Apple explores AI acquisitions to catch up with rivals

OpenAI to open first India office in New Delhi

INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE *Voice* OF INDIAN VALUE ADDED RESELLERS

VOLUME XXVI ISSUE 12 AUGUST 2025 PRICE RS. 50

RAH INFOTECH
...CONNECTING & SECURING YOUR WORLD

ASHOK KUMAR

RAHUL YADAV

BUILDING LEGACY, DRIVING INNOVATION

How the Kumar father-son duo transformed RAH Infotech into India's fastest-growing cybersecurity distributor

Combatting Cybercrime:
OEMs and Trailblazers Leading the Way

As cyber threats become more sophisticated and relentless, the responsibility of safeguarding digital ecosystems extends far beyond end users and service providers. A crucial yet often overlooked stakeholder in this battle is the Original Equipment Manufacturer (OEM). By embedding security into the very core of hardware and infrastructure, OEMs serve as the first line of defense in protecting enterprises, governments, and consumers against the evolving cybercrime landscape.

This feature explores how leading OEMs and cybersecurity trailblazers are reshaping the narrative of digital security through innovation, collaboration, and a strong focus on secure-by-design principles. Their role goes beyond supplying hardware; they are actively setting new benchmarks, adopting advanced technologies, and building resilient frameworks that can withstand today's threats while preparing for tomorrow's challenges.

To understand the strategies shaping this transformation, VARINDIA spoke with leading cybersecurity leaders who shared their perspectives on critical aspects: the integration of new-age technologies for proactive threat detection, the evolution of solutions to stay ahead of attackers, mechanisms to secure firmware, BIOS, and embedded systems, and the anticipated impact of quantum computing on the OEM security roadmap. Together, these insights underscore the indispensable role of OEMs in building a safer and more resilient digital future.

Fortinet pioneers cybersecurity with AI, Zero Trust, and quantum-safe tech

VIVEK SRIVASTAVA
COUNTRY MANAGER,
INDIA & SAARC,
FORTINET

Fortinet's integrated platform approach, built on FortiOS—the common operating system across FortiGate, SD-WAN, and SASE—is the key to proactively detecting and preventing threats. Most customers begin with our ASIC-powered FortiGate firewall, expand into SD-WAN, and then adopt FortiSASE. Since all core SASE functions are natively built into a single OS, we deliver better performance and security, reduce total cost of ownership, and simplify operations—making us unique in the industry. Fortinet is also uniquely positioned in the growing OT security market, recognized as a leader in the Westlands Advisory Report, which reflects over a decade of focused investment and product development.

We've been investing in AI for over 15 years and hold more than 500 issued and pending AI patents—more than any other cybersecurity company. Our AI tools—FortiAI-Assist, FortiAI-Protect, and FortiAI-SecureAI—are embedded across over a dozen products, enabling automated threat detection, AI infrastructure protection, and accelerated response. We also champion secure-by-design practices, embedding security from the ground up. As a first signatory of CISA's Secure by Design Pledge, we support raising cybersecurity standards by embedding secure practices into every stage of product development. As quantum computing emerges, Fortinet remains committed to helping customers stay protected. With FortiOS 7.6, solutions like FortiGate NGFW and Fortinet Secure SD-WAN now include built-in quantum-safe features, protecting against harvest-now, decrypt-later attacks and enabling a smooth, secure transition to post-quantum security.

Trellix advances AI-driven cybersecurity with Trellix Wise platform

GANESH IYER
MANAGING DIRECTOR, INDIA AND SAARC, TRELLIX

Trellix has integrated AI and machine learning into its security platform to detect and neutralize threats in real time. At the core is Trellix Wise, our generative AI-powered foundation that analyzes telemetry from a vast ecosystem of endpoints and network sources. By correlating signals across multiple hybrid environments, it surfaces genuine threats faster, reduces false positives, and enables automated, intelligence-driven responses—improving analyst efficiency fivefold and reducing Mean Time to Response (MTTR) by up to 50%.

We continuously enhance our platform to address evolving threats. Recent advancements include hyper automation for alert investigation, natural-language search for incident data, and integration with a broader range of third-party tools—three times more than many competitors—ensuring greater visibility across hybrid environments. Trellix processes over 68 billion security queries daily and uses this scale to adapt defenses quickly. Enriched threat intelligence from the Trellix Advanced Research Center delivers both speed and precision in countering sophisticated attacks.

Trellix Wise automates triage, investigation, and contextual reporting, saving 8 hours of analyst time per 100 alerts. It supports multilingual interaction, natural language playbook creation, and automated incident summaries, allowing SOC teams to focus on high-value tasks. Trellix also maintains a vast threat intelligence ecosystem, enriched with telemetry, contextual insights, and feeds from Intel 471 and CISA. Through partnerships like the Cyber Threat Alliance and JCDC, and our open-source Data Exchange Layer, we strengthen threat sharing and collective cybersecurity defense.

Securonix leads autonomous cyber defense with GenAI and quantum readiness

DIPESH KAURA
COUNTRY DIRECTOR - INDIA & SAARC, SECURONIX

Securonix, a five-time Gartner Magic Quadrant Leader in Cybersecurity for SIEM, continues to push boundaries in transforming reactive SOC operations into proactive and autonomous digital defense. The Securonix EON platform, embedded with GenAI agents, enables faster threat detection, investigation, and smart response. It is a future-proof platform that unifies SIEM, SOAR, UEBA, and Data Pipeline Management, scaled with Agentic AI, and brings autonomous decision-making to security operations. Securonix Unified Defense SIEM integrates advanced threat detection, real-time analytics, and automated response mechanisms to help organizations proactively protect their assets. Additionally, Securonix Investigate incorporates ChatGPT-powered GenAI to assist analysts, threat hunters, and administrators in rapidly investigating and responding to threats.

Securonix ensures its platform is constantly evolving to stay ahead of threat actors. We've been harnessing AI for over a decade, with our UEBA technology—driven by machine learning and mathematical models—trained on large datasets since 2007. Our innovation is backed by six patents, some dating back to 2015. Unified Defense SIEM merges UEBA capabilities for broader coverage of cyber and insider threats. In August 2023, we launched Securonix Investigate, followed by the April 2025 release of GenAI agents in EON.

Quantum computing, though still emerging, will transform SOC operations by processing vast volumes of data with unprecedented speed. OEMs must adopt post-quantum cryptographic standards and prepare security infrastructure to address new risks and safeguard digital trust.

Quick Heal pioneers AI-first cybersecurity and quantum-ready defense

DR. SANJAY KATKAR
JOINT MANAGING DIRECTOR, QUICK HEAL TECHNOLOGIES LIMITED

At Quick Heal Technologies, we have embraced an AI-first approach to cybersecurity. Our GoDeep.AI technology integrates traditional machine learning with deep learning, large language models, and NLP—a journey that began over two decades ago with malicious URL detection. Today, this powers both our Quick Heal retail solutions and Seqrite enterprise offerings. We recently adopted a freemium model for AntiFraud.AI, India's first fraud prevention solution, to increase accessibility. On the enterprise side, the Seqrite Intelligent Assistant (SIA) enables instant threat analysis and response recommendations. Additionally, our cloud-native metaProtect platform supports remote security management, while behavioural analytics help identify zero-day threats, moving us from reactive to predictive defense.

The cyber threat landscape has evolved from high-volume attacks to sophisticated, AI-driven campaigns. We counter this with three key strategies: behavioural pattern recognition instead of signature-based detection, real-time cloud intelligence via Seqrite Labs, and security convergence—unifying endpoint, network, and cloud protection for comprehensive visibility. We are focused on mitigating threats like AI-generated phishing, deepfake social engineering, and supply chain attacks that bypass traditional defenses.

Quantum computing represents the next major cryptographic disruption since the internet's creation. By the 2030s, RSA and ECC encryption will become obsolete, requiring organizations to migrate to post-quantum cryptography before practical quantum cryptanalysis emerges. This challenge is as much economic and operational as technical. Treating quantum computing as both a threat and opportunity, early adopters will gain long-term security and competitive advantage.