DIGITAL TERMINAL

Seqrite Warns of Escalating Threat Landscape as India Logs 265 Million Cyber Incidents

Seqrite has released the India Cyber Threat Report 2026 along with two enterprise grade services that respond to one of the most intense threat phases the country has ever faced.

Seqrite has released the India Cyber Threat Report 2026 along with two enterprise grade services that respond to one of the most intense threat phases the country has ever faced. The report has been developed by Seqrite Labs, India's largest malware analysis center, and presents a clear picture of a threat landscape that is accelerating at a pace that affects every sector.

Between October 2024 and September 2025, Seqrite Labs monitored more than 8 million endpoints and recorded 265.52 million detections. This equals more than 7,27, 000 detections each day and 505 detections every minute. Trojans and File Infectors dominate this ecosystem with 88.4 million Trojan detections and 71.1 million File Infector detections. Together they contribute nearly 70% percent of all attacks that struck Indian organizations.

Next Generation Antivirus (NGAV) and Anti Ransomware (ARW) engines identified more than 34 million anomalous activities. Ransomware activity peaked in January 2025 with 185 incidents and 113,000 detections. Cryptojacking detections reached 6.5 million. Network-based exploits exceeded 9.2 million scans that frequently attempted to compromise WordPress plugins, Apache Tomcat, and SysAid systems.

Geographically, Maharashtra (36.1 million detections), Gujarat (24.1 million), and Delhi (15.4 million) emerged as the most affected states, with Mumbai, New Delhi, and Kolkata identified as the top targeted cities. From an industry perspective, the Education, Healthcare, and Manufacturing sectors together accounted for nearly 47% of all detections, reflecting their criticality and resource constraints that make them vulnerable to large-scale attacks

Complementing these findings, the India Cybersecurity Preparedness 2026 Survey reveals that while adoption rates are strong in areas such as advanced malware protection (86.7%) and backup readiness (78.5%), significant gaps persist in incident response, secure configuration, and asset hygiene. With an average maturity score of 6.37/10, India's overall cybersecurity preparedness remains uneven, leaving organizations vulnerable to modern and fast-evolving threats.

Given the criticality of today's cyber threat landscape and the severe economic loss that businesses suffer each time operations are disrupted, Seqrite has also introduced Ransomware Recovery as a Service. This specialized recovery solution addresses the crucial gap between breach and restoration by offering expert led, forensic grade recovery that combines advanced cryptanalysis, custom recovery tooling and isolated restoration workflows to safely and quickly recover encrypted files. Its validated restoration prevents reinfection and ensures that business systems resume without hidden risks, allowing organizations to return to normalcy with confidence.

We have also launched Seqrite Digital Risk Protection Services (DRPS), a SaaS platform designed to detect, monitor, and neutralize digital threats that exist beyond traditional IT perimeters. Seqrite DRPS enables enterprises to proactively safeguard their brand, data, and reputation through ML-driven threat detection and predictive & continuous monitoring. For businesses, it eases tracking fake accounts, counterfeit listings, domain spoofing, and IP misuse to safeguard customer trust and brand reputation by continuously scanning across marketplaces, social platforms as well dark web. Automated, audit-ready reports offer detailed digital evidence for investigations, while a dedicated Seqrite DRPS war room ensures swift takedowns, legal escalations, and crisis management.

Commenting on the new developments**, Dr. Sanjay Katkar, Joint Managing Director from Quick Heal Technologies Ltd., said,** "India's cybers ecurity landscape stands at a critical juncture today, facing unprecedented risks. The India Cyber Threat Report 2026 is aimed at providing policymakers, enterprises, and citizens with the intelligence needed to understand evolving threats, and engage in proactive cybersecurity practices. The launch of Seqrite DRPS will empower organizations to extend their defensive posture beyond firewalls and traditional perimeter security, as brand reputation, data integrity, and customer trust are continuously tested. We are also introducing Seqrite RRaaS to transform ransomware recovery from crisis management into structured, expert-led operations with zero ransom dependency. These initiatives reinforce our commitment to equipping organizations with state-of-the-art tools and insights to safeguard digital assets, preserve trust, and maintain operational resilience in an increasingly hostile threat environment."

India's digital expansion, cloud adoption, and large user base continue to attract ransomware syndicates, state-aligned actors, and cybercriminal groups. Cyberattack campaigns such as Operation Sindoor reflect the rise of hybrid attacks driven by financial, political and ideological motives.

The India Cyber Threat Report 2026 presents detailed insights on advanced persistent threat activity, zero-day vulnerabilities, ransomware campaigns, malware families, and shifting attack patterns.

The report is replete with actionable intelligence that organizations of every scale can adopt. It not only deep dives into India’s threat landscape but also provides clear predictions for the year ahead and practical steps that enterprises can refer to in order to strengthen their defense against anticipated risks. 14 out of the 20 predictions made in the previous edition came true, reaffirming Seqrite’s position as an expert with a proven ability to foresee emerging threats in the Indian landscape.

The guidance in this year’s report spans predictive intelligence, identity-centric defense, AI security hardening, automated patch management, resilience frameworks, collaboration and continuous training, giving businesses a roadmap to improve security readiness in an increasingly complex environment.