senior executives, suppliers or customers no longer exhibit the grammatical mistakes and awkward phrasing that traditionally served as warning signs.

Attackers are also exploiting information available through company websites, professional networking platforms and social media to personalise their messages. A procurement manager may receive an email referencing an ongoing supplier contract, while an HR executive may be targeted with what appears to be a genuine recruitment inquiry. The objective is not simply to deceive users but to make malicious communications blend seamlessly into everyday business operations.

The evolution extends beyond email content. Microsoft observed phishing campaigns increasingly employing QR codes, CAPTCHA pages and multiple browser redirects before presenting victims with credential-harvesting websites. These techniques are specifically designed to evade automated email scanning systems that inspect links and attachments before messages reach employees.

In effect, attackers are exploiting the same cloud services and web technologies that enterprises rely on for everyday business.

BUSINESS EMAIL COMPROMISE ENTERS A NEW PHASE

Perhaps the most worrying trend highlighted by Microsoft's research is the continued evolution of Business Email Compromise (BEC)—a form of cybercrime that relies on deception rather than malware.

Unlike conventional phishing attacks, BEC campaigns often involve no malicious software whatsoever. Instead, attackers compromise or impersonate trusted business identities to manipulate employees into transferring funds, modifying payment instructions or disclosing sensitive corporate information.

According to the FBI, BEC remains among the costliest forms of cybercrime globally, accounting for billions of dollars in reported financial losses over the past decade. Microsoft's latest observations suggest that AI is making these attacks significantly more convincing.

Rather than sending a fraudulent invoice out of the blue, attackers increasingly spend weeks monitoring email conversations, studying communication styles and understanding business relationships before inserting themselves into legitimate discussions. AI enables them to imitate writing patterns, maintain natural conversations and respond intelligently to follow-up questions, reducing the chances that employees will suspect foul play.

This shift reflects a broader change in attacker priorities.

Instead of compromising thousands of users with commodity malware, criminal groups are increasingly focusing on high-value targets such as finance executives, procurement managers, payroll administrators and senior leadership teams. A single successful compromise of a corporate finance function can yield millions of dollars—far more than traditional mass phishing campaigns.

The challenge for defenders is that BEC attacks frequently bypass conventional security controls. Since the emails often originate from legitimate or compromised accounts and contain no malware, they appear perfectly normal to many security products.

As enterprises automate financial workflows and expand digital collaboration with suppliers and partners, the opportunities for attackers continue to multiply.

IDENTITY REPLACES MALWARE AS THE PRIMARY TARGET

For much of the last two decades, cybersecurity strategies centred on protecting endpoints against malicious software.

Today, attackers increasingly care less about infecting devices than about stealing identities.

This is perhaps the most significant trend emerging from Microsoft's latest threat intelligence.

Modern phishing campaigns are increasingly designed to harvest Microsoft 365 credentials, authentication tokens, browser session cookies and other forms of digital identity rather than simply delivering malware. Once attackers obtain legitimate credentials, they can often access cloud applications, email systems and collaboration platforms without triggering traditional security alarms.

This represents a fundamental shift in enterprise security.

Historically, an attacker needed to exploit vulnerabilities in operating systems or applications to gain access to corporate networks. Today, logging in with stolen credentials often achieves the same objective.

The consequences extend far beyond email.

A compromised Microsoft 365 account may provide access to Teams conversations, SharePoint repositories, OneDrive documents, calendars, customer records and confidential business correspondence. If the compromised account belongs to an administrator or executive, the impact can be considerably greater.

Microsoft notes that attackers are increasingly chaining together multiple techniques—credential theft, session hijacking, token abuse and cloud identity compromise—to establish persistent access without deploying traditional malware. Such attacks can remain undetected for extended periods because they closely resemble legitimate user activity.

This evolution explains why identity has become the new security perimeter.

Security technologies that focus exclusively on blocking malicious files or suspicious URLs are no longer sufficient. Organisations now require continuous identity monitoring, behavioural analytics and context-aware authentication capable of distinguishing legitimate users from compromised accounts.

The challenge is particularly acute for enterprises embracing hybrid work. Employees routinely access corporate applications from multiple devices, locations and networks, making it more difficult to determine whether unusual login activity represents legitimate business or an active cyberattack.

DEFENDING WITH AI: FIGHTING FIRE WITH FIRE

If artificial intelligence has become the cybercriminal's most powerful weapon, it is also emerging as one of the defender's most effective tools.

Security operations centres today process billions of events every day. Human analysts simply cannot investigate every suspicious login, email or endpoint alert manually. AI is increasingly helping bridge that gap.

Microsoft's security platforms now use AI to correlate seemingly unrelated signals—an unusual login, a suspicious email, an abnormal file download and a privilege escalation attempt—into a single incident that analysts can investigate. Other cybersecurity vendors are pursuing similar approaches, using AI to reduce alert fatigue and accelerate incident response.

The next frontier is autonomous security.

Rather than merely identifying suspicious behaviour, AI-powered security systems are beginning to take action automatically. They can isolate compromised accounts, revoke stolen session tokens, block risky logins, quarantine emails and initiate investigations before analysts even become aware of the incident.

This represents a significant shift in cybersecurity operations.

Just as attackers are using AI to automate reconnaissance and phishing campaigns, defenders are increasingly deploying AI to automate detection, triage and response. The contest is becoming less about who has more analysts and more about whose AI learns and adapts faster.

However, security experts caution that AI is not a silver bullet. Poorly configured AI systems can generate false positives, while sophisticated attackers continue to experiment with techniques designed to manipulate or evade AI-based detection. Human oversight remains essential, particularly for high-impact business decisions.

WHAT INDIAN ENTERPRISES MUST DO NOW

For Indian organisations, the implications extend beyond deploying another email security product.

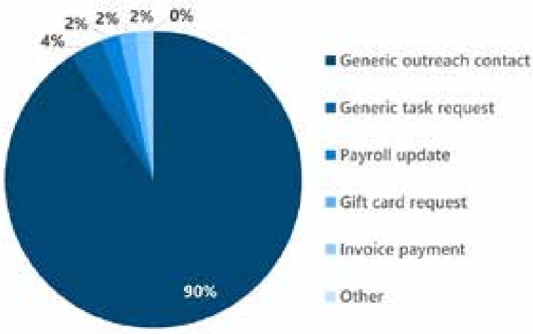
Digital transformation has dramatically expanded the enterprise attack surface. Cloud-first strategies, hybrid work, SaaS adoption and the widespread use of AI assistants have created new opportunities for attackers while simultaneously increasing the importance of identity security.

Sectors such as banking, financial services, manufacturing, healthcare, IT services and government are particularly exposed because they process large volumes of sensitive information and routinely interact with global partners.

The response, security leaders argue, should focus on strengthening identity rather than simply adding more layers of email filtering.

That starts with adopting phishing-resistant authentication methods such as passkeys and hardware security keys, replacing SMS-based authentication wherever possible. Multi-factor authentication remains essential, but organisations are increasingly recognising that not all forms of MFA provide the same level of protection against modern attacks.

Identity governance is another priority. Enterprises need tighter controls over privileged accounts, continuous monitoring for abnormal login behaviour and automated mechanisms to revoke access when risk levels change.



Employee awareness programmes also require an overhaul. Traditional training that teaches staff to spot poor spelling or suspicious attachments is no longer sufficient. Employees must learn to question unexpected payment requests, verify changes to supplier banking details through independent channels and recognise AI-generated impersonation attempts.

Equally important is strengthening resilience through regular incident response exercises. As BEC attacks become more sophisticated, organisations need clearly defined processes for verifying financial transactions, escalating suspected fraud and responding quickly when accounts are compromised.

Finally, email security should no longer be viewed as a standalone technology stack. It must be integrated with broader Zero Trust architectures, identity protection platforms and cloud security strategies.

THE FUTURE OF EMAIL ATTACKS

If today's phishing campaigns are powered by generative AI, tomorrow's attacks are likely to involve autonomous AI agents.

Security researchers increasingly envision AI systems capable of conducting extended social engineering campaigns across multiple communication channels. An attack may begin with a personalised email, continue through Microsoft Teams or WhatsApp, reinforce credibility with an AI-generated voice call and eventually persuade an employee to disclose confidential information or approve a fraudulent payment.

In such scenarios, email is no longer the attack. It is simply the opening move.

The convergence of AI, identity theft and cloud computing is reshaping enterprise cybersecurity in ways that extend far beyond the inbox. Every digital interaction—an email, a login, a document share or a chat message—could become part of a coordinated attack chain.

For security leaders, this demands a shift in mindset.

Success will no longer be measured by how much spam is blocked or how many malicious attachments are quarantined. Instead, it will depend on how effectively organisations can verify identity, detect abnormal behaviour and respond to attacks before trust is exploited.

(L-R): Mr. Pankaj Mittal, Founder & CEO- Digizen Consulting; Dr. Prince Joseph, Global CIO- SFO Technologies; Mr. V V Jacob, Chief General Manager-IT-Malayala Manorama Company Pvt Ltd; Lt. Col. (Dr.) Santosh Khadsare (Retd), CEO-I defence Innovations Pvt. Ltd.; Dr. Pavan Duggal, Chairman-International Commission On Cyber Security Law ; Dr. Arindam Sarkar, Chief Architect- FaceOff Technologies ; Mr. Nitin Mehta, Digital Risk Leader, EY India ;Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA; Mr. Savitur Prasad, Member- High Powered Enquiry Committee- Delhi Government ; Prof. N K Goyal, President- CMAI Association Of India ; Mr. Mylaraiah J N, V.P., Enterprise Business Unit - CommScope, India & SAARC ; Dr. Harsha Thennarasu, Founder & CISO-HKIT Security Solutions; Ms. Preeti Kela, Director- Net Protector Anti Virus; Ms. S Mohini Ratna, Editor- VARINDIA

The 24th edition of the VARINDIA Infotech Forum Leadership Summit 2025 concluded on a high note, reaffirming its position as one of India's leading platforms for thought leadership, innovation, and industry recognition across the ICT ecosystem. Organized by Kalinga Digital Media Private Limited, the summit brought together an eminent gathering of technology leaders, including CIOs, CTOs, CISOs, policymakers, industry veterans, marketing leaders, and senior executives representing the entire ICT value chain.

Held under the theme "Growth through Alliances in a Transformation Era," the summit explored the intersection of digital transformation, responsible technology adoption, and ethical innovation, highlighting their collective role in shaping a resilient and future-ready digital economy.

The day-long summit featured a thoughtfully curated agenda spanning morning, afternoon, and evening sessions. Attendees engaged in insightful keynote addresses, thought-provoking panel discussions, exclusive research report launches, prestigious award ceremonies recognizing the industry's most trusted companies and distinguished CIOs and finally culminating in the grand unveiling of the annual Brand Book coffee table publication.

The proceedings began with a ceremonial welcome, marked by the traditional lighting of the lamp, in the presence of dignitaries like Savitur Prasad, Member- High Powered Enquiry Committee- Delhi Government; Prof. N K Goyal, President- CMAI Association Of India; Nitin Mehta, Digital Risk Leader, EY India (Knowledge Partner); Dr. Pavan Duggal, Chairman- International Commission On Cyber Security Law; Dr. Arindam Sarkar, Chief Architect- FaceOff Technologies; Mr. Mylaraiah J N, V.P., Enterprise Business Unit - CommScope, India & SAARC; Lt. Col. (Dr.) Santosh Khadsare (Retd), CEO-I defence Innovations Pvt. Ltd.; Mr. V V Jacob, Chief General Manager-IT-Malayala Manorama Company Pvt Ltd; Dr. Harsha Thennarasu, Founder & CISO-HKIT Security Solutions; Pankaj Mittal, Founder & CEO- Digizen Consulting; Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA and S Mohini Ratna, Editor- VARINDIA.

The opening address was delivered by Dr. Deepak Kumar Sahu, Editor-in-Chief of VARINDIA, in which he highlighted the current position of where India stands today in terms of IT spending vis-à-vis the global scenario. "India's IT industry is a $250 billion global powerhouse — and yet our domestic IT spending is just one percent of global technology expenditure. For a nation of our scale and ambition, that is not a statistic. That is a wake-up call. Global compute spending stands at $250 billion a year — a $1 trillion opportunity over four years. If India moves decisively into this space, the dividends go well beyond technology. We are talking about transforming healthcare, education, agriculture, and climate resilience, all riding on the renewable energy infrastructure we are already building."

The welcome address was delivered by Savitur Prasad, Member- High Powered Enquiry Committee- Delhi Government, in which he emphasized upon governance, accountability, and institutional excellence.

Following this, Nitin Mehta, Digital Risk Leader, EY spoke on the current data trends in India and how this throws great opportunities for the private sector to work collectively with the government.

Dr. Pavan Duggal, Chairman- International Commission On Cyber Security Law outlined his deep insights into cyber law, cybersecurity, AI regulation, and the evolving legal landscape through a powerful presentation that gave the audience a valuable perspective on how to navigate the digital future responsibly.

The event progressed with a series of engaging corporate presentations, featuring insightful and thought-provoking sessions delivered by leading industry experts. Anuj Sharma, Presales Manager- Kaspersky shared his perspectives on today's evolving cyber threat landscape and the importance of proactive security, advanced threat protection, and cyber resilience.

Through his presentation, Dr. Arindam Sarkar, Chief Architect- FaceOff Technologies, while giving a glimpse of how FaceOff works, also focused on how identity intelligence, fraud prevention and digital trust converge in the synthetic intelligence era.

Ankur Patial, Sr. Solutions Architect- VARONIS enlightened the audience on AI ethics, and how it is the need of the hour to take a safe, secure, humane, and environmentally friendly approach to AI.

The morning session concluded with a vibrant panel discussion moderated by Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA. Titled 'From Digital India to AI India: The Next Leap', the esteemed CIOs who joined the discussion as panelists include - Vijay Sethi, Chairman-Mentorkart; Golok Kumar Simli, President - Technology & Innovation- BLS International; Sujoy Brahmachari, CIO & CISO- Rosmerta Technologies Ltd.; Bharat B Anand, Global CITO- Contec Global; Lt Col (Dr) Santosh Khadsare (Retd), CEO-I defence Innovations Pvt. Ltd.; Dr. Prince Joseph, Global CIO- SFO Technologies and V V Jacob, Chief General Manager-IT, Malayala Manorama Company Pvt Ltd.

AFTERNOON SESSION

The afternoon session started with felicitating the "Most Promising VARs in India", who have been recognized for their differentiation, excellence, and unwavering customer focus.

Jagbir Singh, Manager, Sales Engineering (Pre-Sales)- Check Point Software next came up on stage to share his perspectives on today's evolving cybersecurity landscape and best practices.

Sumeet Kela, Director at Net Protector AntiVirus through his presentation delved into the security offerings that his company offers, while also sharing his perspective on his research done in malware is helping drive innovations in endpoint security, ransomware prevention, and data protection.

Gaurav Saxena, Director – Channels & Alliances- VEEAM Software gave his presentation on The Convergence Era: Unified Platform; Winning with Alliances, in which he shared his insights on data protection, cyber resilience, and the importance of a strong partner ecosystem.

A panel discussion themed "Post Quantum Security: The Race Against Time" was moderated by Gyana Swain, Consulting, Editor, VARINDIA. The panelists who joined the session were Rohit Ponnapalli, CISO- Envoy Global; Dr. Rakshit Tandon, Founder- R T Cyber Academy; Sarita Padmini,Sr. DirectorProtiviti India; Jaspreet Singh, Partner and GCC Industry Leader- Grant Thornton Bharat; Dr. Harsha Thennarasu, Founder & CISO-HKIT Security Solutions and Garvit Sharma, CTO- Athenian Tech.

The third and the last panel discussion for the day was moderated by S Mohini Ratna, Editor-VARINDIA and the theme of the discussion was "Geopolitics Reshaping Marketing Budgets". The panelists for the discussion included Ankesh Kumar, Chief Marketing Officer- Ingram Micro India Pvt. Ltd.; Pranab Mohanty, Chief Business Officer- Data Safeguard Inc.; Dr. Mithilesh Singh, Marketing Head- Commscope India Pvt Ltd. Debraj Dam, Chief of VAD, Supertron VAD Venture and Sanjay Chaudhary, Head of Marketing Enterprise, SAP India.

VARINDIA then announced the Most Influential CMO's in India 2026-27 awards. The awards felicitated the marketing leaders and CMOs who are spearheading digital transformation, highlighting their efforts in redefining brand engagement and customer experience in the digital age.

This was followed by the felicitation of Eminent CIOs, CTOs, and CISOs from across industries for their role in driving enterprise transformation and digital excellence and guided their organisations through complexity and disruption.

EVENING SESSION

The evening session commenced with a welcome address by S. Mohini Ratna, Editor, VARINDIA, who summarized the key highlights of the day while reflecting on the central theme that shaped the summit's discussions and deliberations. "Every conversation today points to the same truth - closing the response gap is the defining cybersecurity challenge of our time. That is where the future of cybersecurity lives — intelligent systems are acting at machine speed, because that is the only speed that matters."

The evening session featured inspiring speeches and insightful presentations by distinguished industry leaders whose vision and expertise continue to shape the future of the industry. Among them are eminent policymakers and influential thought leaders who play a pivotal role in formulating policies and driving India's digital and technology agenda.

While Arun Kumar Sharma, Director- Cypress Solutions Pvt. Ltd. presented his ideas on Techfluential Edge and the Way Forward through an insightful presentation, Atul Kumar, Director-Global Trade, Cyber Diplomacy, Government Initiative- DSCI offered his perspectives on cyber diplomacy, global trade, and building trusted digital ecosystems.

Dr. Gulshan Rai, India's first National Cyber Security Coordinator, Government of India delivered the keynote address for the evening in which he shared his visionary perspectives on cybersecurity, digital resilience, and India's evolving cyber ecosystem.

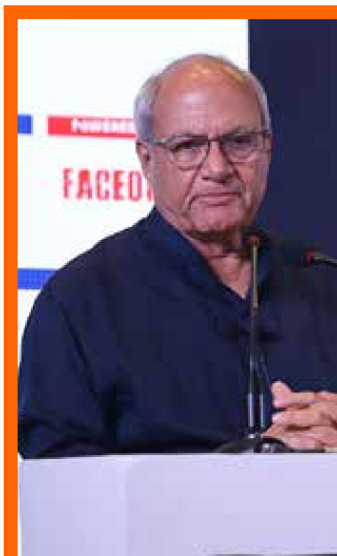
In his address to the audience, Dr. Amar Patnaik, Former Member of Parliament, Rajya Sabha, shared inspiring insights on data security, privacy, and the transformative potential of quantum innovation.

The next speaker was Prof. Charru Malhotra, Professor, Indian Institute of Public Administration (IIPA), who has made significant contributions to Digital India. She gave her presentation on Responsible AI, digital governance, cybersecurity, and data privacy.

KEY HIGHLIGHTS OF THE EVENT

- A significant highlight of the evening session was **the grand launch of the 15th edition of the Brand Book 2026.** As a trusted industry resource, the Brand Book offers in- depth white papers, CXO interviews, and expert analysis of evolving market dynamics.
- **Dr. Ajai Chowdhry, Co-Founder of HCL** was presented with the **Lifetime Achievement Award 2026** to, in recognition of his extraordinary vision, pioneering leadership, and an enduring legacy that shaped the Indian technology industry.
- The signing of an **MoU between FaceOff Technologies and NACOF (National Federation of Farmers Procurement, Processing and Retailing Cooperative of India Ltd.)** was yet another defining moment. Ram Iqbal Singh, Founder & Chairman, NACOF, Dr. Deepak Kumar Sahu, Founder & CEO, FaceOff Technologies, and Dr. Arindam Sarkar, Chief Architect, FaceOff Technologies participated in the signing ceremony.
- VARINDIA also took the opportunity to recognize the **Most Promising VARs in India, Eminent CIOs of India, Most Influential CMOs in India 2026-27, Most Promising VARs in India25, Most Trusted Companies** followed by **50 Most Admired Brands** of India's ICT ecosystem. These organizations were selected through rigorous evaluation of brand performance, market reputation, and customer trust.

INFOTECH FO
FORGING A
FUELING



SUPPORTING PARTNER
nixi
Empowering Netizens

PLATINUM PARTNER
Inflow
Information Integrity
Cypress Solutions

PRINCIPAL PARTNER
VARONIS

POWERED BY
FACEOFF
OPINION MATTERS

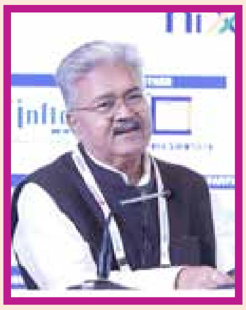
GOLD PARTNERS
kaspersky
veeam

ORUM 2026: ALLIANCES, GROWTH

HECK POINT

CYBER SECURITY PARTNER	NETWORKING PARTNERS	PASSWORD LESS SECURITY PARTNER	DATA PRIVACY PARTNER
Net Protector NPAV Cyber Security	COMMSCOPE an Amphenol company; DELL Technologies	yubico	datasafeguard

Rethinking Imperialism in a Technology-Driven Era: The rise of Digital Dependence



SAVITUR PRASAD, MEMBER- HIGH POWERED ENQUIRY COMMITTEE- DELHI GOVERNMENT

The future is increasingly uncertain, making it difficult to predict what the next few years may hold. I would like to take you back to the history - we all have read Karl Marx, and he had predicted long back third world imperialism. This concept offers an interesting lens through which to view today's global landscape. Rather than territorial occupation, as witnessed in the colonial era, the argument is that influence is now exercised through the global reach of corporations headquartered in economically advanced nations. In expanding their markets, these enterprises can create new forms of economic and technological dependence. Marx had rightfully argued that as capitalism will expand, it will inherently create a global system of exploitation where core industrial nations will extract surplus and resources from the less developed, colonized, or "Third World" peripheries.

In today's time, this holds true for technologically less developed countries that are completely dependent on countries both economically and technologically strong. Talking about India, our contribution in technology is still comparatively less. While the country has made significant strides in technology, there remains considerable scope to strengthen its indigenous innovation and technological leadership to reduce dependence and enhance global competitiveness. The country continues to rely heavily on imports and foreign technology in several strategic domains, including semiconductor manufacturing, advanced chip design, high-performance computing, specialized electronics, and certain cybersecurity and AI platforms. Reducing this dependence requires sustained investment in research and development, stronger collaboration between academia, industry, and government, and the creation of a robust ecosystem that nurtures deep-tech startups and product innovation.

As Deepfakes grow more convincing, Quantum Security becomes a Strategic Priority

PROF. CHARRU MALHOTRA, PROFESSOR, INDIAN INSTITUTE OF PUBLIC ADMINISTRATION (IIPA)

Thanks to the Government of India's vision through Digital India, the country is well prepared through IndiaAI Mission, National Supercomputing Mission, and India Semiconductor Mission.

AI has transformed organizational spaces and citizen expectations, but trust remains the biggest challenge in the digital domain. Synthetic media can support entertainment, education, capacity building, library sciences, information sharing, or student empowerment. However, when combined with mal-intention and wrong information, it can create deepfakes capable of damaging the sanity of a country through social media.

Deepfakes create two major problems. One is fabricated content designed to spread misinformation to spoil community harmony. The other is the liar's dividend, where politicians or celebrities make a statement and, after the damage is done, disown it by claiming it was a deepfake. Synthetic media itself is not harmful if handled responsibly. This is where responsible AI becomes essential. Citizens who actively use UMANG, DigiYatra, DigiLocker, UPI, and other digital initiatives increasingly question the authenticity of online content.

Quantum computing adds another dimension. It is not to be dreaded but prepared for because it can process multiple possibilities far faster than traditional systems and may challenge current verification and encryption mechanisms. India launched the National Quantum Mission in April 2023 with an approved outlay of Rs. 6,365 crore, aiming to develop quantum computers, secure quantum communication networks, advance quantum sensing technologies, build indigenous quantum systems, strengthen India's global competitiveness in quantum technologies, and enhance telecom security. India must prepare for post-quantum cryptography (PQC), as it is a strategic necessity.

Harnessing AI effectively requires a calibrated approach balancing Innovation, Responsibility, and Impact

DR. PAVAN DUGGAL, CHAIRMAN- INTERNATIONAL COMMISSION ON CYBER SECURITY LAW

Today we are all into AI. When we talk of this growth through alliances in a transformative era, you have to start realizing that your approaches to growth will have to be substantially different. Because somewhere down the line AI will be an integral part of this.

So, when we start using AI for growth, for transformation, for alliances, we have to keep in mind certain broad things that are not yet existing on the ground. First, the technology is moving far, far more rapidly than law. Second, India doesn't have a dedicated law on artificial intelligence yet. But that's not new. India didn't even have a dedicated law on cyber security. The only law that India has in place is the Indian Information Technology Act 2000 which is a 26-year-old legislation. The IT Act 2000 happened when wanted to focus on coming up with a new legal framework for electronic governance, and we came up with this law. The law was one of the best in the world. India was the 12th nation in the world to have enacted a cyber-law. We based ourselves substantially on the UNCITRAL model law on electronic commerce. But those were the.com boom days, and things have now changed completely. I reiterate that what you were thinking of, or what you were doing in 2021 is absolutely obsolete today. Whether we realize it or not, while we were sleepwalking, we rode a new 'Tiger' and that 'Tiger' is AI. The tiger has started running very, very fast, and we are just about beginning to wake up from our slumber.

Future of Trust depends on Strong Data, Governance and Quantum Preparedness

DR. AMAR PATNAIK, FORMER MEMBER OF PARLIAMENT, RAJYA SABHA

Data security has been fundamental to technology since digital systems first emerged. However, it is important to distinguish between data security and data privacy. Data security protects all forms of data, while data Privacy applies only to personal data.

Data security acts as the outer protective wall or vault of an organization's digital assets. Effective security requires strong IT controls, continuous monitoring, and regular audits. Data privacy applies only to personal data, which includes permissions, consent, and purpose.

India has a well-established data privacy regime. Protecting personal data is important because the penalties are significant under the new data law. This ensures trust in the future of systems.

Privacy is part of Article 21 of the Constitution, the Right to Life. Auditability, traceability, and reasonable restrictions are all part of our fundamental rights. Regardless of how advanced a technology solution you have developed, you must adhere to this.

The future of trust depends on preparedness to handle the advent of quantum computing, which will challenge the encryption architecture built to safeguard data, business, goals, and trust. If you want to retain trust in your product, technology, or offering, you must be prepared to face this onslaught.

The future of trust will depend on strengthening data security and privacy policies. Whether it is quantum computing or not, the principles of privacy remain the same because they are part of our Constitution.

AI and Quantum are expanding India’s Digital Opportunity

DR. GULSHAN RAI, INDIA'S FIRST NATIONAL CYBER SECURITY COORDINATOR, GOVERNMENT OF INDIA

Today’s era is totally different from earlier. Digitization is scaling up. Every sector is digitization, implementing applications and different kinds of technologies in place. We are observing transformation in digital technology, not digital transformation.

AI has become the underlying fabric of every technology. Every technology implemented for any application has a layer, whether it is AI or quantum computing. We are creating and implementing very complex technology with multiple interfaces and layers together. Hence, the threat surface has increased. Handling these areas requires a 360-degree approach with four pillars - governance, technology, crime, and diplomacy. Governance includes regulations, legislation, and legal frameworks. Technology focuses on secure implementation. Crime covers the evolving spectrum of cyber threats, while diplomacy has become increasingly important as geopolitics now plays a critical role in cybersecurity.

AI operates across four layers: hardware infrastructure, AI models and tools, data, and applications. Building a trustworthy AI ecosystem requires expertise, collaboration, and ethical standards across all these layers. No single country is self-sufficient across the entire AI stack.

The same challenge exists with quantum computing. Legacy and modern systems will coexist. That is why RSA algorithms can be easily broken today. The ultimate result is the demand for equipment and manpower that can configure these systems will rise. AI, post-quantum, and other new technologies will soon reach MSMEs and SMEs. This will create manpower requirements and increase overall market strength. The future is bright, but it depends on how we prepare ourselves.

As Tech Geopolitics reshapes the world, India eyes a bigger Strategic Role

ATUL KUMAR, DIRECTOR-GLOBAL TRADE, CYBER DIPLOMACY, GOVERNMENT INITIATIVE- DSCI

Geopolitics is changing the whole paradigm of technology. In the last few months, sovereignty has become a central theme, driven by wars, export controls, sanctions, and restrictions on frontier technologies. AI model access, rollout delays, acquisitions, and government interventions highlight that technology usage is increasingly influenced by state-level decisions. The global conversation has shifted toward AI geopolitics, sovereign AI, sovereign compute, and control over frontier technologies. Massive capital investments in AI, rapid advancements in physical AI and device-level AI, and tighter government oversight are creating a complex technology landscape, and India must determine how to maintain its strategic edge.

The global technology order is being rewired. Supply chains are moving from cost optimization to trusted ecosystems. Internet governance has expanded into AI, cloud, telecom, and data governance, while cybersecurity has evolved from compliance to real-time resilience. The strategic drivers behind this shift include AI chips, semiconductors, quantum computing, cyber tools, regulatory frameworks such as the EU AI Act, and global technology standards.

Technology has also become the new geopolitical choke point. Critical minerals, semiconductors, GPUs, cloud infrastructure, firmware, and Electronic Design Automation (EDA) tools now shape national competitiveness, making supply chain diversification and trusted partnerships essential. India has already established global leadership through Digital Public Infrastructure and digital payments. The next phase is building resilience across critical infrastructure, trusted technology ecosystems, startup innovation, regulatory participation, and international collaboration, to strengthen Brand India as a trusted technology and cybersecurity leader.

India following the right AI path with indigenous LLMs and SLMs

DR. AJAI CHOWDHRY
CO-FOUNDER
HCL

Everyone says that India is doing nothing in AI. This is a typical narrative, but it is absolutely incorrect because what we need to see is what our requirement is in this country. Is a Large Language Model (LLM) a requirement for this country or not?

All the LLM companies were present during the AI Summit and wanted to be part of what India is doing. Why did they come here? They came because India is a very big market and their LLMs are doing so well in this country, consumers are lapping them up. But the real impact of LLMs will be in other areas. If we look at the enterprise or SME market, when you start to use LLMs, you will realize how expensive they are.

India has taken the right route. India has realised that we must have our own LLMs. Sarvam and few other companies have come up, and a range of voice-based LLMs has emerged. Therefore, we are going to be self-sufficient in LLMs if we truly believe in our own products.

The real application of AI will come through Small Language Models (SLMs). SLMs will be developed for different areas like agriculture, education, climate, and more, and these are going to be made in India.

The good news is that a research institute was set up just four months ago at GIFT City in Gujarat, where we have brought some Indians back from the US to get it started. The whole idea is that if we look at our capability in AI, it is at the lower end. At the higher end, we do not have the experience today. So, to gain that experience, it is absolutely essential that we bring some of our diaspora back. The whole strategy was that the AI Mission, the Gujarat government, and the Pharma Association got together and invested ₹300 crore budget through which this AI research institute could be established. The whole objective of this AI research institute is to create SLMs for India so that we can actually solve India's problems.

SLMs will be very critical, and one of the first SLMs being introduced is the industrial AI SLM, which will be used by factories to reduce downtime. These are the kinds of applications where this research institute will work, create products, and collaborate with start-ups to take them to market.

So, do not think that India is doing nothing in AI. We have already created great LLMs, we have also created many voice-based LLMs, and now we are working on SLMs.

Foresight, Resilience, and Proactive Risk: The keys to navigating the Digital Future

NITIN MEHTA
DIGITAL RISK LEADER, EY

Navigating the digital landscape requires foresight, resilience and a proactive approach to risk. Only then can we unlock the true potential of technology. I was reading a research report, and it said that 20% of data globally is generated in India, but only 3% of that data is hosted in India. So, India is the data source, but it is not the data infrastructure for the world. If you look at AI in India, the problem is, we are still adapters, we are not creators. If you look at industrial revolutions, right from steam engine through electricity, and then ERPs and the technology beyond, India is known to have jumped revolutions. We never went into mainframes, we directly jumped into mini computers and then into client server technology. But we always had time in all the previous industrial revolutions.

In the era of the Fourth Industrial Revolution and the rapid rise of AI, India no longer has the luxury of time to adapt at a gradual pace. Unlike previous technology shifts, the current AI-driven industrial revolution leaves little time for Indian organizations to adapt before the next disruption arrives. I won't say that India is lagging behind the world, simply because we don't have our sovereign elements yet. We continue to depend on technology superpowers such as the United States, where access to some of the most advanced AI models—including those developed by companies such as Anthropic and others—is subject to restrictions, limiting their availability outside the country. So we have a dependency on them, but I believe it's not about where we are lagging behind, but it's about the potential and the opportunity that all of us together have. I think there is a phenomenal opportunity for the private sector to work with the government and have a strong public private collaboration to build on this.

All the current emerging trends that we hear today – semiconductor, AI, advanced analytics, data center & cloud infrastructure, cyber security, quantum computing. - all these elements are not really separate, isolated, segregated, different trends, but this is one full stack that forms a part of interdependent layers. This is how I look at it. If we start at the fundamental foundation of this four-layered structure, there is the compute. We all understand the government is pushing to promote and incentivize the semiconductor industry or the data centers, and unless we have that foundation, none of the other three layers will work. The second layer built is around cybersecurity, which serves as the foundation for protecting every other layer of the technology stack. The third layer focuses on intelligence, encompassing automation, advanced analytics, and AI-driven capabilities. The fourth and final layer is trust—the cornerstone that enables secure, reliable, and responsible digital transformation.

Cypress Solutions & Inflow simplify enterprise infrastructure with single-window support

When Inflow Technologies and Cypress Solutions joined hands, we started analyzing how a data center is designed and built. While setting up a data center, the customer begins with a business plan, defining what the data center is meant to support. As both management teams discussed how to create value and build a strong ecosystem for customers, we mapped the complete journey of building a DC.

The first step is the customer's business plan. It is supported by applications, which define the number of users, transactions per day, hour, and minute, along with compute, storage, and bandwidth requirements. These requirements are converted into a hardware plan, determining the number of servers, storage systems, and other infrastructure required year by year.

Once the hardware plan is ready, it is integrated into a network with the required security. These systems need conditioned power to ensure 24x7 availability. Since powered equipment generates heat, the conditioned power plan naturally leads to the cooling plan. Together, these components create a perfectly synchronized and customized solution, where the business plan is systematically converted into infrastructure requirements.

The cooling systems, conditioned power, and utility spaces determine the total raw power requirement, which is backed by alternate sources. Every component also has a physical footprint, enabling accurate planning for racks, UPS systems, cooling equipment, substations, and the overall building space. The result is a complete building plan derived directly from the business plan. During execution, the process works in reverse, first the building, then power, cooling, network, hardware, and finally the applications that run the business.

While analyzing this process, we also identified the specialized expertise customers require, including architects, structural engineers, IGBC-certified professionals, etc. We also recognized the need for data center-specific certifications covering design, construction, operations, and ratings. Additional certifications apply to network, security, hardware, and business governance, including relevant ISO standards. Inflow already delivers the complete infrastructure with a strong OEM ecosystem and extensive execution capabilities. Together with Cypress Solutions, we realized we could offer customers a true single-window solution. With this alliance, every aspect of the data center lifecycle, from planning and design to execution, certification, and operations, is delivered seamlessly, leaving no component for the customer to worry about. That is the value we have created for our customers.

ARUN KUMAR SHARMA
DIRECTOR, CYPRESS SOLUTIONS PVT. LTD.

Embracing Synthetic Intelligence through integrated audio, video, and text modalities

Talking about Anthropic Claude, it has managed to write 80% of the codes. We are expecting Anthropic Claude to write 100% of these codes. We are also expecting whatever codes are written by Claude, it should check and verify by Claude itself. And then we are asking: what about Mythos and the Fable 5? Whenever we are training our data and our model, this data is actually the fuel. Whenever we have a data crunch, we readily generate it, which we call it synthetic data. So, whenever we are training our data, we are using synthetic intelligence, and we are generating synthetic identity or Frankenstein Identity. We are talking about machine learning that is just a statistical representation. We are talking about predictive intelligence - your algorithm should be such that it can give you predictive intelligence, or in other words prediction. But the challenge is that deep learning is a complete black box.

The five capabilities that ordinary AI does not have are: multimodal fusion, agentic reasoning, neuro-symbolic explainability and privacy-native cognition. When we watch any video, your AI should be able to tell you everything about the audio, video, lip sync, the text, and so on and that is multimodal fusion. Synthetic intelligence is the future, where we use every modality: audio, video, lip sync, and the speech. FaceOff Technologies is a deep-tech company pioneering the future of digital trust through AI-powered multimodal verification. Another aspect at FaceOff is data privacy. When we say that our AI is trained with our data, we are talking about data privacy, data encryption algorithms, and securing our data using post quantum cryptography. It deploys a "Neuro-Quantum Safe" architecture that integrates AI-powered identity verification with Post-Quantum Cryptography (PQC).

Whenever you train your machine learning algorithm how do you feed your data? Is your data encrypted or is it plain data? How can you guarantee that the data privacy model you are using is not actually leaking your data? Will you be able to erase data from your AI model that has already been trained on that data?

So AI is right now in a situation where we have to think it as a complete engine, and this is what we are doing at FaceOff. Powered by its proprietary Adaptive Cognito Engine (ACE), Faceoff goes beyond traditional biometrics by combining behavioral intelligence, visual signals, voice sentiment, and contextual analysis to generate real-time Trust Scores from video interactions. a proprietary multimodal AI. It is a deep-tech architecture developed to combat deepfakes, synthetic identity fraud, and AI impersonation. Rather than acting as a single AI chatbot, it acts as a dynamic security framework combining visual, audio, behavioral, and contextual analysis to establish human authenticity in real time.

DR. ARINDAM SARKAR
CHIEF ARCHITECT- FACEOFF TECHNOLOGIES

AI transforming the very foundations of research, knowledge creation, and professional excellence

DR. DEEPAK KUMAR SAHU
PUBLISHER & EDITOR-IN-CHIEF
VARINDIA

India's IT industry is a $250 billion global powerhouse and yet our domestic IT spending is just one percent of global technology expenditure. For a nation of our scale and ambition, that is not a statistic. That is a wake-up call. Global compute spending stands at $250 billion a year — a $1 trillion opportunity over four years. If India moves decisively into this space, the dividends go well beyond technology. We are talking about transforming healthcare, education, agriculture, and climate resilience, all riding on the renewable energy infrastructure we are already building. The opportunity is here. The question is whether we are ready to claim it. We live in a moment that history will remember. Not because of a single invention, not because of one breakthrough — but because of something far more profound: the quiet, relentless, and accelerating transformation of how human beings think, discover, and create. Artificial Intelligence is no longer a promise on the horizon. It is here. It is now. And it is reshaping everything we thought we knew about research, knowledge, and professional excellence. The world you trained for five years ago is not the world you work in today. The tools have changed. The pace has changed. And the expectations — of institutions, of employers, of the public — have changed dramatically. We are living through what many are calling the Fourth Industrial Revolution. But unlike those that came before it — this one is driven by intelligence itself. Machine intelligence, Adaptive intelligence, Intelligence that learns, evolves, and, increasingly, surprises even its own creators.

Data analytics is unlocking patterns in human behaviour, climate, disease, and economics that no human mind could process alone. Digital verification tools are redefining what it means to establish truth in an era flooded with information. And AI — the engine powering all of this — is breaking boundaries that once seemed permanent.

Artificial Intelligence is not merely a tool. It is a paradigm shift. It is reading medical scans with greater accuracy than specialist physicians. It is predicting crop failures before they happen. It is translating languages in real time, writing code, generating research hypotheses, and analyzing decades of academic literature in minutes. For researchers and academics, this is not a threat — it is an invitation. An invitation to go further, ask bigger questions, and produce work of greater depth and rigour than any previous generation could achieve.

But with that invitation comes responsibility. Because AI is only as powerful as the judgement of the person wielding it. And in a world where AI can generate convincing content at extraordinary speed, the ability to verify, validate, and exercise critical thinking is not diminishing in importance — it is becoming the most essential skill of our time.

UNVEILING OF THE 15TH BRAND BOOK 2026

The Brand Book brought out annually by VARINDIA is dedicated to helping brands carve out a distinctive identity and position themselves effectively in today's crowded, tech-driven landscape. The 15th edition of the BRAND BOOK, inaugurated at the Infotech Forum offers an in-depth overview of the Indian tech industry, covering the latest trends, innovations, and key players.

Ms. S Mohini Ratna, Editor- VARINDIA; Mr.Sarthak Bhuiyan, MD- Quantum Technology Systems; Ms. Sarita Padmini, Director-Protiviti India; Mr. Jagannath Pattnaik, CEO- NNR IT Solutions ; Mr. Nitin Mehta, Digital Risk Leader- EY India ; Mr. Kamal Matta, CIO, CISO-Sonic Biochem Extractions ; Ms. Rini Agarwal, CEO & Founder- Kaizen Nextgen;Mr. Atul Kumar, Director-Global Trade, Cyber Diplomacy, Government Initiative- DSCI;Dr. Amar Patnaik, Member of Parliament -Rajya Sabha; Mr. Ramiqbal Singh, Founder& Chairman-NACOF; Mr.Manish Shrivastava, G.M- NACOF; Mr. Mylaraiah J N, V.P., Enterprise Business Unit - CommScope, India & SAARC; Dr. Mithilesh Singh, Marketing Head-Commscope India Pvt Ltd.; Mr. Golok Kumar Simli, President - Technology & innovation bls international; Mr. Arun Kumar Sharma, Director - Cypress Solutions Pvt. Ltd.; Mr. Pranob Mohanty, Chief Business Officer- Data Safeguard Inc.; Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA; Mr. Subir Mahapatra, President(Global Sales)- Denave

This essential resource is the go-to guide for anyone seeking insights into the dynamic Indian tech landscape. We believe brands thrive by understanding and connecting with people on a deeper level, recognizing their needs, desires, and aspirations. Personalization is key; without it, a brand loses its purpose. This philosophy is embodied in the annual unveiling of the Brand Book at the 24th Infotech Forum, celebrating innovation and customer-centricity.

The Brand Book remains the ultimate platform for corporates to showcase their innovation & offerings, standing out as a powerful media vehicle. With a focus on people, it reflects a unique identity through careful design and impactful messaging, embodying connection and trust.

Cybersecurity, AI integration & data analytics are today's reality of every technology leader

S MOHINI RATNA, EDITOR- VARINDIA

For over 27 years, VARINDIA and the Brand Book — the flagship publications of Kalinga Digital Media — have been a constant presence in India's ICT industry. Not just as publications, but as trusted partners to every segment of this ecosystem. VARINDIA has earned its place as the number one source for technology news and insight in this country — not by chance, but through an unwavering commitment to quality, credibility, and genuine industry relevance.

The Brand Book is something special in its own right. Each edition captures the leadership, vision, and strategic journeys of India's most influential technology brands — the companies and the people who have quietly, and sometimes not so quietly, shaped the nation's IT story. Our survey of India's Eminent CIOs tells a clear story - priorities have fundamentally shifted. Cybersecurity, AI integration, data analytics, and talent management are no longer items on a future agenda — they are the day-to-day reality of every technology leader. On security, Zero Trust is the new baseline. Leaders are moving fast on compliance, and investing in proactive threat intelligence — including dark web monitoring — to get ahead of threats before they land. On AI, the debate has moved on. It is no longer about whether to adopt — it is about adopting responsibly, with real ROI discipline and automation that actually simplifies rather than complicates. Every conversation today points to the same truth - closing the response gap is the defining cybersecurity challenge of our time. That is where the future of cybersecurity lives — intelligent systems are acting at machine speed, because that is the only speed that matters.

CORPORATE PRESENTATION

Secure enterprise data before accelerating AI adoption

ANKUR PATIAL, SR. SOLUTIONS ARCHITECT, VARONIS

Despite significant investments in cybersecurity technologies over the years, data breaches continue because attackers have shifted their focus from breaking into systems to exploiting legitimate identities. Once credentials are compromised, attackers can often access sensitive enterprise data without triggering traditional security controls. At the same time, the growing use of cloud collaboration platforms has expanded the 'blast radius', making it essential for organisations to understand where their sensitive data resides, who has access to it and whether those permissions are still appropriate.

The rapid adoption of AI has further increased the importance of data security. AI systems inherit user permissions and can surface information across multiple repositories much faster than humans, which makes strong data governance a prerequisite for responsible AI adoption. Many organisations remain cautious about deploying enterprise AI because of concerns around overexposed data, shadow AI, limited visibility and the shortage of specialised security skills required to manage these environments effectively.

At Varonis, we believe organisations should secure their data before accelerating AI adoption. Our focus is on helping customers gain visibility into their data, identify excessive access, automate remediation and detect abnormal user behaviour through behavioural analytics. By combining data-centric security with AI visibility, automated remediation, guardrails and governance, organisations can reduce risk and confidently accelerate AI adoption, recognising that successful AI deployment begins with securing the underlying enterprise data.

Meaningful AI outcomes depend on trusted, well-governed data

GAURAV SAXENA, DIRECTOR - CHANNELS & ALLIANCES, VEEAM SOFTWARE

Digital transformation has significantly expanded the enterprise data landscape, with organisations today managing workloads across physical, virtual, cloud, SaaS, containerised and AI environments. At the same time, ransomware, AI-enabled threats and evolving regulatory requirements have made data resilience a strategic business priority rather than just an IT function. In this rapidly changing environment, a strong partner ecosystem plays a vital role in helping organisations adopt technologies at scale, strengthen cyber resilience and deliver uninterrupted business outcomes.

At Veeam, we have evolved from being a backup and recovery company to enabling cyber resilience and, now, AI resilience. As enterprises accelerate AI adoption, the focus is shifting beyond protecting data to ensuring that the data powering AI models is secure, governed and trusted. Meaningful AI outcomes depend on trusted, well-governed data, making visibility into enterprise data, governance, compliance and the right trust layer between data and AI applications increasingly important for secure and trusted AI adoption.

Our focus is to help customers protect, recover and govern their data through an integrated platform that combines data protection, security, governance and resilience across diverse workloads. By providing greater visibility into the complete data lifecycle and helping organisations understand how data is created, accessed and protected, we aim to strengthen cyber resilience, support business continuity and enable customers to embrace AI-driven innovation with confidence while maintaining trust in their enterprise data.

AI demands a prevention-first approach to cybersecurity

JAGBIR SINGH, MANAGER, SALES ENGINEERING (PRE-SALES), CHECK POINT SOFTWARE

Cybersecurity has become significantly more complex as organisations operate across hybrid environments spanning data centres, cloud, edge, remote workforces and AI-powered applications. At the same time, AI is transforming both enterprise operations and the threat landscape. While organisations are using AI to improve productivity and automation, threat actors are also leveraging it to accelerate attacks, reducing the response window and making traditional security approaches less effective. This makes it essential for organisations to continuously reassess their security posture and adopt a prevention-first approach to address evolving cyber risks.

At Check Point, our focus is on securing the entire enterprise rather than addressing isolated security challenges. As organisations deploy multiple security solutions, operational complexity can increase and visibility may become fragmented. We believe security should be integrated across networks, cloud, endpoints, workspaces, exposure management and AI-powered environments, enabling customers to simplify operations while strengthening prevention and resilience. As AI adoption accelerates, organisations must also secure AI usage, AI agents, AI applications and the underlying data that powers them, ensuring innovation is accompanied by governance, resilience and trust. Our approach combines AI-driven threat prevention, exposure management and comprehensive security services to help organisations strengthen cyber resilience across diverse environments. By embedding AI into security while continuing to prioritise prevention, visibility and operational simplicity, we aim to help customers protect critical assets, securely embrace AI-driven transformation and remain prepared for emerging threats in an increasingly dynamic digital landscape.

Leveraging intelligence-led cyber defense

ANUJ SHARMA, PRESALES MANAGER- KASPERSKY

If we see over 10-15-year period, most of the organizations and enterprises have adopted best of the breed security solutions comprising of the best firewalls and VPNs. At the same time, certain companies that have come up with services like darker services, credential surveillance, brand monitoring, and so on. Now, despite having best for the breed security and spending crores of money on security, why are there still breaches and leakages. There appears to be a gap somewhere and we need to understand that even if those security solutions are competent enough, there will be some human factors and misconfigurations because of why these breaches are still happening.

In order to bridge that gap on a real-time basis, we have to move forward with AI-based threat intelligence. So at Kaspersky, we have AI security; we have multiple sources from where we enrich our threat intelligence that includes bot farms, spam traps, and sensors. We have billions of sensors for the users which are providing real-time intelligence to us on a nearly real-time basis. We do have a dedicated research team – GreAT (Global Research and Analysis Team). The moment we receive the data, it goes to the team, they churn out the data, and then forward it to respective threat intelligence products.

We also have multi-layered AI-based threat detection combines machine learning (ML), behavioral Endpoint Detection and Response (EDR), and global threat intelligence to proactively block ransomware, zero-day exploits, and Advanced Persistent Threats (APTs). In other words, Kaspersky has been using AI and ML technologies from past 30 years. We have a legacy of databases, which we are trying to consolidate into our threat intelligence.

Identity security requires phishing-resistant authentication

RAHUL DANI, PRESALES ENGINEER, YUBICO

As organisations continue to accelerate digital transformation, identity has become one of the most critical aspects of cybersecurity. Attackers are increasingly relying on phishing and credential theft rather than exploiting technical vulnerabilities, making traditional password-based authentication progressively less effective. Even conventional multi-factor authentication methods, including SMS-based codes, one-time passwords and push notifications, can be vulnerable to sophisticated phishing attacks when users unknowingly authenticate malicious sessions. This highlights the need for authentication approaches that reduce dependence on passwords while strengthening protection against evolving identity-based threats.

At Yubico, our mission is to help make the internet safer by enabling phishing-resistant authentication. Through the FIDO standards, advanced in collaboration with the broader industry, and YubiKey hardware security keys, we enable phishing-resistant authentication based on public key cryptography rather than shared secrets. By securely storing private keys on dedicated hardware, binding credentials to legitimate domains, and requiring user verification and physical presence, this approach helps reduce common credential theft risks while improving trust in the authentication process.

As organisations continue expanding cloud adoption and digital services, strengthening identity security has become a critical element of cyber resilience. Our focus is on helping customers adopt passwordless, phishing-resistant authentication that combines strong security with a seamless user experience. By reducing reliance on passwords and strengthening identity protection, organisations can better secure users, applications and digital assets against an increasingly sophisticated threat landscape.

Building enterprise cyber resilience through Made-in-India innovation

SUMEET KELA, DIRECTOR, NET PROTECTOR ANTIVIRUS

As organisations continue to strengthen their cybersecurity posture, identity protection, data security and controlled access have become increasingly important. Password-based authentication alone is no longer sufficient, while AI adoption and expanding digital ecosystems have introduced new challenges around data leakage, insider risks and regulatory compliance. At Net Protector AntiVirus, our focus is on delivering comprehensive cybersecurity solutions that help organisations strengthen resilience across endpoints, networks, users and critical business applications. With over three decades of cybersecurity experience and a 100% Make in India approach, we continue to develop technologies that address evolving enterprise security requirements.

Our portfolio includes solutions such as Krypton Secure MFA, AI Insight, Zero Trust Network Access (ZTNA), Endpoint Data Loss Prevention (DLP), XDR, EDR, MDR, PAM and compliance-focused security capabilities. These solutions are designed to support stronger authentication, AI-aware data protection, least-privilege access, continuous monitoring, intelligent threat detection and secure governance while helping organisations balance security with operational productivity. We also place significant emphasis on supporting regulatory and compliance requirements across sectors, including BFSI, government and large enterprises.

We believe cybersecurity is most effective when advanced technology is combined with strong customer support, continuous innovation and close collaboration. Our commitment is to provide reliable, enterprise-grade security solutions backed by responsive service while contributing to India's growing cybersecurity ecosystem. As organisations accelerate digital transformation, our objective remains to help customers securely protect their users, data, infrastructure and critical digital assets against an increasingly dynamic threat landscape.

Forging a National Alliance for Trusted AI and Digital Security

Mr. Ram Iqbal Singh, Founder & Chairman of NACOF; Dr. Deepak Kumar Sahu, Founder & CEO of FaceOff Technologies; and Dr. Arindam Sarkar, Chief Architect at FaceOff Technologies, sign an MoU aimed at strengthening cybersecurity solutions for India's banking sector.

There is landmark moment in India's journey toward secure and trusted digital transformation. The Memorandum of Understanding (MoU) between FaceOff Technologies and NACOF (National Federation of Farmers Procurement, Processing and Retailing Cooperative of India Ltd.) marks the beginning of a strategic partnership dedicated to strengthening cybersecurity, digital trust, and fraud prevention across Cooperative Banks and other institutions.

Through this collaboration, FaceOff's Sovereign AI platform, powered by Post-Quantum Cryptography, will help organizations detect and prevent deepfakes, synthetic identities, cloned voices, and AI-generated fraud while supporting privacy-first digital verification and regulatory compliance. This partnership reflects a shared commitment to protecting India's digital economy with homegrown innovation and next-generation security technologies.

Honouring Dr. Ajai Chowdhry: Lifetime Achievement Award 2026–27

Dr. Deepak Kumar Sahu, Editor-in-Chief of VARINDIA, and Dr. Gulshan Rai, India's first National Cyber Security Coordinator, Government of India, present the Lifetime Achievement Award to Dr. Ajai Chowdhry, Co-Founder of HCL.

The Lifetime Achievement Award 2026–27 is the highest recognition presented by VARINDIA to celebrate an extraordinary individual whose vision, leadership, and lifelong contributions have transformed India's technology landscape. This prestigious honour recognizes not only professional excellence but also a legacy of innovation, institution-building, and nation-building that continues to inspire generations.

Today, we proudly honour Dr. Ajai Chowdhry, Co-Founder of HCL and Padma Bhushan awardee, whose pioneering leadership has been instrumental in shaping India's IT, electronics manufacturing, startup ecosystem, and digital transformation journey. His unwavering commitment to technological self-reliance, policy advocacy, and the National Quantum Mission has strengthened India's position as a global technology powerhouse, making him a true architect of the nation's digital future and an inspiration to the entire ICT industry.

(L-R): Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA; Dr. Prince Joseph, Global CIO, SFO Technologies; VV Jacob, Chief General Manager - IT, Malayala Manorama Co. Ltd; Sujoy Brahmachari, CIO & CISO, Rosmerta Technologies Ltd; Vijay Sethi, Chairman, Mentorkart; Golok Kumar Simli, President - Technology & Innovation, BLS International; Lt. Col. (Dr.) Santosh Khadsare (Retd), CEO, iDEFENCE Innovations Pvt. Ltd; and Bharat B Anand, Group CITO, Contec Global.

PANEL DISCUSSION : I

FROM DIGITAL INDIA TO AI INDIA: THE NEXT LEAP

The first panel discussion at the event, moderated by Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA, brought together leading technology and business leaders on the theme, “From Digital India to AI India: The Next Leap.” The panellists included Vijay Sethi of Mentorkart, Golok Kumar Simli of BLS International, Sujoy Brahmachari of Rosmerta Technologies, Bharat B Anand of Contec Global, Lt. Col. (Dr.) Santosh Khadsare (Retd) of iDEFENCE Innovations, Dr. Prince Joseph of SFO Technologies, and VV Jacob of Malayala Manorama.

The discussion focused on leveraging India's digital foundation to accelerate AI adoption through sovereign capabilities, trusted governance, indigenous innovation, talent development and collaboration across government, academia, enterprises and startups.

Bharat B Anand, Group CITO, Contec Global

“The journey from Digital India to AI India is not a transition but an evolution, where AI builds on the strong digital foundation created through initiatives like Aadhaar, UPI and the country’s expanding digital infrastructure. India’s scale of data, digital infrastructure and talent presents a unique opportunity, provided government, enterprises and startups work together while investing in R&D, sovereign infrastructure and AI talent. AI should be viewed as a value creator rather than merely a cost-cutting tool. While it will reshape jobs, it will also create new opportunities, making continuous upskilling, strong governance and a collaborative ecosystem essential to realizing the vision of ‘Jan Jan AI, Ghar Ghar AI.’”

Dr. Prince Joseph, Global CIO, SFO Technologies

“India’s AI journey must be anchored on data, trust and good governance. As enterprises increasingly adopt AI tools, the bigger challenge is ensuring that sensitive information remains protected through effective guardrails and governance mechanisms. While organizations have little choice but to embrace AI, concerns around data security and policy enforcement continue to persist. Building sovereign AI is therefore not just about technology or infrastructure, but about creating trusted systems that inspire confidence among enterprises and citizens alike. Unless these foundational elements are addressed, India’s vision of emerging as a global AI leader by 2030 will remain difficult to realize.”

Golok Kumar Simli, President - Technology & Innovation, BLS International

“The journey from Digital India to AI India is about building intelligence on the strong digital foundation the country has already created. The next step is leveraging data responsibly while ensuring AI remains trusted, ethical and empowering for citizens. Building sovereign AI requires semiconductor and hardware capabilities, cloud sovereignty, indigenous AI models and a strong AI talent ecosystem. By 2030, India should not merely be a consumer of AI but help define the global path for ethical, interoperable and India-centric AI innovation.”

Lt. Col. (Dr.) Santosh Khadsare (Retd), CEO, iDEFENCE Innovations Pvt. Ltd.

“Sovereign AI is critical for sectors such as defence and digital forensics, where trust, credibility and data integrity cannot be compromised. Governments and security agencies will always prefer trusted indigenous AI solutions, particularly when accuracy has direct operational consequences. Developing indigenous LLMs and integrating them into AI solutions will strengthen trust while addressing India’s security and operational requirements more effectively. Enterprises and users must also adopt and promote homegrown AI innovations to accelerate their maturity and help India become a leader in sovereign AI by 2030.”

Sujoy Brahmachari, CIO & CISO, Rosmerta Technologies Ltd.

“AI will build on India’s strong digital foundation by making digital payments, identity and communication systems more intelligent, secure and efficient, while enhancing the overall user experience. In the enterprise, AI adoption should be driven by measurable business outcomes such as higher productivity, improved efficiency, better product quality and reduced rejections, rather than workforce reduction. Successful AI implementation also requires continuous training and refinement of models to deliver sustained value. By 2030, AI will become an integral part of everyday life, supported by data models and infrastructure tailored to India’s unique requirements.”

Vijay Sethi, Chairman, Mentorkart

“Building AI for India begins with developing AI models trained on Indian data, reflecting our unique culture, languages and real-world contexts. Alongside strengthening semiconductor capabilities, we must harness India’s vast talent pool to create AI solutions that address domestic priorities. In enterprises, AI should be viewed as a driver of productivity, quality and value creation. By 2030, India’s AI ambitions will depend on close collaboration among academia, government, corporates, startups and citizens to build a globally competitive and inclusive AI ecosystem.”

VV Jacob, Chief General Manager - IT, Malayala Manorama Co. Ltd.

“India has built a strong digital ecosystem that is generating enormous volumes of data, but we must now focus on developing our own AI models and capabilities instead of remaining dependent on foreign LLMs. Strengthening indigenous AI models, increasing investments in R&D, and fostering stronger collaboration with universities to nurture AI talent should be national priorities. By 2030, we must reimagine products using the latest AI technologies, ensuring they remain relevant, competitive and capable of addressing India’s evolving needs.”

(L-R): Gyana Swain, Consulting, Editor, VARINDIA; Rohit Ponnapalli, CISO- Envoy Global; Sarita Padmini, Sr. Director- Protiviti India; Dr. Rakshit Tandon, Founder- R T Cyber Academy; Jaspreet Singh, Partner and GCC Industry Leader- Grant Thornton Bharat; Dr. Harsha Thennarasu, Founder & CISO-HKIT Security Solutions and Garvit Sharma, CTO- Athenian Tech

PANEL DISCUSSION : II
POST-QUANTUM SECURITY: THE RACE AGAINST TIME

A panel discussion themed "Post Quantum Security: The Race Against Time" was moderated by Gyana Swain, Consulting, Editor, VARINDIA. The panelists who joined the session were Rohit Ponnapalli, CISO- Envoy Global; Dr. Rakshit Tandon, Founder- R T Cyber Academy; Sarita Padmini,Sr. DirectorProtiviti India; Jaspreet Singh, Partner and GCC Industry Leader- Grant Thornton Bharat; Dr. Harsha Thennarasu, Founder & CISO-HKIT Security Solutions and Garvit Sharma, CTO- Athenian Tech.

Gyana Swain set the stage for the discussion by highlighting the importance of post-quantum security and examining how today's CIOs are preparing for it. "When we discuss about or talk about quantum computing, we used to think this is a future technology. But for the panelists and the cyber security professionals who are sitting here, they have a very tough tasks to do. They are already working on quantum computing because for them the future will be decided what they are doing or acting upon right now. For CIOs, the future of quantum computing depends on the actions they take today," he said.

Dr. Rakshit Tandon, pointed out that businesses are still in the awareness phase and talking and discussing about quantum computing, but the threat is inevitable. "Looking at the past incidences, we have seen a lot of data breaches, and if we look at the approach of these notorious hackers, it is 'harvest now and decrypt later'. So now they have started this phase. They are already started dumping your encrypted data, and they are waiting for the Q-Day, the day when they will be able to break all these encryptions, whether it is RSA or ECC, and they will be misusing your data. In other words, quantum computing threatens cybersecurity by rendering foundational encryption algorithms (like RSA and ECC) obsolete. So I think the threat is immediate, and immediately the CISO should start identifying their crypto assets. They should start working on crypto agility and how to modify their algorithms with the minimum expenditure in coming future."

Jaspreet Singh cited an example he read recently, "I recently read that an iPhone secured with a six-digit PIN could, in theory, be unlocked using brute-force methods and today's available computing power in roughly seven to eight hours by systematically testing every possible PIN combination. Anybody wants to take a guess using quantum tech, which is available today in developed countries, how much time will it take? 21 seconds is what they are claiming. If we look at all our infrastructure from an IT perspective and legacy systems that we have in our country, including hard-coded passwords. Are we equipped or is our preparedness enough for the crisis ahead? That only time can tell."

According to **Dr. Harsha Thennarasu,** any new technology needs a minimum of five to 10 years to accommodate to or adopt it. "But at this point of time, we are in need of quantum security because quantum is going to break any encryptions and the outcome can be as disastrous as anyone can expect. USA's NIST (National Institute of Standards and Technology) has already finalized the framework for quantum computing. The government of India also has allocated ₹6,003.65 crores for the 2023–2031 period. When you talk about the industry, corporate have started adopting it, but where are the small medium enterprises? How they are going to adapt to this big change or are they going to lose their big business by succumbing to threats by the quantum attacks? So that is the biggest challenge at this point of time."

Sarita Padmini stated that business organizations are yet to discuss about or bring the topic of quantum computing to the boardroom. "I would suggest it's high time now. If we are not starting the journey right now or begin discussion around how to plan the road ahead, it may be too late before we finally wake up to this realization. Until now, the elephant in the room was AI. Mythos happened and no one was ready. So tomorrow, the Q-Day would happen and nobody would be ready. It is very essential that the organizations understand and align their quantum plans with their business resiliency strategies. The skillset needs to be developed within the organization at this point of time because it would not be something that we cannot develop within a year. It may take another five to 10 years for the organization to develop that skillset."

Rohit Ponnapalli contradicted a bit and said, "So far, quantum technology is not even an agenda in the boardrooms. We are still trying to assess the kind of attacks we see from implementing AI or what kind of breaches we see by incorporating third-party SaaS platforms. But definitely, they have a clarity that over a period of time quantum will be the way forward. There are a few industries who are definitely interested in understanding the implementation of quantum technology, followed by the security controls around how do we safeguard our data. But from my point of view, right now the challenge is AI."

Garvit Sharma said that Shor's algorithm was developed in 1994, and before that there was RSA 2048, an asymmetric cryptographic algorithm running for quite a decade. "The challenge is that quantum will break Shor's algorithm and RSA 2048 in sometime. But can it break it now? It is not possible and will take ages for quantum to break RSA 2048. The threat is definitely there 10 – 15 years from now, when we would have quantum computers with 20 million qubits, and they can break RSA within few hours."

(L-R): S Mohini Ratna, Editor, VARINDIA, Debraj Dam, Chief of VAD, Supertron VAD Venture, Dr. Mithilesh Singh, Marketing Head, Commscope India Pvt Ltd., Pranab Mohanty, Chief Business Officer, Data Safeguard Inc., Sanjay Chaudhary, Head of Marketing Enterprise, SAP India, and Ankesh Kumar, Chief Marketing Officer, Ingram Micro India Pvt. Ltd.

PANEL DISCUSSION : III
GEOPOLITICS RESHAPING MARKETING BUDGETS

The last panel discussion of the day, themed “Geopolitics Reshaping Marketing Budgets”, was moderated by S Mohini Ratna, Editor, VARINDIA. Opening the discussion, she said, “Geopolitical shifts evolving trade policies, supply chain challenges and the rapid rise of AI are reshaping how organizations plan and prioritize their marketing investments. Today's CMOs are moving beyond traditional brand building towards data driven ROI focused and agile marketing strategies.”

Ankesh Kumar, Chief Marketing Officer- Ingram Micro India Pvt. Ltd.

"The main effect of the geopolitical tensions is how they are affecting the overall economy. There is price rise, supply chain issues, and we are already facing chip shortages for infrastructure projects. We also have uncertainties around the ongoing geopolitical situation. There are tariff issues, there are issues with China, and eventually all of this is affecting the overall economy, the supply chain, and demand.

The moment demand is affected, it has a trickle-down effect on the marketing budget as well. There is not much change in terms of reduction or any major impact, but there is a lot of uncertainty when it comes to planning. In the middle of all this, we are trying to figure out how we are going to adopt AI and automation. So, there are many things happening around.

So there is uncertainty for sure, and it will settle down once we get more clarity as things progress."

Debraj Dam, Chief of VAD, Supertron VAD Venture

"The marketing budget scenario is dynamic right now for most organizations, whether they are manufacturing companies, OEMs, distributors, or channel partners. As leaders, we no longer focus only on metrics like clicks; our priority is the customer lifecycle. We have to focus on the customer lifecycle and long-term value. It is very important that the money we spend on marketing translates into customer satisfaction. If we own one customer, we must ensure that we provide prompt service, continue to promote our product. We also need to ensure that that the customer to be in our custodian for a long time as a value propositions."

Pranab Mohanty, Chief Business Officer- Data Safeguard Inc.

"Any crisis always puts pressure on the CMO's marketing strategy, but during geopolitical crisis, it also adds pressure on supply chain management. For companies operating globally, cost becomes a much bigger challenge. When costs increase, organizations naturally start cutting expenses, and marketing is often seen as a soft target. However, marketing is also one of the most essential business functions. In such a scenario, it is very important that marketing spending is treated as an investment. The focus should be on where to invest. Instead of investing in customer acquisition, organizations should invest more in retaining existing customers and generating recurring business from them. That approach is far more effective in helping businesses navigate the crisis."

Sanjay Chaudhary, Head Marketing Enterprise, SAP India

"If we look back, every generation has had one technology innovation that transformed the way we live and work. AI is different because it is changing everything in terms of the how work is getting done. Earlier, the conversation around AI was about improving efficiency, but today organizations are focusing on how they can bring more revenue generation through AI. the race to AI-driven ROI is really intensifying. AI helps identify the right signals, enables mass personalization, analyzes historical trends, and combines internal and external realities, including geopolitical factors, to make marketing more targeted. This enables account-based marketing, faster execution, and maximum ROI from marketing investments."

Dr. Mithilesh Singh, Marketing Head- Commscope India Pvt Ltd.

"Geopolitics has a big impact on marketing because the moment the map moves, money moves with it. Tensions, conflicts, tariffs, and supply chain disruptions affect product launches and reduce marketing budgets, shifting planning from annual budgets to agile, quarterly, scenario-based programs. There is greater emphasis on local sourcing, national pride campaigns, and consistent investment in corporate reputation and public relations. AI is playing a big role, especially in B2C, but in B2B, multi-million-dollar deals are built on relationships. People trust people, and sales happen through human connections. So we should not forget the importance of human relationship, it is very critical."

YOGENDRA SINGH - BARISTA

EMINENT CIOS OF INDIA

Digital transformation is not simply a technology upgrade. It is a fundamental reimagining of how businesses operate, compete, and serve their customers — demanding bold leadership, cultural courage, and strategic clarity.

Recognizing this year's Eminent CIOs of India (ECIO) for the year 2026-27 celebrates the leaders who have embodied that philosophy. They are the CIOs, CTOs, CDOs, and CISOs who have guided their organisations through complexity and disruption, never losing sight of what technology is truly for driving growth, building resilience, and creating lasting impact. Their contributions span architecting robust digital strategies, fortifying cyber resilience and fostering innovation ecosystems that empower their enterprises to thrive in a hyper-connected world.

SUJOY BRAHMACHARI, ROSMERTA TECHNOLOGIES LTD.

SURJEETY THAKUR, RAJAGIRI HOSPITAL KOCHI

SUSHIL MOHAPATRA - SEDEMAC MECHATRONICS LTD

V V JACOB - MALAYALA MANORAMA COMPANY LIMITED

VIJAY SETHI , MENTORKART

VIVEKANAND NASKAR

ABHISHEKA KUMAR
ECO-MAIL

AMIT BHATIA
KARAM GROUP

ANAND RUHELA
SGT UNIVERSITY

ARINDAM SARKAR
FACEOFF TECHNOLOGIES
PRIVATE LIMITED

ARINDAM SINGHA ROY

ARVIND KUMAR
PATHKINDS LABS

BHARAT B ANAND
CONTEC GLOBAL LIMITED

DR. HARSHA THENNARASU,
HKIT SECURITY SOLUTIONS

DR. SUBROTO PANDA,
ANAND AND ANAND

DINESH GOYAL
HIND TERMINALS PRIVATE LIMITED

GANESH VISWANATHAN, ASSISTO
TEHNOLOGIES PRIVATE LIMITED

GAURAV RANADE,
TECHNOCENTRIC ADVISORY

GOLOK KUMAR SIMLI, BLS
INTERNATIONAL SERVICES LTD

JASPREET SINGH - GRANT
THORNTON BHARAT LLP

KAMAL MATTA - SONIC BIOCHEM
EXTRACTIONS PRIVATE LIMITED

KAMALESH KUMAR - MG CONTRACTORS PRIVATE LIMITED

LT COL SANTOSH - DEFENCE INNOVATIONS PRIVATE LIMITED

MEETALI SHARMA - SDG SOFTWARE (I) PVT. LTD.

MOHAN SHAH - CLAIMPRO ASSIST PRIVATE LIMITED

SANJEEV JAIN, INTEGREON MANAGED SOLUTIONS INDIA PVT. LTD.

PANKAJ MITTAL DIGIZEN CONSULTING

PARVEEN KUMAR SHARMA - MIGSUN GROUP

RAJVEER SINGH - SAXO BANK

RAVI RAZDAN - JYOTHY LABS LIMITED

ROHIT KACHROO - OMNI CYBERX PRIVATE LIMITED

ROHIT PONNAPALLI - ENVOY GLOBAL, INC.

SANDEEP PANDITA - AGI GROWTH X PRIVATE LIMITED

SARITA PADMINI - PROTIVITI INDIA MEMBER PRIVATE LIMITED

SHIKHA SHARMA - MAHARAJA AGRASEN GROUP OF HOSPITAL

SONAM MALLIK - INTERARCH BUILDING SOLUTIONS LIMITED

EMINENT CIOs OF INDIA	
NAME	COMPANY NAME
ABHISHEKA KUMAR	ECO-MAIL
AJAY AJMERA	ROCKMAN INDUSTRIES LIMITED
AJAY YADAV	SBL (P) LIMITED
AMIT BHATIA	KARAM GROUP
AMIT KAPOOR	PRISTINE GROUP
ANAND RUHELA	SGT UNIVERSITY
ARINDAM SINGHA ROY	ADAA GROUP
ARVIND KUMAR	PATHKIND LABS
AVNEESH VATS	TECHNO ELECTRIC AND ENGINEERING COMPANY LIMITED & TECHNO DIGITAL
BALMUKUND KESHAV	JAGSONPAL PHARMACEUTICALS LIMITED
BHARAT B ANAND	CONTEC GLOBAL LIMITED
DINESH GOYAL	HIND TERMINALS PRIVATE LIMITED
DR. ARINDAM SARKAR	FACEOFF TECHNOLOGIES PRIVATE LIMITED
DR. HARSHA THENNARASU	HKIT SECURITY SOLUTIONS
DR. JAGANNATH SAHOO	INOX WIND LIMITED
DR. PAVAN DUGGAL	SUPREME COURT OF INDIA
DR. RAKSHIT TANDON	GURUGRAM POLICE CYBER SECURITY SUMMER INTERNSHIP (GPCSSI)
DR. SUBROTO PANDA	ANAND AND ANAND
DR. VINEET BANSAL	SURYA ROSHNI LIMITED
FARMAN KHALID	EMAAR INDIA
GANESH VISWANATHAN	ASSISTO TECHNOLOGIES PRIVATE LIMITED
GAURAV RANADE	TECHNOCENTRIC ADVISORY
GAURAV VIJ	HOOLIV.COM
GOLOK KUMAR SIMLI	BLS INTERNATIONAL SERVICES LTD
HARSH ARORA	CHAMBAL FERTILIZERS & CHEMICALS LIMITED
J. P. DWIVEDI	RAJIV GANDHI CANCER INSTITUTE & RESEARCH CENTRE
JASPREET SINGH	GRANT THORNTON BHARAT LLP
KAMAL MATTA	SONIC BIOCHEM EXTRACTIONS PRIVATE LIMITED
KAMALESH KUMAR	MG CONTRACTORS PRIVATE LIMITED
KANISHK GAUR	ATHENIAN TECH LIMITED
KAPIL MADAAN	MAX HEALTHCARE INSTITUTE LIMITED
LAKSHMANA VADAGA	RATNAM SOLUTIONS PRIVATE LIMITED
LT COL SANTOSH KHADSARE (RETD)	IDEFENCE INNOVATIONS PRIVATE LIMITED
MEETALI SHARMA	SDG SOFTWARE (I) PVT. LTD.
MOHAN SHAH	CLAIMPRO ASSIST PRIVATE LIMITED
PANKAJ MITTAL	DIGIZEN CONSULTING
PARVEEN KUMAR SHARMA	MIGSUN GROUP
PRINCE JOSEPH	SFO TECHNOLOGIES
RAJ K. RAJPOOT	JAGATJIT INDUSTRIES LIMITED
RAJVEER SINGH	SAXO BANK
RAVI RAZDAN	JYOTHY LABS LIMITED
ROHIT KACHROO	OMNI CYBERX PRIVATE LIMITED
ROHIT PONNAPALLI	ENVOY GLOBAL, INC.

SANDEEP JAMDAGNI	CENTRAL PARK GROUP
SANDEEP PANDITA	AGI GROWTH X PRIVATE LIMITED
SARITA PADMINI	PROTIVITI INDIA MEMBER PRIVATE LIMITED
SAURABH GUGNANI	TMF GROUP
SAURBH GUPTA	GUJARAT FLUOROCHEMICALS LIMITED
SHAILESH KUMAR	TIRATH RAM SHAH HOSPITAL
SHIKHA SHARMA	MAHARAJA AGRASEN GROUP OF HOSPITAL
SONAM MALLIK	INTERARCH BUILDING SOLUTIONS LIMITED
SUJOY BRAHMACHARI	ROSMERTA TECHNOLOGIES LIMITED
SUNIL GUBRANI	FRATELLI WINES PRIVATE LIMITES
SURJEET THAKUR	RAJAGIRI HOSPITAL KOCHI
SUSHIL MOHAPATRA	SEDEMAC MECHATRONICS LTD
SANJEEV JAIN	INTEGREON MANAGED SOLUTIONS INDIA PRIVATE LIMITED
V V JACOB	MALAYALA MANORAMA COMPANY LIMITED
VIJAY SETHI	MENTORKART AND CRAFSOL TECHNOLOGIES
VINOD KUMAR GUPTA	PAYTM MONEY
VIVEKANANDA NASKAR	PROTEGRITY
YOGENDRA SINGH	BARISTA COFFEE COMPANY LTD.

MOST TRUSTED COMPANY IN INDIA 2026

The 'Most Trusted Brands in India 2026' is an initiative led by VARINDIA and the Brand Book editorial team that acknowledges 25 technology brands that have earned consumer confidence while contributing meaningfully to India's digital growth.

Featured in the 15th edition of the Brand Book 2026, these organizations have earned the trust of customers and the industry through innovation, excellence, reliability, and outstanding customer service. Based on VARINDIA's annual research, industry benchmarks, and extensive voter feedback, we proudly honour the companies that have set new standards of leadership and trust.

DELL TECHNOLOGIES PVT. LTD.

LENOVO INDIA PVT. LTD.

AIRTEL LTD.
AMAZON INDIA LTD.
AMD INDIA PVT. LTD.
APPLE INDIA PVT. LTD.
CISCO SYSTEMS (INDIA) PVT.LTD.
DELL INDIA PVT.LTD.
GOOGLE INDIA PVT. LTD.
HCL TECHNOLOGIES LTD.
HEWLETT PACKARD ENTERPRISE INDIA PVT. LTD.
HP INDIA SALES PVT.LTD.
IBM INDIA PVT. LTD.
INFOSYS LTD.
INGRAM MICRO INDIA PVT.LTD.

INTEL TECHNOLOGY INDIA PVT. LTD.
LENOVO INDIA PVT. LTD.
MICROSOFT CORPORATION (INDIA) PVT. LTD.
NVIDIA GRAPHICS PVT. LTD.
REDINGTON LTD.
RELIANCE JIO INFOCOMM LTD.
"SALESFORCE INDIA"
SAMSUNG INDIA ELECTRONICS PVT. LTD.
SAP INDIA PVT. LTD.
TATA CONSULTANCY SERVICES LTD.
TECH MAHINDRA LTD.
WIPRO LTD.

MOST PROMISING PARTNERS 2026

The digital revolution has a secret weapon: the Value-Added Resellers and Partners who turn technology into real-world impact every single day. In today's fast-evolving technology landscape, Value-Added Resellers (VARs) and Channel Partners have evolved beyond their traditional role as intermediaries to become strategic enablers of business transformation. Leveraging deep domain expertise and strong partnerships with global technology providers, they deliver customized, future-ready solutions that empower enterprises to accelerate digital transformation, enhance operational efficiency, and maintain a competitive edge in an increasingly dynamic marketplace.

To celebrate their contributions, VARINDIA felicitated the outstanding VARs and Partners across 5 categories — recognized for their differentiation, excellence, and unwavering customer focus. These winners have demonstrated remarkable differentiation through innovation, customer-centricity, and measurable impact—extending the reach of technology vendors and empowering enterprises with transformative capabilities.

As VARINDIA honors these achievers, we celebrate their dedication, leadership, and their invaluable role in powering India's journey toward a digitally empowered economy.

MOST PROMISING PARTNERS

ACMA COMPUTERS LTD.
BM INFOTRADE PVT. LTD.
CACHE DIGITECH PVT.LTD.
DATAMATION SERVICES
DIAMOND INFOTECH PVT. LTD.
E SQUARE SYSTEM & TECHNOLOGIES PVT. LTD.
GURUSONS COMMUNICATIONS PVT. LTD.
HARITASA ELECTRONICS SOLUTIONS PVT. LTD.
I2K2 NETWORKS PVT. LTD.
INFLOW TECHNOLOGIES PVT. LTD.
INGRAM MICRO INDIA PVT.LTD.
INTENSITY GLOBAL TECHNOLOGIES LTD.
IRIS GLOBAL SERVICES LTD.
IVALUE INFOSOLUTIONS LTD.
PAR DATA SYSTEMS PVT. LTD.
PENTAGON SYSTEM AND SERVICES PVT. LTD.
RAH INFOTECH PVT. LTD.
RASHI PERIPHERALS LTD.
REDINGTON LTD.
SANGHVI INFOTECH PVT. LTD.
SATCOM INFOTECH PVT. LTD.
TECH DATA ADVANCED PVT. LTD.
SUPERTRON ELECTRONICS (SEPL)

SUPERTRON ELECTRONICS (SEPL)

TECH DATA ADVANCED SOLUTIONS INDIA PVT. LTD.

RASHI PERIPHERALS LIMITED

ACMA COMPUTERS LTD.

BM INFOTRADE PVT. LTD.

CACHE DIGITECH PVT. LTD

DATAMATION SERVICES

E SQUARE SYSTEM & TECHNOLOGIES PVT. LTD.

I2K2 NETWORKS PVT. LTD.

INFLOW TECHNOLOGIES PVT. LTD.

INTENSITY GLOBAL TECHNOLOGIES LTD.

IRIS GLOBAL SERVICES LTD.

PAR DATA SYSTEMS PVT. LTD.

PENTAGON SYSTEM AND SERVICES PVT. LTD.

RAH INFOTECH PVT. LTD.

SANGHVI INFOTECH PVT. LTD.

SATCOM INFOTECH PVT. LTD.

BEST MAKE IN INDIA BRAND - NET PROTECTOR ANTIVIRUS

MOST INFLUENTIAL CMOS IN INDIA 2026

DR. MITHILESH SINGH, MARKETING HEAD- COMMSCOPE INDIA PVT LTD.

MR. ANKESH KUMAR, CHIEF MARKETING OFFICER- INGRAM MICRO INDIA PVT. LTD.

MR. NIKHIL DUDWADKAR, HEAD OF MARKETING - KASPERSKY

ANKESH KUMAR	CHIEF MARKETING OFFICER	INGRAM MICRO INDIA PVT. LTD.
PUNEET CHADHA	GLOBAL CMO	REDINGTON LTD.
DR. MITHILESH SINGH	MARKETING HEAD	COMMSCOPE INDIA PVT.LTD.
VINNY SHARMA	SR. MARKETING DIRECTOR- APJ, EUROPE & EMEA	SECURONIX INDIA PVT. LTD.
NIKHIL DUDWADKAR	HEAD OF MARKETING	KASPERSKY
KUSHAGRA SHARMA	DIRECTOR AND HEAD OF MARKETING - INDIA AND SAARC	VEEAM SOFTWARE PVT. LTD.

SOLUTION DISPLAY KIOSKS

CHECKPOINT

COMMSCOPE

FACEOFF

KASPERSKY

INFLOW

IRIS GLOBAL & DELL TECHNOLOGIES

NETWORKING

NP AV

DELEGATES IN THE EVENT

MOST ADMIRED BRANDS 2026

VARINDIA and the Brand Book editorial team have conducted an extensive survey to identify the '50 Most Admired Brands' in the Indian technology sector. Hundreds of brands were meticulously evaluated through a rigorous selection process. This process involved invaluable insights from industry leaders and the VARINDIA editorial team played a critical role in compiling the final list.

The 50 companies recognized and felicitated at the Infotech Forum represent the pinnacle of achievement in the Indian ICT industry and are featured in the 15th edition of the Brand Book 2026. They have earned the admiration of consumers by consistently delivering high-quality products, prioritizing research and development, ensuring timely availability, and providing outstanding post-sales support.

NEMETSCHEK INDIA PVT. LTD.

DYNABOOK INDIA

YOTTA NETWORK SERVICES PVT. LTD.

ACER INDIA PVT. LTD.

SUPERTRON ELECTRONICS (SEPL)

IVALUE INFOSOLUTIONS LTD.

VEEAM SOFTWARE PVT. LTD.

QUALYS SECURITY TECHSERVICES PVT. LTD.

DENAVE INDIA PVT. LTD.

PRAMA INDIA PVT. LTD.

TECH DATA ADVANCED PVT. LTD.

KASPERSKY

ACRONIS INDIA PVT. LTD.

INFLOW TECHNOLOGIES PVT. LTD.

COMMSCOPE INDIA PVT. LTD.

TP-LINK INDIA PVT. LTD.

SEAGATE TECHNOLOGY (INDIA) PVT. LTD.

ADITYA INFOTECH LTD. (CP PLUS)

SIFY TECHNOLOGIES LTD.

ESDS SOFTWARE SOLUTION LTD.

IBM, Sarvam partner to strengthen India's sovereign AI ecosystem

The collaboration will develop sovereign AI solutions for governments and regulated enterprises, enabling secure, governed and multilingual citizen services.

IBM and Sarvam, India's full-stack sovereign AI company, have announced a strategic collaboration to accelerate the development and adoption of sovereign AI technologies across the country. The partnership will focus on developing AI solutions for central and state governments, public sector organisations and regulated enterprises, supporting secure and compliant AI deployment aligned with India's regulatory, security and operational requirements.

The collaboration combines IBM Sovereign Core, IBM's sovereign-by-design AI platform, with Sarvam's India-first sovereign AI stack, which includes reasoning models and multilingual language and voice AI trained in India. Together, the companies aim to promote trusted and governed AI through innovation pilots, solution accelerators, technical advisory and knowledge-sharing initiatives.

AI FOR GOVERNMENT AND REGULATED SECTORS

The partnership will support use cases such as citizen services, grievance redressal, document processing and administrative workflows. The integrated platform is designed to enable secure, multilingual and voice-enabled government-to-citizen services while helping organisations move AI initiatives from pilots to production.

The IBM GovTech AI Innovation Center in Lucknow will serve as a joint incubation and demonstration hub where government agencies, public sector organisations and enterprises can evaluate sovereign AI technologies and address implementation, governance and operational requirements. Sriram Raghavan, General Manager, IBM Software, India and Software Innovation Lab, said, "Sovereign AI is not simply about where AI runs. It is about giving organizations control over how AI is governed, deployed, and operated. IBM Sovereign Core provides an open, enterprise-grade platform designed to help governments and regulated enterprises scale AI while addressing governance, security and compliance requirements." Pratyush Kumar, Co-Founder of Sarvam, added, "Sovereign AI has to run inside the systems governments and enterprises already depend on. IBM's Sovereign Core gives governments an AI-ready technology foundation they control."

Cloud Migration in the AI Era:
Insights from Across the Industry

Cloud Migration Across Industry

Cloud migration is undergoing a fundamental redefinition. What was once framed primarily around agility, scalability, and cost savings has evolved into a far more complex conversation spanning around AI readiness, data governance, regulatory compliance, security, and long-term business value. Across the industry, leaders from hyperscalers, infrastructure providers, systems integrators, and value-added distributors are converging on a similar conclusion: moving workloads to the cloud is no longer the finish line. It is the starting point of a much longer transformation journey.

For many organizations, the earliest barriers to migration are not technical at all. Internal alignment, change management, total cost of ownership etc., often shape the pace and direction of a cloud strategy. Once that alignment is secured, the real complexity begins to surface which involves dependencies between applications, data, and legacy systems that have accumulated over years, sometimes decades, of business logic and integration.

The emerging consensus favours a structured, phased approach: assess the environment, map dependencies, prioritize workloads based on business relevance, pilot before scaling, and continuously optimize after migration. The goal is not simply to move faster, but to move with precision.

At the same time, compliance and data governance has become a starting-point requirement. Regulatory frameworks such as India's DPDP Act, data residency and sovereignty are now shaping where workloads run and how they are governed. This has accelerated the shift toward hybrid and multi-cloud models, where sensitive workloads remain in more controlled environments while other workloads leverage the elasticity of the public cloud.

On top of this is the growing influence of AI. Organizations are increasingly recognizing that migrating a workload to the cloud does not automatically make it AI-ready. Building a strong, secure, and well-governed data foundation has become a prerequisite for scaling AI initiatives.

Migration revenue is finite; once a workload is moved, that phase of the engagement ends. The greater opportunity for enterprises and their technology partners lies in what comes next: managed services, continuous optimization, proactive security monitoring, compliance assurance, and AI-led business transformation. The organizations poised to extract the greatest value from the cloud are not those that migrate the fastest, but those that treat migration as the beginning of a continuous, outcome-driven journey.

Building AI-Ready Clouds with Governance at the core

Mayank Chaturvedi
Hybrid Cloud Solutions Sales Leader - HPE India

HPE India's Mayank Chaturvedi asserts that AI is changing the way organizations think about cloud migration. "A few years ago, the conversation was largely about agility, scale, and cost. Today, customers are evaluating cloud decisions through a much broader lens that includes AI readiness, data governance, regulatory compliance, security, and long-term operational control."

"In India, we are hearing this consistently from customers. Requirements driven by the DPDP Act, RBI and SEBI guidelines, growing focus on data sovereignty, and even geopolitical considerations are influencing where data resides, how it is governed, and who ultimately controls critical technology platforms. Organizations want to innovate faster, but they also want greater visibility and control over their data and operations," Mayank adds.

TAILORING THE RIGHT CLOUD STRATEGY

It is true that cloud migration is no longer just an IT modernization project. "Before organizations can scale AI successfully, they need a strong data foundation with the right governance, security, and accessibility built in. We are also seeing a clear shift away from one-size-fits-all cloud strategies. Data, applications, and AI workloads often have different requirements, which is why many organizations are adopting a hybrid-by-design approach," he says.

"At HPE, we believe successful AI transformation requires the right data, the right infrastructure, and the right operating model working together. Through the GreenLake platform, we help customers modernize their cloud environment on their own terms while maintaining control, resilience, and compliance. Looking ahead, the organizations that will be best positioned for the future are those that allows data, applications, and AI to work together seamlessly while maintaining control over security, operations, and costs," he says.

Building Intelligent, Resilient enterprises on the Cloud

Sanjeev Chauhan
Vice President, Cloud Engineering - Oracle India

Oracle India's Sanjeev Chauhan is of the view that over the next three to five years, cloud migration will shift from being a one-time infrastructure modernization initiative to becoming a continuous business transformation journey. "The focus will no longer be on simply moving workloads to the cloud, but on continuously optimizing applications, data, and operations to improve agility, resilience, innovation, and business value," he says. "Rather than migrating for the sake of cloud adoption, enterprises will prioritize migrations that enhance customer experiences, accelerate product development, strengthen resilience, and unlock insights from data."

He also adds that instead of adopting a single-cloud strategy, organizations will deploy applications and data across public, private, hybrid, and multicloud environments based on business, regulatory, performance, and cost considerations. "Increasingly, the emphasis will be on bringing AI and analytics closer to where data resides, minimizing unnecessary data movement. At the same time, automation and AI will transform how migrations are planned and managed."

PRESERVING BUSINESS CONTINUITY WHILE MIGRATING

The challenge while cloud migration is ensuring that organizations can modernize without introducing unacceptable business risk, performance degradation, compliance issues, or unplanned downtime. "The most effective approach is to make migration a business transformation initiative rather than a technology project. It starts with a comprehensive assessment to establish a clear understanding of the application landscape, dependencies, data flows, security requirements, and business criticality."

"Equally important is executing the migration in well-defined phases. Establishing secure landing zones, automating infrastructure provisioning, validating application performance, replicating data, and building rollback and recovery into every migration wave significantly reduces operational risk," Sanjeev explains.

Role of Cloud: Shifting from Infrastructure to adding Enterprise Value

Venkat Sitaram
Senior Director & Country Head- Infrastructure Solutions Group - Dell Technologies India

Venkat Sitaram believes that cloud migration will become less about infrastructure transformation and more about business transformation. "The future won't belong to enterprises that simply move to the cloud—it will belong to those that build infrastructure capable of evolving with every new business and technology opportunity," he says.

However, the hardest part in cloud migration today isn't moving workloads but modernizing them for the AI era without compromising business continuity, security or performance. "Many organizations have successfully migrated applications over the years, but they are now realizing that simply moving workloads to the cloud doesn't automatically make them AI-ready. Organizations therefore need a modern data foundation that can support both traditional enterprise applications and next-generation AI workloads, while allowing them to continuously evolve without disruptive infrastructure refreshes," Venkat assesses.

DATA TRUST & SECURITY

As organizations accelerate cloud adoption and AI deployment, the conversation is no longer just about data security; it's about data trust. "Organizations today must navigate an increasingly complex regulatory landscape, with requirements around data privacy, sovereignty and industry-specific compliance continuing to evolve. This is prompting many enterprises to adopt a workload-first approach, where sensitive data and mission-critical applications remain in environments that provide greater control, while less-sensitive workloads leverage the scale and agility of the public cloud."

"Successful cloud migration is built on trust. Organizations that integrate security, governance and cyber resilience into their infrastructure from the outset will be better positioned to build resilient digital businesses prepared for the future," says Venkat.

Cloud Migration success story begins with Data Modernization

Sudharsan Aravamuthan

Head - Systems Engineering, India - Everpure

According to Sudharsan Aravamuthan of Everpure, cloud migration will increasingly become a data modernisation journey rather than simply an infrastructure migration exercise. "As organisations move from AI experimentation to production, they will require intelligent data platforms that securely manage data across hybrid and multi-cloud environments while supporting traditional, virtualized and cloud-native applications," he says. "Another major shift will be the growing adoption of enterprise storage platforms running natively within hyperscale cloud environments. Rather than relying solely on cloud-native storage services, organisations will increasingly seek consistent enterprise storage, protection and disaster recovery capabilities across both on-premises infrastructure and public clouds."

MIGRATING LEGACY WORKLOADS TO THE CLOUD POSES CHALLENGES

The biggest challenge isn't moving workloads - it's modernizing without disrupting the business, is what Sudharsan believes. "The most effective approach is to focus on the data rather than the destination. Today's enterprises operate traditional applications, virtual machines, containers and AI workloads across data centres, edge locations and multiple cloud environments. Success depends on having a common data platform that delivers consistent performance, resilience, security and mobility regardless of where applications run. Equally important is adopting a cloud operating model where infrastructure is automated, policy-driven and programmable, allowing applications and data to move seamlessly across private infrastructure and hyperscale cloud environments," he says.

NO 'ONE-SIZE-FITS-ALL' CLOUD STRATEGY

Sudharsan says that the right cloud mix strategy depends on workload characteristics, data sensitivity, performance requirements, regulatory obligations and business priorities. "For most organisations, hybrid cloud offers the greatest flexibility. As a result of this approach, applications benefit from consistent performance, availability, data protection and disaster recovery regardless of where they run, while IT teams manage both environments through a common operating model," he says.

Cloud Migration evolves as a strategic business enabler for AI, analytics, and long-term growth

Sajiv Nair

Chief Technology Officer & Chief Information Officer - ESDS Software Solution Ltd.

Cloud migration will no longer be viewed by businesses as just an IT modernization initiative but will increasingly serve as the foundation for AI adoption, data-driven decision-making, and long-term business growth, says Sajiv Nair of ESDS Software Solution. "The focus will shift towards building secure, compliant, and future-ready digital ecosystems that can scale with evolving business requirements. At the same time, intelligent automation, hybrid cloud strategies, and sovereign cloud models will see wider adoption as businesses seek greater flexibility, stronger data governance, and enhanced operational efficiency."

CHALLENGES TO MOVING WORKLOADS TO CLOUD

The biggest challenge is not moving workloads, but it is ensuring business continuity while doing so. "Legacy applications often have complex dependencies, making downtime or data loss unacceptable," says Sanjiv. "A successful migration therefore begins with a thorough assessment, followed by a phased, well-orchestrated approach that minimizes disruption, validates performance at every stage, and aligns technology decisions with business priorities rather than treating migration as a standalone IT exercise."

Additionally, security and compliance should be integrated into the migration strategy from the outset, and not addressed after workloads are moved. "Organizations must choose cloud environments that provide robust encryption, strong access controls, continuous monitoring, and compliance with applicable regulatory frameworks. The right cloud strategy depends on the criticality of workloads, regulatory obligations, performance requirements, budget considerations, and long-term business objectives. For many organizations, a hybrid cloud model offers the right balance by enabling sensitive workloads to remain in a secure private environment," Sanjiv asserts.

Redefining Cloud Migration in the AI Era

Sachin Kotian

Head Architecture, Customer Advisory - SAS India

Sachin Kotian of SAS India commends that the cloud landscape is entering a more mature phase, going beyond simply moving workloads. "Cloud environments will increasingly serve as the foundation for real-time decision making, automation, and innovation at scale, with organizations placing greater emphasis on interoperability, governance, and responsible AI. Cloud-native analytics platforms, embedded intelligence, and AI-driven automation will help enterprises respond faster to change, improve operational efficiency, and create competitive advantage in an increasingly digital economy."

IS MIGRATING TO CLOUD A DAUNTING TASK?

As pointed out by many, the biggest challenge to migrating workloads to cloud will be to maintain business continuity.

"Legacy environments often contain complex dependencies, large data volumes, and processes that cannot tolerate disruption. A phased approach, combining data validation, application regression testing, parallel operations, and rollback planning, reduces risk and helps organizations modernize while maintaining operational stability," says Sachin.

Sachin also adds that security and compliance should be embedded throughout the migration lifecycle. "Organizations need clear governance covering data ownership, access controls, encryption, identity management, audit requirements, and continuous monitoring. It begins with understanding what data exists, where it resides, and the regulations that apply to it. This assessment helps determine the right deployment model. Ongoing compliance monitoring, automated policy enforcement, regular security reviews, and visibility into data usage help organizations meet regulatory requirements while protecting customer trust."

Beyond Lift-and-Shift: A Modernization-first cloud strategy

Piyush Gupta
VP – India, APAC & Middle East - Vultr

Piyush Gupta of Vultr states that as organizations move AI initiatives from experimentation to production, they will require scalable, high-performance infrastructure capable of supporting data-intensive and GPU-powered workloads. "We also expect hybrid, multi-cloud, and distributed cloud architectures to become the norm as enterprises seek greater flexibility and resilience. Ultimately, cloud migration will no longer be viewed as an IT project - it will be a business transformation strategy that enables organizations to innovate faster, scale AI adoption, and participate more effectively in India's growing digital economy."

MIGRATION – PART OF MODERNIZATTION STRATEGY

Piyush also asks customers to move beyond a simple lift-and-shift approach and instead view migration as part of a broader modernization strategy. "A phased approach, starting with workload assessment and prioritization helps reduce risk while ensuring applications are optimized for the cloud. By combining flexible infrastructure, predictable cloud economics, and scalable compute capabilities, organizations can modernize with confidence while building a foundation for AI, analytics, and future innovation,"

Security and compliance should be embedded into the migration strategy from day one rather than addressed after workloads have been moved. "As regulations like the DPDP Act and industry-specific requirements continue to evolve, organizations need greater visibility into where their data resides, how it is managed, and who has access to it. Enterprises should prioritize cloud platforms that offer robust security controls, encryption, identity and access management, and local infrastructure that supports data residency requirements. Beyond technology, strong governance frameworks and continuous monitoring are equally important," he says.

Cloud migration represents India's biggest IT opportunity over the next decade

Sonia Ahluwalia
Vice President – Cloud Practice - Kyndryl India

According to Sonia Ahluwalia of Kyndryl, businesses are entering a completely new phase of cloud adoption in India. "Cloud migration is increasingly being driven by what I see as four powerful forces shaping every boardroom discussion—AI adoption, cyber resilience, regulatory compliance and the need for continuous innovation. Today's cloud decisions are no longer about where applications run; they are about how organizations innovate faster, remain secure, comply with evolving regulations and build resilient digital businesses."

"Banks are balancing AI innovation with RBI regulations and cyber resilience. Manufacturers are modernizing factories with AI and Industrial IoT while protecting operational technology. Healthcare organizations are digitizing patient experiences while ensuring data privacy. Government agencies are accelerating citizen services under Digital India and MeghRaj while maintaining sovereignty and trust," she cites a few instances. Over the next five years, Sonia expects cloud migration to evolve into continuous modernization—where enterprises continuously optimize applications, data, security and operations to remain competitive in an AI-first economy. "For Indian enterprises, cloud is no longer the destination. It is the strategic platform that will enable the country's next wave of innovation, resilience and digital growth," she states.

CHALLENGES TO CLOUD MIGRATION

"In my conversations with CIOs and CTOs across banking, manufacturing, telecom, healthcare and the public sector, the challenge they consistently describe is modernizing decades of business-critical technology without disrupting the business. The real complexity lies in understanding application interdependencies, managing operational risks and ensuring that modernization does not compromise resilience. That's why I believe cloud migration is fundamentally a business transformation initiative."

The journey from Cloud-First to Cloud-Smart – the new Business Imperative

Rajesh Gupta
VP & Cloud Business Head - Tata Teleservices

Rajesh Gupta of Tata Teleservices asserts that cloud migration will increasingly become AI-driven rather than infrastructure-driven. "As businesses invest in AI, automation, advanced analytics, and intelligent applications, cloud will serve as the digital foundation that enables these technologies to scale effectively. For India's MSMEs, cloud adoption will become significantly simpler through managed cloud platforms and integrated digital services. Solutions spanning IaaS, PaaS, UCaaS, CCaaS, and AI-powered business applications will increasingly be consumed as services, allowing businesses to focus less on managing technology and more on driving innovation, improving customer experiences, and accelerating growth," he states. As businesses modernise their operations, the conversation today is no longer about being cloud-first; it is about being cloud-smart.

DATA SECURITY & COMPLIANCES

Security should be treated as a design principle, not an afterthought, says Rajesh. "As data becomes more distributed across cloud environments, organizations need consistent governance, identity management, encryption, and continuous visibility across workloads. Equally important is selecting the right cloud architecture. Different workloads have different security and compliance requirements. While customer-facing applications may benefit from the scalability of the public cloud, sensitive financial data or regulated workloads may be better suited to private or hybrid cloud environments."

"For instance, a healthcare provider managing patient records or a financial services firm handling sensitive customer information can adopt a hybrid cloud model that keeps critical data secure while leveraging the agility of the public cloud for applications such as customer engagement and analytics. Compliance becomes significantly easier when security, governance, and cloud architecture are planned together rather than independently," Rajesh explains.

Beyond the Move: Creating Long-Term Value in Cloud Migration

Ranjan Chopra
Founder and CEO - Team Computers

Team Computers believes the most successful cloud journeys begin with understanding business priorities first and technology choices second, ensuring every migration creates lasting customer value.

Overcoming the Toughest Barriers in Cloud Migration

The biggest challenge isn't moving workloads to the cloud; it's ensuring they continue to deliver business value once they get there. Legacy environments often support mission-critical applications with years of business logic, complex integrations, and stringent performance and compliance requirements. Simply lifting and shifting these workloads can lead to higher costs, performance bottlenecks, and operational complexity.

At Team Computers, we begin with a workload-centric assessment rather than a cloud-first mandate. We evaluate application dependencies, data sensitivity, performance requirements, and long-term business objectives before recommending the right migration strategy. Some workloads are rehosted, others are re-platformed or modernized, while certain applications are better suited to hybrid environments. The objective is not just a successful migration, but building a cloud foundation that is secure, scalable, cost-efficient, and ready to support future innovations such as AI, automation, and advanced analytics.

Building Long-Term Customer Value Beyond Cloud Migration

Migration is the starting point, not the destination. The greatest long-term opportunity lies in helping customers continuously extract business value from their technology investments after migration is complete. Enterprises increasingly expect partners to provide proactive operations, intelligent automation, continuous security monitoring, performance optimisation, and cost governance throughout the lifecycle of their cloud environments.

At Team Computers, we are strengthening our capabilities across AI-led managed services, cloud operations, cybersecurity, digital workplace solutions, and infrastructure management. As enterprises continue their digital transformation journeys, the role of a VAR is evolving from implementation partner to long-term strategic advisor. The real opportunity is not simply enabling cloud adoption but helping customers continuously modernise, innovate, and realise measurable business outcomes from the cloud.

Modernising with Confidence, Not Just Migrating with Speed

Gurpreet Sngh
M.D. - Arrow PC Network

Cloud migration isn't just about moving workloads anymore, it's about future-proofing the business. With AI, compliance, and data sovereignty now shaping every decision, Arrow PC Network helps enterprises modernize with confidence — not just migrate with speed.

Overcoming the Toughest Barriers in Cloud Migration

The hardest part is rarely the technology, it's the fear of disruption. Most enterprises are not worried about moving workloads; they're worried about what happens if something breaks during the move.

Our approach is simple: modernize with purpose, not urgency. We focus on assessment, dependency mapping, phased migration, and business continuity planning before moving a single workload. Cloud migration is not a "lift-and-shift" exercise anymore. It's an opportunity to eliminate technical debt, improve performance, strengthen security, and build a foundation for future innovation.

Aligning Cloud Migration with AI Adoption and Compliance Requirements

GenAI has increased the demand for scalable compute, better data management, and faster access to information. At the same time, DPDP and data localisation requirements have made governance a boardroom discussion. As a result, cloud strategy can no longer be separated from security, compliance, and data architecture. Modernization today is about building an environment where innovation and governance can coexist.

Building Long-Term Customer Value Beyond Cloud Migration

Migration opens the door, but the real value begins after the move. The biggest opportunity lies in helping customers continuously optimize, secure, and extract intelligence from their cloud environments.

At Arrow PC Network, we are positioning ourselves as a long-term transformation partner. Whether it's AI-ready infrastructure, cyber resilience, managed services, or cloud governance, our focus is on helping customers derive measurable business outcomes long after the migration project is complete. The future belongs to partners who can manage the entire technology lifecycle, not just the migration milestone.

Supertron VAD Venture Helps Enterprises Turn Cloud Migration into a Growth Opportunity

Debraj Dam
Chief of VAD - Supertron VAD Venture

At Supertron VAD Venture, the role goes beyond enabling technology access, it's about helping customers make the right decisions at every stage of the cloud journey. From untangling complex application dependencies to aligning migration strategies with compliance and AI adoption, it brings the expertise that turns cloud migration from a risk into a growth opportunity.

Overcoming the Toughest Barriers in Cloud Migration
The biggest challenge is understanding the dependencies between applications, data, and existing systems. A direct migration may not always deliver the expected benefits. Our approach is to first assess the environment, identify dependencies, optimize workloads, and then migrate them in a planned manner. This helps reduce risks, minimize downtime, and improve overall performance.

Aligning Cloud Migration with AI Adoption and Compliance Requirements
Today, cloud migration is not only about scalability and cost savings. Compliance, data security, and data residency requirements have become equally important. We ensure that governance, security, and compliance requirements are considered from the beginning of the migration journey. This helps customers adopt new technologies, including GenAI, while maintaining compliance and protecting their data.

Building Long-Term Customer Value Beyond Cloud Migration
We see the biggest long-term opportunity in Managed Services and Cloud Optimization. Migration is the first step, but customers need ongoing support to manage performance, security, costs, and cloud resources effectively. We are focused on helping customers maximize the value of their cloud investments through continuous optimization and support services.

Intelegain Technologies Builds Recurring Customer Value Beyond Cloud Migration

Neeraj Gargi,
CTO & Director - Intelegain Technologies

At Intelegain Technologies, cloud migration is approached as a business transformation initiative rather than a technology project. By combining structured migration planning, AI-led process transformation, and continuous security optimization, the company helps organizations reduce risk, improve operational performance, and create long-term business value beyond migration.

Overcoming the Toughest Barriers in Cloud Migration

Disruption to an established infrastructure initially brings internal challenges related to factors such as change management, TCO, and stakeholder alignment. Once buy-in is secured from internal stakeholders, organizations can begin evaluating other factors that influence the cloud migration strategy, including:

- Licensing complexities from OEMs related to running workloads on-premises versus in the public cloud.
- Regulatory compliance requirements for migrating business-critical applications to the public cloud, although most compliance frameworks support cloud adoption with appropriate adjustments to the migration strategy.
- System integration requirements with external applications and third-party platforms.
- Understanding the TCO implications when transitioning from a CAPEX to an OPEX model.

The following is an industry-proven approach as cloud migration strategy:

Discovery:
We conduct an end-to-end assessment of the existing IT landscape — legacy applications, their dependencies, and their actual relevance to current business needs. This phase is designed to answer three fundamental questions: What exists? What is being used? What can be retired?

Take Baby Steps:
We follow a repeatable, workload-by-workload framework that allows each application to move at its own pace: **Discover → Assess → Prioritize → Pilot → Migrate → Optimize**. Throughout this journey, the focus stays on business outcomes, not migration metrics. Success is measured by improved performance, reduced costs, stronger compliance, and tangible value delivered to the business.

Building Long-Term Customer Value Beyond Cloud Migration

The biggest long-term value creation opportunity is not in migration itself, but in the intersection of AI and security. Migration revenues are finite. Once the workload is moved, the project ends. The real opportunity is creating recurring business value after migration.

Guided AI Led Business Process Transformation
Most customers do not need another chatbot. They need measurable improvements in productivity, customer experience, revenue, compliance, and operational efficiency. Organizations should therefore begin with clearly defined business objectives rather than the technology itself, focusing on metrics such as revenue growth, customer acquisition, customer retention, employee productivity, working capital reduction, faster decision making, and compliance improvement.

Driving Cloud and Data Security
As organizations accelerate their digital transformation journeys, maintaining a strong security posture is no longer optional—it is a fundamental business requirement. For solution providers and technology partners, helping customers strengthen and continuously improve their security posture creates significant long-term business value. Security is not a one-time implementation project; it requires ongoing monitoring, optimization, policy enhancements, compliance assessments, and adaptation to an evolving threat landscape. This creates opportunities for recurring engagement through managed security services, security operations, compliance consulting, vulnerability management, and cloud security optimization.

Enabling Secure, AI-Ready Cloud Transformation

Atul Gupta
Director - RX Infotech

As organizations accelerate cloud adoption and AI initiatives, the focus has shifted from simply moving workloads to building secure, compliant, and scalable digital environments. Lapcare supports this transition through offering premium dependable technology solutions that enables partners to build secure, productive, and future-ready digital environments

Overcoming the Toughest Barriers in Cloud Migration
Cloud migration today is no longer a technology refresh—it is a strategic business transformation. At Lapcare, we believe the biggest challenge in migrating legacy workloads such as ERP, CRM, or inventory management systems to the cloud is ensuring business continuity while preserving data integrity and security. Many organizations rely on customized legacy applications that are deeply integrated with day-to-day operations. Our approach is to adopt a phased migration strategy, beginning with a comprehensive assessment, followed by workload prioritization, rigorous testing, and secure data migration. This minimizes disruption while enabling customers to modernize their IT environment with confidence.

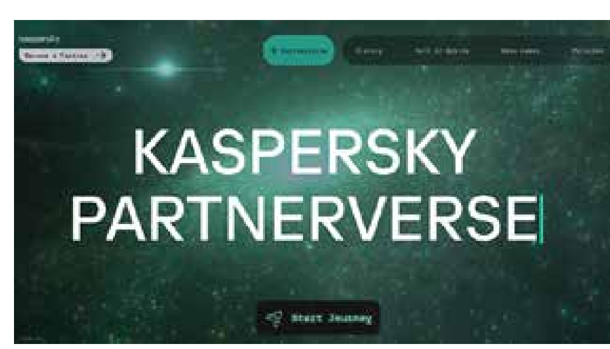
Aligning Cloud Migration with AI Adoption and Compliance Requirements
The rapid adoption of Generative AI, coupled with India's Digital Personal Data Protection (DPDP) Act and data localization requirements, has significantly changed how organizations plan their cloud journey. Cloud infrastructure must now be designed with security, governance, compliance, and scalability at its core. At Lapcare, we see cloud modernization as the foundation for AI-driven innovation. Organizations require secure, compliant, and high-performance infrastructure to unlock the full potential of AI, analytics, and intelligent automation. As a trusted technology brand, we support this transformation through a comprehensive portfolio of IT peripherals, networking products, storage solutions, power solutions, and enterprise accessories that enable reliable hybrid and cloud-first workplaces.

Building Long-Term Customer Value Beyond Cloud Migration
Looking beyond migration, the greatest long-term opportunity for Value-Added Resellers (VARs) and solution partners lies in delivering end-to-end managed services that combine AI enablement, cybersecurity, cloud optimization, and lifecycle support. Customers increasingly seek strategic technology partners rather than product suppliers. Our focus is to strengthen this ecosystem by providing high-quality, dependable technology solutions that empower partners to build secure, productive, and future-ready digital environments. As cloud adoption accelerates across India, we believe sustainable value will come from helping businesses continuously optimize, secure, and innovate on their cloud investments rather than

---

Kaspersky launches Partnerverse to showcase global partner ecosystem

The initiative reflects Kaspersky's long-term channel strategy, bringing together partner recognition, industry collaboration and business growth through an interactive digital experience.



Kaspersky has launched Partnerverse, an interactive digital platform designed to showcase its global partner ecosystem and highlight the role of channel partners in strengthening cybersecurity worldwide. The portal offers an interactive view of the company's worldwide partner network, recognising partner achievements while creating opportunities for existing and prospective collaborators.

The launch reinforces Kaspersky's partner-led business strategy. Over nearly three decades, the cybersecurity company has built a network of more than 18,000 partners delivering cybersecurity solutions to businesses and consumers globally. Through Partnerverse, Kaspersky aims to demonstrate how collaboration and co-innovation with channel partners contribute to business growth and digital resilience.

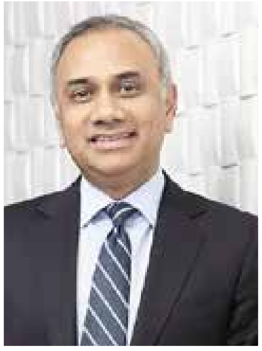
INTERACTIVE PARTNER ECOSYSTEM

Partnerverse visualises Kaspersky's global network as a digital universe, with individual "planets" representing partners across the Sell, Manage and Deploy categories. Visitors can search for companies, browse partners by region, and view programme participation along with Silver, Gold and Platinum partner status.

The portal also features six regional systems, a timeline of Kaspersky's partner programme, a "Hall of Orbits" recognising Global Partner Conference award winners, and a "Hero Cases" section showcasing successful customer engagements. Users can also access the United Partner Portal to explore collaboration opportunities.

STRENGTHENING CHANNEL COLLABORATION

Yury Novikov, Global Head of Channel at Kaspersky, said, "Partners are undoubtedly at the heart of our business, since our collaboration is essential to helping organizations stay protected in an increasingly complex threat landscape. Through Partnerverse, we want to emphasize that our partners are more than just associates – they are a whole universe of trusted ambassadors. We thank them for shaping our image and ensuring that our values, expertise and commitment to cybersecurity reach customers of all segments worldwide. We also invite potential partners to explore the Partnerverse platform, discover how we can elevate your business, and join us on this journey as trusted security leaders."



Salil Parekh to step down as Infosys CEO

Infosys announced that Chief Executive Officer and Managing Director Salil Parekh will step down, concluding a nearly nine-year stint. During his tenure, Salil steered India's second-largest IT services company through a period of operational stability, digital transformation, and the early wave of enterprise artificial intelligence.

According to Infosys, Parekh will step down effective April 1, 2027. The board appointed Ashiss Kumar Dash as CEO Designate. Parekh joined Infosys in January 2018 and is currently the longest-serving non-founder CEO in the company's history. His current five-year term was scheduled to end on March 31, 2027. The announcement comes weeks after Infosys' annual report and AGM notice remained silent on whether the board intended to extend Parekh's tenure beyond March 2027, prompting investor questions about succession plans.

Anthropic appoints Jai Gidwani to founding go-to-market team in India

Anthropic has appointed Jai Gidwani to its founding go-to-market (GTM) team in India as the artificial intelligence company continues to strengthen its presence in the country. Gidwani announced the development in a LinkedIn post, stating that he will be part of the India team led by Irina Ghose. Before joining Anthropic, Gidwani spent more than two years at GitLab, where he progressed from Business Development Executive to Senior Business Development Representative. During his tenure, he was involved in enterprise business development initiatives.

Sharing the announcement, Gidwani said, "Happy to share that I've joined Anthropic as part of the founding GTM team in India, under Irina Ghose's leadership. It's an exciting time to be building in AI, and I'm looking forward to contributing to Anthropic's mission of developing AI that's safe, reliable, and genuinely useful."

Zoom appoints Carlos Quaderi as Head of APAC

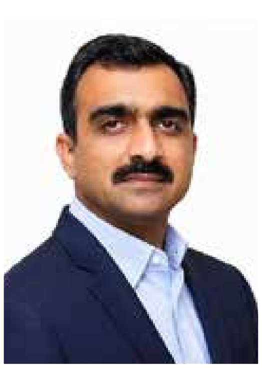
Zoom Communications has announced the appointment of Carlos Quaderi as Head of Asia Pacific (APAC), effective 1 August 2026, underscoring the company's continued investment in APAC as a strategic growth region. His appointment comes as organisations across APAC look beyond standalone productivity tools to AI-powered systems that reduce complexity, connect workflows and help teams move more quickly from conversations to completion.

Reporting directly to Graeme Geddes, Zoom's Chief Sales and Growth Officer, Quaderi will lead Zoom's go-to-market strategy across APAC: Australia and New Zealand (ANZ), Asia, India and Korea, excluding Japan. Quaderi previously served as Zoom's Head of Asia where he drove regional strategy, sales execution and go-to-market initiatives for Southeast Asia, Hong Kong SAR and Taiwan. He will now oversee the broader APAC region, working closely with regional teams and global leadership.

Fortinet names Luca Simonelli as Senior VP, Asia Pacific

Fortinet announced the appointment of Luca Simonelli as Senior Vice President, Asia Pacific (APAC). Based in Singapore, Luca will lead Fortinet's Asia Pacific sales organisation, overseeing the company's businesses across Japan, North Asia and South Asia (Southeast Asia, India & SAARC, Australia and New Zealand). He will be responsible for further driving regional strategy, strengthening customer and partner relationships, and accelerating Fortinet's continued growth across the region.

Luca brings more than 30 years of international technology leadership experience spanning cybersecurity, networking, SASE, cloud security, and managed services. Most recently, he served in a senior leadership role at GCX Managed Services. Throughout his career, he has built and scaled high-performing teams across Europe, the Middle East, Africa and Asia Pacific, holding leadership positions across the cybersecurity, networking and managed services industries, including nearly eight years at Fortinet, where he previously led the company's EMEA business.



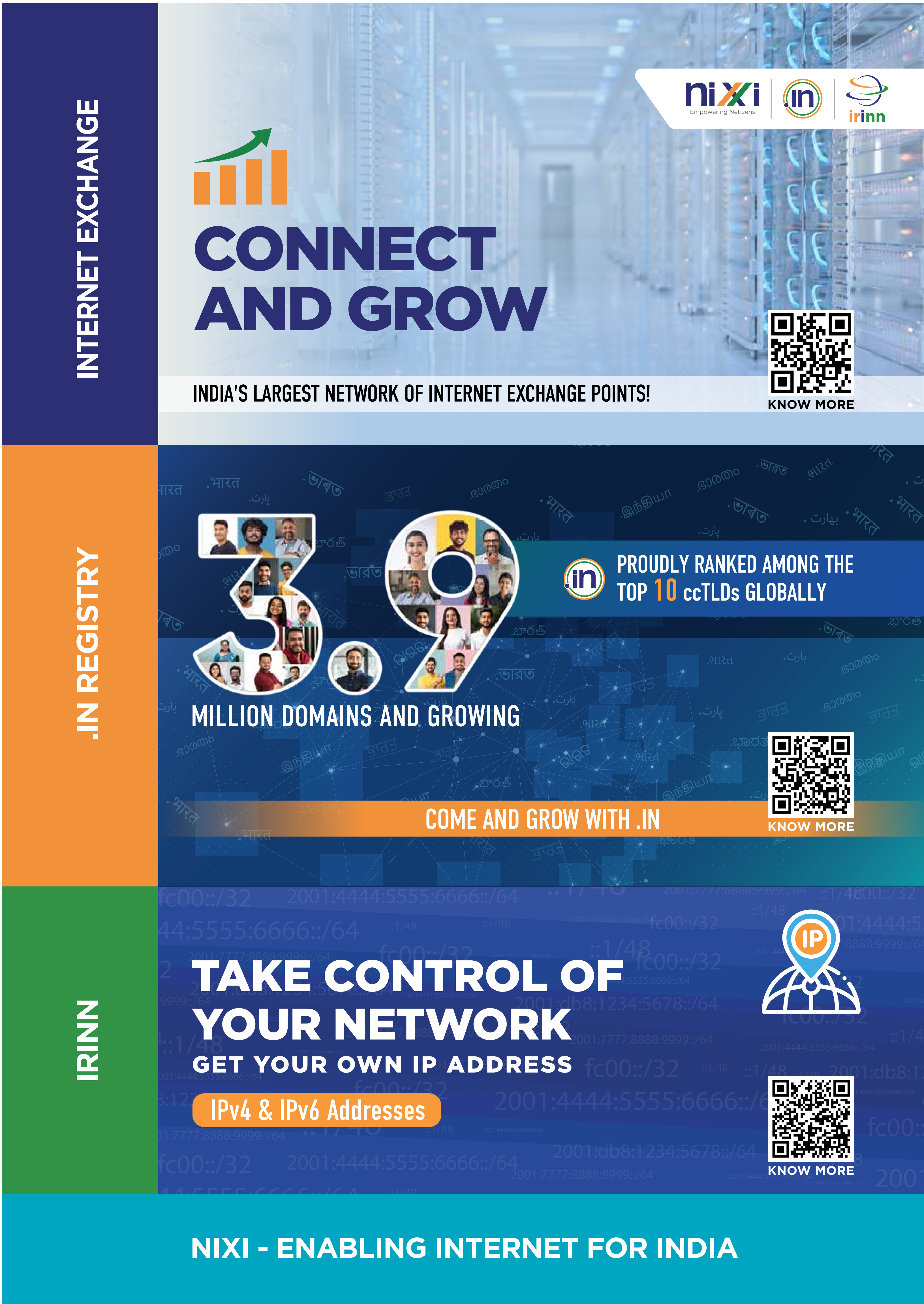
SAP names Mani Shekhar as Head of Partner Ecosystem Success for India

SAP SE has announced the appointment of Mani Shekhar as Head of Partner Ecosystem Success (PES) for SAP India, effective July 1, 2026. In this role, Mani will lead SAP India's partner ecosystem strategy to accelerate AI-driven transformation, cloud adoption, and customer success. He will strengthen strategic partnerships and scale innovation across SAP Business AI, Industry AI, and the SAP Autonomous Suite, empowering partners to co-innovate, build AI-first capabilities, and deliver measurable business outcomes for customers.

"In the era of the Autonomous Enterprise, SAP partners are not just helping customers unlock value from AI and cloud transformation; they are co-creating this new operating model together with SAP and our customers," said Peter Moore, Regional Head of Partner Ecosystem Success, SAP Asia Pacific. "Mani's deep understanding of our business, customers, and ecosystem makes him ideally positioned to strengthen our partner network and accelerate innovation and growth across India."

Accenture assigns Pradeep Prabhala to head India market unit

Accenture has appointed Pradeep Prabhala as lead of its India Market Unit, effective September 1, 2026. His appointment underscores Accenture's continued investment in leadership and talent in India a key growth market and in the differentiated capabilities that help clients unlock new growth opportunities. In this role, Pradeep will work with clients in India to harness data and AI to accelerate growth, boost productivity, and build more agile, future-ready businesses. He will also support global organizations in building Global Capability Centers as engines of innovation, transformation, and resilience - a strategic priority for Accenture globally. Pradeep brings more than two decades of experience advising global organizations on growth and enterprise transformation across AI, digital, commercial excellence, supply chain transformation, M&A, and sustainability. Previously, he was a partner at McKinsey & Company, where he led the Consumer sector in India and Agriculture across Asia.


INTERNET EXCHANGE
nixi
Empowering Netizens
.in
irinn
CONNECT AND GROW
INDIA'S LARGEST NETWORK OF INTERNET EXCHANGE POINTS!
KNOW MORE
.IN REGISTRY
3.9
MILLION DOMAINS AND GROWING
PROUDLY RANKED AMONG THE TOP 10 ccTLDs GLOBALLY
COME AND GROW WITH .IN
KNOW MORE
IRINN
TAKE CONTROL OF YOUR NETWORK
GET YOUR OWN IP ADDRESS
IPv4 & IPv6 Addresses
IP
KNOW MORE
NIXI - ENABLING INTERNET FOR INDIA

RNI - NO 72399/1999

Reg. No: DL-SW-01/4030/24-26
Posted at LPC Delhi RMS Delhi - 110006

Date of Posting 20 & 21
Date of Publishing / Printing: 18 & 19

64 pages including cover