AI AND ML: IS IT A BOON OR BANE FOR CYBER SECURITY?

The year 2020 has been an year of roller coaster ride for all. Due to pandemic, at the work font we have witnessed a boost in remote working which gave an opportunity to cyber criminals to attack remote working group as there are working away from the protected environment of office networks. There was a surge in the number of malicious attacks and cyber frauds across the globe. Cyber fraud including payment and identity card theft which account for more than 55% of all cybercrime lead to major losses for organizations. Security Professionals all over the world are constantly ensuring safety for the companies and their employees. According to experts, stay up to date, backup data and cyber awareness among employees are the major guidelines to fight against this. To know more about this, VARINDIA has asked some questions to security experts and here are their answers:

Cyber-attacks has grown with the surging adoption of the BYOD policy

ASHIS GUHA
CEO, Rah Infotech

With the number of devices getting connected to the network increasing, the attack surface was expected to grow. During the ongoing pandemic, BYOD practices happened over communications network that are not fully secured as employees had to resort to various internet networks including public and mobile networks. BYOD has increased the probability of more cyber-attacks.

As the entire world worked from home (WFH) during the pandemic, the hitherto not-so-tech-using domains like education, sports, healthcare professionals, entertainment professionals etc had to use UC solutions as well as mobile banking to offer their services. All these factors combined, opened up newer channels for the bad guys to enter into the cyber space and eventually cyber attacks increased.

Every organization has to follow three key guiding principles that needs to be followed to protect data. First, enterprises should select the right kind of technologies to secure their data and the selection should always correspond to the kind of business they are in and the kind of problem they want to solve. A tech solution for BFSI may not be too right for, say, manufacturing.

Second, a robust security policy at the enterprise level. This clearly defines the do's and don'ts which ultimately minimizes the security vulnerabilities. And the policy should be revisited time to time keeping pace with the changing global cyber practices and industry dynamics and finally always have a plan B. It has been noticed, despite all the security apparatus functioning perfectly well, the bad guys, at times, breach the wall. In those cases, it's always better to have a system ready that can retrieve the lost data. For that a robust and reliable data backup solution should be there.

RAH Infotech, with the help of its technology OEMs, offers data security solution at every stage and on every layer. From securing the network, to secure data at every layer, we offer end to end data management solutions for securing data including data storage, back up, and recovery.

More organizations to leverage AI to tackle cyber threats

RAJESH CHANDIRAMANI
Senior VP and Global Business Head - ESRM,
AI & Data Analytics, Tech Mahindra

"COVID-19 has transformed businesses, making digital first a business priority. The rapid transition to remote working and increased use of technology and collaboration tools and widespread use of BYOD(Bring Your Own Device) policy, has exposed organizations to higher cyber threats making robust cybersecurity policies imperative. Digital solutions, powered by Artificial Intelligence (AI), are proving to be a game-changer to secure IT networks by monitoring signs of malicious behaviour to safeguard people, communication and data. Therefore, we expect more organisations to leverage AI to tackle cyber threats, analyse risks, accelerate response time and augment security vastly to safeguard sensitive data and assure maximum compliance with privacy and regulatory requirements. We, at Tech Mahindra, have the right alliance partnerships, in-house solution capabilities on all major AI driven cyber-defence solutions, tool providers to ensure that security posture of our customers are always updated and aligned to latest threats, and advanced features like zero trust framework, cyber analytics, threat intelligence, auto-remediation & orchestrations to keep them secure and one step ahead of the attackers."

Malicious attacks and cyber frauds growing rapidly

PARVINDER WALIA
President of Asia Pacific and Japan (APJ), ESET

"The pandemic has created additional considerations for cybersecurity. Globally, businesses have adapted by embracing technology to provide connectivity to networks, videoconference, collaboration tools and cloud services, so employees can work from home. However, not all employees have the feasibility to bring their corporate computers home. This has resulted in many businesses allowing or relaxing their BYOD policy.

At the beginning of the pandemic, ESET had extended free trials for our security solutions including those that are designed to protect home devices, so our customers and their employees remained protected from cyberthreats.

Businesses should also adopt a Zero Trust model where access to corporate network and data must be backed by multi-factor authentication to certify a user's identity. As devices no longer resides within the four walls of the office, there is also a higher risk of business data being lost or stolen. This can be minimized by encrypting disk systems on devices as well as data passing through company servers using solutions such as ESET Full Disk Encryption and ESET File Security.

Other than that, phishing is one of the most common avenues used for ransomware attacks. Solutions like ESET Mail Security can help block spam emails and malware at the server level before they reach mailboxes. Businesses must also ensure cloud productivity applications such as Microsoft 365 are protected as these applications often allow the storage and exchange of sensitive data.

Going through vast numbers of samples to determine if a threat is present requires technology and this is where Machine Learning play a crucial part in cybersecurity. At ESET, we have been using Machine Learning in our products since the 90s and the latest iteration, Auger, uses the combined power of deep learning, long short-term memory and a selected group of six classification algorithms. This allows our security solutions to swiftly and accurately label samples as clean, potentially unwanted or malicious with high detection rates and lowest possible number of false positives.

While ML has greatly improved a business' capability to combat cyberthreats, it is not a silver bullet as cybercriminals are constantly looking for new ways to exploit vulnerabilities. Therefore, ESET has always advocated for a more balanced approach to cybersecurity. We do so through the use of multi-layered technologies that leverage Machine Learning along with other detection and prevention technologies as well as human expertise."

There is no established model for cloud security

HARPREET BHATIA
Director, Channels & Strategic Alliances – India & SAARC, Palo Alto Networks

"The world around us is changing faster than ever. The COVID-19 pandemic has almost instantly changed the way we live and work. Businesses, including ours, have had to adapt quickly to enable a massive remote workforce. Unfortunately, cybercriminals have also been quick to adapt to cash in on the pandemic, causing an increased risk of cyberattacks.

The first aspect companies need to consider is network traffic protection. The inspection of traffic is a vital requirement for securing access and controlling the movement of data. Security teams must build policies that are consistently enforced, regardless of whether the operating endpoint is remote or internal. Besides traffic, data also needs to be protected by securing the network internally – not all users within an organization need access to every nook and cranny of the corporate network. Security teams thus have to adopt network segmentation measures that allow for the partitioning of their network, and to enforce precise controls for access to internal resources based on business needs. Mobile device management is an integral part of any BYOD security strategy. This includes both pre-usage controls, such as providing strong authentication options, as well as other preventive measures such as protection against phishing and credential theft. Although these devices may be privately owned, policy-based security must be instated across the BYOD environment. Possible measures can range from simple – such as requiring a PIN to unlock the phone – to technology-based solutions, such as the ability to remotely lock specific apps if one's device is lost or stolen.

Using AI, the frequently observed threat data & multiple threat feeds can be automated and left to ML algorithms which can decipher attack patterns, leaving the cybersecurity teams to spend time on advance threat hunting. The future of cybersecurity depends on a platform approach. This will allow cybersecurity teams to focus on security rather than continue to integrate solutions from many different vendors. It allows them to keep up with digital transformation.

The cloud, however, is a completely different story. There is no established model for cloud security. The good news is that there is no big deployment of legacy security solutions in the cloud. This means organizations still have a chance to get it right. We can fix how to access the cloud and manage security operations centers (SOCs) to maximize ML and AI for prevention, detection, response and recovery. Only with an integrated platform can cybersecurity teams leverage automation to rapidly monitor, investigate and respond across multi cloud environments and distributed networks that encompass users and devices around the globe."

AI proven to be extremely useful in detecting cyber threats

DEBASISH MUKHERJEE
VP, Regional Sales - APAC, SonicWall

"With its flexibility, BYOD has a security impact on existing IT infrastructure, such as modern organizations using a mix of LANs, WLANs, and distributed WANs. When employees across an organization connect their devices to the network, in certain cases, it may create an entry vector point for cyberattacks.

Companies clearly need to find a way to provide their mobile workers secure access to any data from any device at all times. That said, companies' IT organizations need to understand the risks they are opening themselves up to, if they don't take necessary precautions including data loss, malware, device proliferation, rogue applications, lost and stolen devices with data onboard, credential theft, etc.

As the world grapples with the unforeseen security concerns, robust, boundless security infrastructure and network security are the only answer. SonicWall's Boundless Cybersecurity approach helps solve the cybersecurity business gaps as employees are more prone to attacks while working from home, as unsecured networks create loopholes and may expose critical data. The 'Boundless Cybersecurity' model is purpose-built for today's era of hyper-distributed IT that ensures 'anytime, anywhere business' by protecting exposure points, including a 'boundless' workforce of remote, mobile, and cloud-enabled users. The term 'boundless' personifies SonicWall's recognition of the ability to proactively mitigate cyberattacks and mobilize any organization operating in the new business normal, irrespective of their size.

Artificial intelligence is no more just a buzz word but is making some significant impact on various industries. Artificial Intelligence has proven to be extremely useful when it comes to detecting cyber threats based on analyzing data and identifying a threat before it exploits a vulnerability in your information systems. Machine Learning enables computers to use and adapt algorithms based on the data received, learning from it, and understanding the consequent improvements required. In a cyber-security context, this will mean that machine learning is enabling the computer to predict threats and observe any anomalies with a lot more accuracy than any human can. AI can be used to identify activities that human oversight would mostly fail to catch. The newer threats like never-before-seen attacks require a much more sophisticated capability. The use of AI + ML technology helps to recognize attacks rather than defending a known vulnerability. Machine learning and AI truly protect against modern cyber warfare."

5Ps : The most common causes for breaches

VENKAT KRISHNAPUR
Vice President of Engineering and Managing Director, McAfee India

"With remote working and BYOD now being the new normal, cybercriminals are increasingly looking to capitalize on the widespread panic, by targeting gullible employees with surreal offers, cures, vaccine updates and fake news. A large number of people using their personal devices also pose increased risks, since often these devices don't have proper endpoint security solutions, potentially leaving organisations open to both malicious attacks on their devices as well as loss of crucial corporate information. Malicious actors also leverage spear-phishing, and target select employees to gain access to critical data like staff credentials, intellectual property and customer data.

Businesses as well as employees need to remember the 5Ps that are usually the most common causes for breaches - Phishing, Passwords, People, Patching and Privileges. These are all the more important when it comes to securing corporate data in a highly remote working environment.

Organisations must implement measures to protect their devices and data by establishing remote working policies, list the right tools and platforms, increase the levels of monitoring and audit, and enforce a Zero Trust architecture to mitigate threats. By putting in place anti-malware solutions, which employ cloud-based behavior analysis, and threat intelligence combined with cloud-based web security, organisations can help ensure nearly equal level of security - both on and off the network.

On the home front, it is critical to establish a secure remote connection. This would require the use of a VPN (Virtual Private Network) to ensure data flow is encrypted and controlled within a secure corporate network and by configuration and remote management of devices by enforcing the appropriate security policies. It is strongly advised that employees regularly change cloud passwords with multi-factor authentication to confirm their identity. Having DLP (Data Leakage Prevention) on the devices and configuring appropriate cloud policies – both private and public, would further ensure that the scope for data leakage is minimized. Taking this a step further, organizations must add an additional layer of security of authentication to access company data on mobile devices.

The ever-increasing number of attacks intensified by speed and complexity can overpower experienced and efficient human security professionals. In response to this unanticipated challenge, AI based tools for cybersecurity have emerged to be instrumental in helping security teams reduce risk and efficiently improve their security posture.

By applying advanced analytics and AI to vast amounts of internal and external data, security teams can generate predictive, usable insights that help businesses make better cyber decisions and protect organizations from threats. These actionable insights also help detect and respond to threats faster by monitoring the external environment with a level of speed and accuracy only machines can deliver. "

Corporate Security Protocols and Guidelines for BYOD must be developed

DEVANATHAN BALAJI
Principal Consultant – Cyber Security, NTT Ltd. India

"While BYOD has been around for a while now, its significance has resurfaced with the remote working scenario brought about by the pandemic. In the current situation, we are witnessing a considerable uptick in the number of devices entering the ecosystem. Employees have no choice but to access corporate resources from less secure devices outside the secured corporate perimeter, opening opportunities for cyber criminals to infiltrate networks. Add to this, employees are now more reliant on remote conferencing and collaboration tools, which are also susceptible to various threats. All this has led to many unprecedented changes and added layers of security complexity, which enterprises were not necessarily prepared for.

Organizations are now gearing up for the post-COVID world, where enabling productivity of remote workers will be as important as other business priorities. This, however, must be done while keeping security at the core and embedded in every business decision undertaken. While several security solutions exist, considering workloads and data moving to cloud organization should look security holistically and try to adapt Zero trust framework to improve the security posture.

IT teams must develop and implement corporate security protocols and guidelines for BYOD, put in place roles and responsibility for remote access and limit personal device access to corporate services. Integration of multifactor authentication protocols, implementing screen locks, encryption of devices that transmit data to and from the servers and in case of theft, and enforcing tighter controls over home network security through use of VPNs are key features that a comprehensive security solution must also incorporate. Al and ML can also play a role in unearthing cyber threats, by analysing data and thereafter predicting any threats and abnormalities before it exploits a vulnerability in the information system. Through ML, a subset of AI, computers could apply and adapt algorithms on data, further learn from it and recommend corrections, as required.

Lastly, allocation of resources and budgets must also be reconsidered and not limited to revenue generation and operational efficiency. Along with technology spending, there will be a need to allocate resources specifically towards strengthening remote working capabilities and effective security awareness programs as people impact security outcomes than technology or process."

Cybersecurity training addressing access and responsibilities required for employees

J KESAVARDHANAN
Founder & CEO, K7 Computing

"The overnight transition to working from home, and other increased dependence on online services for shopping, socialising, and even schooling, has definitely cause a spurt in threat activity with a 500% increase in cyberattacks. Work from Home has made many organisations involuntarily adopt a BYOD policy as they have not been able to procure devices for all their employees to use at home, and are relying on their employees using their personal devices. Additionally, these employees are using their personal networks as well which is often not considered by organisations when framing an enterprise BYOD policy.

It is not surprising to see that employees who are now outside the protection of the enterprise IT perimeter are at greater risk of cyberattack. Business leaders have to accept that their enterprise has no perimeter and will never have one in future even after this pandemic is behind us, and adopt a new cybersecurity posture which leverages cloud deployed endpoint security to ensure that all devices and users are protected irrespective of when and where they work. Cybersecurity training that addresses different levels of access and responsibilities is also required for employees as they cannot depend on having an IT team nearby to take care of their security needs.

If data is the new gold, it should be protected as if it is gold. DSCI/PWC estimate that the average cost of a data breach in India is Rs. 11.9 crore. Businesses can avoid such risk by adopting a data security strategy which includes data classification, access based on the principle of least privilege, encryption at rest and in transit, data backup and retention, and physical security of data storage devices. Additionally, a robust endpoint security solution should be deployed to prevent cyberattacks that aim to steal data or hold enterprise data to ransom.

Artificial intelligence enables rapid analysis of large troves of data to identify patterns and draw actionable conclusions. This capability can be utilised to identify threats and block or warn before they can inflict harm in a world where lakhs of new malware are generated every day and manual analysis is not feasible. AI can also help mitigate some of the concerns arising from the deficit in qualified and capable cybersecurity talent by shouldering some of the analytical workload."

Algorithms spot suspicious patterns in network traffic

SUNIL SHARMA
MD- Sales, India & SAARC, Sophos

"The sudden onset of the pandemic forced businesses to very quickly set up working from home facilities/ services, with little time to plan out robust IT security infrastructures to protect these facilities. Additionally, the rise of remote working has also resulted in a decentralised workforce wherein employees are accessing data via their company's network through multiple endpoints, making it difficult for businesses to manage so many identities. Adversaries are exploiting VPN and Remote Desktop Protocol vulnerabilities to gain access and move laterally to create more damage.

PATCH EARLY, PATCH OFTEN

We've won part of this battle already, because most businesses these days do install security patches, if not immediately, but regularly. But there are still many organizations out there that take their time about it, putting off updates for weeks or even months "in case something goes wrong".

KNOW WHAT YOU'VE GOT

Whether you call it an asset register, an IT inventory, or just a plain old list of computers and software you're using, make an effort to know what's on your network – even if you're a small company where everyone works remotely from home. Cybercrooks go looking for old, unloved, unpatched computers, because they know that they could be easy stepping stones to bigger things.

SET UP A SECURITY HOTLINE

Even the tiniest business can do this: make it easy for your users to report anything that doesn't look right. You don't need a dedicated phone number or a call centre – an easy-to-remember email address might be all you need.

REVISIT YOUR BACKUP STRATEGY

As with patching, this is a battle that we've won in part: many companies do know that backups are important, and make at least some effort to keep secondary copies of vital data.

The use of machine learning, specifically deep neural networks, continues to be one of the most significant drivers of new technologies in security. Machine learning allows us to analyze and process massive amounts of data. Machine learning algorithms can be used to detect threats in executable and other files, such as user-generated documents. They are also useful for detecting malicious websites just by looking at the URI. An algorithm can be used to scan emails for simple spam and phishing campaigns, but also for more dangerous threats like thread-jacking and business email compromise attacks.

But more than that, these algorithms can learn what normal looks like in an organization and spot suspicious patterns in network traffic, authentication, and user behavior. These types of security products act as an early warning system for organizations. It allows the security team to react to events as they are happening and well before any long-lasting damage can occur."

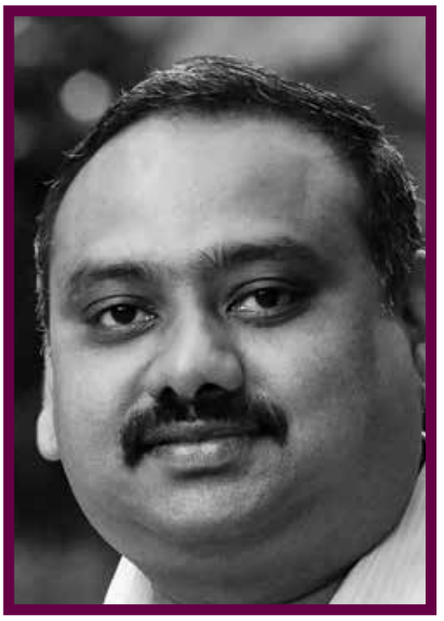
Citrix Workspace protect users from visiting sites with known risks

RAVINDRA KELKAR
Area Vice President, Indian Subcontinent, Citrix

"Leading organizations were already trying BYOD in a limited way, but with remote working becoming mainstream post the pandemic, BYOD has become a norm for organizations across the board. Whilst choice of having a preferred device may have led to more productivity in employees and also given flexibility to employers to 'uberize' IT, BYOD opens up a whole new world of challenges for IT teams struggling to maintain cyber security and data integrity.

At a time when cybersecurity has become more critical than ever, there has been a rise in the use of solutions that take the Zero-Trust approach that follows the principle 'Never Trust, always verify'. The architecture represents a shift from the old 'handing over the keys-to-the-castle approach' of VPNs to requiring all users to incrementally earn trust over time. Trust is never assumed, never an afterthought, but instead is always verified for appropriateness and carefully measured to be commensurate with a user's risk level. At the same time, this approach also considers the user experience. Further, to protect against malware, we designed Citrix Workspace in a way that it not only provides secure, VPN-less access to all apps and data, but also web filtering capabilities that protect users when they visit sites with known risks.

Artificial Intelligence (AI) and Machine Learning (ML) have evolved tremendously over the years. AI's ability to leverage algorithms against massive data sources and determining unusual patterns can be one of the key arsenals to determine new types of phishing and spear phishing attacks that are based on social engineering. We've also been harnessing the tremendous potential of AI/ML through Citrix Analytics to help our partners and customers detect and mitigate risks in their infrastructure. The more information and users analysed over time, the more powerful Citrix Analytics becomes for you, all because of AI."



Risks associated with personal devices can be mitigated by developing effective BYOD strategies

PRADEEPAN V
CTO, Inflow Technologies

"Bring-Your-Own-Device (BYOD) policies are becoming more and more popular in the workplace. Billions of devices are expected to be in use at workplaces. The rapid adoption is due to the surge in usage of mobiles devices like smartphones, laptops and tablets. Employees prefer using their own devices rather than using organization-owned devices at workplaces as it gives more flexible working options.

While BYOD increases productivity, users who does not understand their company's BYOD security policies expose their organization to security vulnerabilities to a greater extent. The growing concern among organizations are users unknowingly downloading malware-ridden apps which has the potential to take control over the user's mobile device followed by breaches due to theft or stolen devices with sensitive business data. BYOD is also acting as driving force to increase insider threats and detecting and mitigating these insider threats are also becoming difficult to IT teams.

Risks associated with personal devices can be mitigated by developing effective BYOD strategies. Organizations have started embracing BYOD actively and are modifying their IT policies anticipating the share of BYOD devices that use corporate network will continue to increase at a fast pace. A Mobile Device Management solution (MDM) is crucial in BYOD security as it gives IT admins the control to lock the device or remotely erase the data in case of an incident or when an employee leaves the organization to ensure sensitive information is not exposed. When MDM's are coupled with features like app visibility, access control, apps management and file integrity monitoring, IT admins will have the optimum level of device control.

Practises like use of SSO, Multifactor Authentication and VPN's along with MDM solutions prevent sensitive data getting leaked especially over public wireless hotspots when users are outside the organization network, and can create barriers between personal and official data on a personal device. Implementing these solutions along with security awareness trainings for employees will address most concerns around the Bring Your Own Device programs in organizations.

Organizations are now exploring on how AI can help Cybersecurity analysts improve on the accuracy responding to Cyber-attacks. The rate of adoption of AI in Cybersecurity is increasing and more organizations are expected to adopt AI in the coming years to detect, predict and respond to cyber threats in real time. However, as on date most organizations are using AI for threat detection primarily as tracking anomalies in real time is becoming a challenge due to the increase in data volume. With Cyber-attacks increasing and threats becoming more sophisticated, AI in Cybersecurity is becoming a key mitigation strategy to counter Cyber-attacks by organizations."

Organizations must consider user education a high priority

NILESH JAIN
Vice President, Southeast Asia and India, Trend Micro

"The risks of implementing BYOD are not just limited to device theft or loss but in securing the valuable enterprise data and apps contained in and accessed by multiple devices outside the network. Targeted attacks and exploiting vulnerabilities are a key security issue for organizations.

As mobile devices form a large portion of an organization's BYOD ecosystem, organizations must be aware of the risks they face from malicious mobile apps downloaded by the users of these devices. Companies should consider providing endpoint security solutions that feature app reputation technology that can detect whether certain apps are safe to use.

While phishing is not just a BYOD problem, it becomes an especially significant threat in a BYOD ecosystem due to the tendency of organizations to focus on the security of the devices within their own network. Cybercriminals often start with the weakest link in the security chain—end users. Phishing attacks can be a very effective way to trick employees into thinking that a malicious email or message is actually a legitimate one. Organizations should make user education a high priority. Employees should be taught to detect phishing attacks and briefed on what to do in case they receive suspicious messages or emails.

At any point along the way, your financial data, customer information, intellectual property, or trade secrets could be lost or stolen. To avoid the embarrassment, reputation damage, regulatory fines, and revenue loss, today's enterprises must be able to identify, track, and secure all confidential data from multiple points within the organization and in the cloud, without impacting employee productivity and performance. It is very important to keep ahead of the latest threats and protect your critical data with ongoing threat prevention and analysis.

The future threat landscape requires AI-powered protection that leverages expert rules and machine learning. AI and ML work in tandem – AI leverages ML capabilities to increase its intelligence and evolve – these systems can be considerably advantageous when it comes to identifying and working to guard against the latest and broad range of security threats including spam, ransomware, exploits, targeted attacks and business email compromise (BEC)."