MICRO FOCUS

IVALUE
Maximizing Value of Technology Investments

"PARTNERS ARE THE ESSENCE OF MICRO FOCUS' BUSINESS STRATEGY AND OUR CHANNEL PARTNER PROGRAM PROVIDES PARTNERS A GREATER OPPORTUNITY TO DRIVE MORE REVENUE THROUGH PORTFOLIO SPECIALIZATION AND CROSS-SELL POTENTIAL, TO GROW AND EXPAND THEIR BUSINESSES"

MR. PRAVEEN PATIL KULKARNI

COUNTRY MANAGER – SECURITY RISK & GOVERNANCE AT MICRO FOCUS

"MICRO FOCUS, TOGETHER WITH INDIA'S LEADING TECHNOLOGY AGGREGATOR, IVALUE INFOSOLUTIONS, COMMITS TO DELIVER MODERN CYBERSECURITY IN COLLABORATION WITH CHANNEL PARTNERS."

Tell us more about your partnership with iValue and how does the partnership enhance your tech and business capabilities?

Partners are the essence of Micro Focus' business strategy and our Channel Partner Program provides partners a greater opportunity to drive more revenue through portfolio specialization and cross-sell potential, to grow and expand their businesses.

iValue has been delivering over four times market growth for its OEMs consistently over the last 12+ years with its unique go-to-market approach and focused teams. Its strong enterprise customer base, across BFSI and ITeS verticals have helped us grow exponentially.

This collaborative approach has helped win recognition across APAC, owing to iValue's robust and scalable delivery models for niche, complementing and compelling offering, through customer engagements. Going forward, Micro Focus aims at partnering more deeply for world level recognitions. We remain committed to providing an easier path for our partners to confidently generate predictable revenue, build pipeline and do business.

What is iValue's contribution towards Micro Focus' business growth and customer needs?

iValue has been a long standing and trusted business partner. They have made an incredible impact in creating a sustainable, high-performance partner ecosystem that has greatly contributed to the growth of Micro Focus business in APAC. Their proactive support and expertise in ensuring a successful partner enablement program has helped Micro Focus and our partners achieve continued success in large and Hybrid IT environments, especially in the Government, BFSI and Enterprise segments.

Why identity is the foundation of security?

Identity serves a key purpose in cybersecurity. Businesses, today, have become information banks handling massive quantities of personal and confidential data – their intellectual capital as well as information belonging to their customers and partner vendors. This data is stored, processed, and accessed in a multi-cloud, multi-device environment by different users. Identity provides a means to control how this data is accessed.

By using identity-based security measures, businesses can ensure that each user can access the information they need to accomplish their objectives without exposing the larger enterprise dataset to the risk of unauthorised access, leaks,or breaches. It can also be used to monitor the way different applications, platforms, networks,and users interact with the enterprise network and data – whether on-premise or on-cloud – and ascertain if this behaviour is aligned with their level of permission. This drastically minimises the risk of a security breachwhile ensuring more robust and seamless operations.

Today's multi-cloud, multi-device environment is a bonanza for hackers - who have more entry points to choose from and are armed with sophisticated software tools to sniff out vulnerabilities across the internet. On this note, how is Zero Trust Model enabling secured work environment

Today's world is unimaginably interconnected. The boundaries between personal and professional, digital and physical, have blurred completely.We are using the same devices to access our workspace and manage our private information – and the evolution of the enterprise IT landscape reflects that.

PRAVEEN PATIL KULKARNI

COUNTRY MANAGER – SECURITY RISK & GOVERNANCE AT MICRO FOCUS

On-premise and cloud-based networks, systems, and processes have merged to give rise to complex hybrid IT architectures. The traditional security perimeter has been completely demolished. A host of new and previously unimaginable vulnerabilities are threatening the integrity and security of enterprise data and systems. Imagine this: hackers can now gain access to large enterprise networks by compromising a single IP-connected device.

The 'Zero Trust' model addresses these challenges with a simple premise: no security measure is completely foolproof and no device or application can be taken to be definitively secure. It focuses on ensuring stronger real-time security through a healthy mix of different security measures; these include, amongst others, pattern recognition, context-based behavioural analysis, user/application access control, ad-hoc audits, and multifactor authentication.

As a result, IT managers and security teams have complete visibility of the risk profiles and security health of all the components comprising their enterprise network, whether on-premise or on-cloud. This helps them to identify and address emerging threats and attacks on a proactive basis, as well as to map and plug any potential security vulnerability.

How can enterprises future proof themselves with Zero trust security?

The most future-ready aspect of the 'Zero Trust' model of cybersecurity is its constant focus on verification. It works with the inherent assumption that vulnerabilities can never be completely eliminated from enterprise IT networks.Whether it is a user, a device, an application, or a line of code, it maps and tracks their behaviour and flags any deviation from its 'normal' or expected behaviour. This helps security teams prioritise real threats over false flags and respond more effectively to threats by automating authorisation and access control processes.