

How AI-powered attacks are changing enterprise security forever: Dr. Sanjay Katkar, Joint Managing Director, Quick Heal Technologies on defending at machine speed



As India accelerates toward a digitally connected economy powered by UPI, cloud, AI, and Digital Public Infrastructure, cybersecurity has moved from being a technology concern to a national and business imperative. The scale, speed, and complexity of India's digital growth are creating unprecedented opportunities, but also exposing enterprises, institutions, and critical infrastructure to an increasingly sophisticated and relentless threat landscape.

In this interview, **Dr. Sanjay Katkar** shares a ground-level view of how cyber threats are evolving in the age of AI, automation, and hyperconnectivity. Drawing insights from Seqrite Labs' latest threat telemetry and cybersecurity research, he discusses why organisations are now operating in a state of continuous cyber exposure, how AI is reshaping both attack and defense strategies, and why legacy vulnerabilities continue to remain a critical concern despite advancements in security technologies.

Some edited excerpts:

India is rapidly digitizing from UPI to digital public infrastructure to enterprise cloud adoption. Do you believe India's cybersecurity posture is keeping pace with this scale and speed of digital growth? Or are we building faster than we can secure?

India's digital transformation is unprecedented. However, threat telemetry from Seqrite Labs, India's largest malware analysis facility, clearly indicates we are

building faster than we are securing. In 2025, our researchers made 265.52 million detections across 8 million endpoints, averaging 505 attacks every minute.

Further, our Cybersecurity Maturity Survey reveals an overall preparedness score of just 6.3/10 among Organisations. While we see strong adoption in basic malware protection (86.7%) and backups (78.5%), significant gaps persist in foundational areas. Nearly 36% of Organisations still operate End-of-Life systems, and 27.6% lack any defined incident response process. While India is rapidly expanding its digital footprint across critical sectors like education, healthcare, and manufacturing, which together absorbed 47% of all attacks last year, the country's defensive maturity has not kept pace with the scale of its digital ambition.

Your report indicates that India is witnessing continuous, automated attack patterns rather than isolated incidents. Are we now in a state of “always under attack”? How should Organisations adapt to this reality?

Yes, we have transitioned from episodic outbreaks to a continuous state of siege. India, as a rising global power with strategic interests in technology, finance, and defense, faces heightened scrutiny from nation-state actors amid geopolitical tensions, including border disputes and supply chain rivalries, amplifying the relentless cyber pressure. The fact that detections consistently hovered between 17.6 million and 23.1 million every month throughout FY25 proves that threat actors no longer wait for specific opportunities; they use automation to constantly scan, exploit, and monetize digital weaknesses. While the DPDP Act compliance pressures create operational whiplash for Organisations, it does pave the way for security hardening and consent infrastructure deployment.

Organisations need to adapt by abandoning the “perimeter defense” mindset and embracing adaptive security where detection, response, and resilience are embedded into core operations. This requires shifting from manual SOC triage to autonomous, AI-driven security operations that can anticipate and respond to threats in real-time, building strong incident response playbooks, and adopting continuous attack surface monitoring.

The report highlights AI-assisted phishing, contextual attacks, and the rise of cognitive intrusions. How significantly is AI tilting the balance in favor of attackers today?

AI has dramatically compressed the attacker's timeline and scaled their sophistication, tilting the immediate balance heavily in their favor. We are seeing AI-assisted phishing frameworks capable of real-time, contextual responses that make social engineering almost indistinguishable from legitimate interaction. Attackers are using AI to construct digital twins of victims' contacts, mimicking writing styles and even video presence, while automating vulnerability discovery and exploit development. This allows adversaries to launch attacks in hours instead of months. Defending against AI-driven threats now mandates an AI-driven defense, which essentially means security that matches the speed and intelligence of the attackers through predictive anomaly detection and telemetry correlation.

Despite all advancements, the report shows that legacy systems, poor patching, and weak hygiene remain the biggest vulnerabilities. Why does this gap continue to exist, even in large, mature enterprises?

This gap persists because patch orchestration and asset visibility remain operationally complex in hybrid environments. Our survey found that while 64.1% of Organisations have a patch management process, only 69.6% of those focus on critical updates, and 39.8% still operate End-of-Life or End-of-Support systems. Large enterprises struggle with IT/OT convergence, where patching an industrial control system or legacy healthcare application requires significant downtime that businesses are reluctant to take. Consequently, decades-old threats like W32.Pioneer.CZ1 and W32.Expiro.R3 continue to dominate our detections, proving that attackers prioritize reliability over novelty by targeting these unmanaged assets.

Your findings suggest that while on-prem systems drive most detections, cloud threats are more identity-centric and stealthy. Is cloud security creating a false sense of confidence among enterprises?

Absolutely. Because cloud environments accounted for only 9% of total malware detections compared to 91% for on-premise systems, many Organisations misinterpret this low volume as low risk. This is a dangerous false sense of security. Cloud compromises do not rely on noisy, traditional malware; instead, they weaponize identity through OAuth abuse, API exploitation, and credential theft. As we observed in major cloud breaches, a single compromised identity can bypass perimeter defenses entirely and unlock the entire enterprise environment. Endpoint visibility alone is insufficient for the cloud; enterprises must treat identity as the new perimeter and enforce continuous authentication and Zero Trust principles.

With multi-extortion models becoming common, how should Organisations rethink risk, especially from a reputation and trust standpoint?

We need to recognize that ransomware is no longer just a business continuity issue; it is a profound trust crisis. In 2025, ransomware evolved into “Ransomware 2.0” with stealth-oriented, multi-stage campaigns like Xelera and Weaxor that prioritize data theft, financial fraud, and public leaks before encryption even occurs. When an organization’s sensitive customer data or intellectual property is weaponized for extortion, the reputational damage far outlasts the operational downtime. Moreover, the DPDP Act’s ₹250 crore penalties for security breaches and mandatory customer notifications make data exfiltration exponentially more damaging. There is an urgent need for a shift from simply measuring “time to recover systems” to focusing on data-centric security, proactive digital risk protection to monitor brand exposure on the dark web, and maintaining transparent stakeholder communication when incidents occur.

As GenAI adoption accelerates, what are the biggest security blind spots you are seeing in AI deployments today?

The most critical blind spot is the assumption that AI infrastructure is secure by default. We are already seeing the first wave of AI stack-oriented attacks, such as the Langflow RCE vulnerability, which signals that developer and ML infrastructure are highly valuable targets. This emerging threat landscape is comprehensively

mapped by the MITRE ATLAS framework, which details adversary tactics and techniques specifically targeting AI systems, including model poisoning, evasion, and supply chain compromises. This further stresses the need for structured defenses.

As organisations deploy AI for decision-making, we anticipate a rise in “Poisoning the Well” attacks, where adversaries insert biased or maliciously crafted samples into training data to distort model behavior or implant logic-based backdoors. At the same time, DPDP Act compliance requires documenting AI processing decisions affecting data principals, exposing businesses deploying unverified GenAI models to regulatory scrutiny they cannot currently meet. Organisations are largely unprepared for these challenges and urgently need to implement AI security governance, model integrity validation, and adversarial data testing.

You forecast the rise of cognitive intrusions, context-aware, AI-driven attacks.

What does this mean in practical terms for enterprises over the next 2–3 years?

In practical terms, it means enterprises will face adversaries capable of autonomous reconnaissance, real-time payload adaptation, and highly convincing deception at scale. AI-enabled APTs will autonomously refine their tactics, mutate malware, and spoof behavioural patterns to evade detection.

For organisations, this means that static, rules-based defenses will become obsolete. Enterprises must shift to autonomous security operations powered by GenAI, implement cross-layer visibility (endpoints, cloud, identity, network) to identify behavioural deviations, and continuously validate their defenses against AI-augmented threats. Security will no longer be about blocking known threats, but about anticipating anomalous context.

India is both a high-value target and a rapidly growing digital economy. Can India also emerge as a global cybersecurity leader? What will it take?

India has all the foundational elements to transition from being a primary target to a global cybersecurity leader, but it requires a paradigm shift from reactive defense to cognitive resilience. Our digital scale provides unparalleled threat intelligence, as evidenced by our researchers at Seqrite Labs analyzing over 265 million detections. DPDP Act positions India as a regulatory innovator, and combining this with indigenous AI security capabilities like our GoDeep.AI technology creates a unique leadership opportunity.

To lead, we have to move beyond importing security tools and build sovereign, AI-driven security capabilities tailored to our unique challenges, much like our success with DPI and UPI. This requires strengthening national-level intelligence sharing across public and private sectors, prioritizing proactive predictive intelligence, and embedding data protection into the very fabric of our digital innovation.