

Seqrite highlights surge in software supply chain attacks in 2026, urges enterprises to secure digital vendors

Seqrite has warned Indian organizations about the growing threat of software supply chain attacks as businesses increasingly rely on interconnected vendor ecosystems and third-party software.

The logo for Seqrite, featuring the word "SEQRITE" in a bold, black, sans-serif font. The letter "Q" is stylized with two red diagonal lines crossing through it.

The cybersecurity firm said attackers are increasingly exploiting trusted digital relationships to infiltrate enterprise systems. In a typical supply chain attack, hackers compromise a vendor, software provider, or open-source component used by an organization. Malicious code is then inserted into legitimate updates or services, allowing attackers to gain

access to the target organization's systems through trusted channels.

Several global incidents have demonstrated the scale and impact of such attacks. The SolarWinds cyberattack in 2020 compromised widely used network management software, enabling attackers to infiltrate multiple government and corporate systems. Similarly, the Kaseya ransomware attack in 2021 spread through managed service providers, disrupting hundreds of businesses. Earlier, the NotPetya cyberattack in 2017 spread via a compromised tax software update, causing billions of dollars in damages globally.

According to Seqrite's India Cyber Threat Report 2026, which analysed telemetry from more than 8 million endpoints, cyber threats targeting the country are rising rapidly. Between October 2024 and September 2025, Seqrite Labs—one of India's largest malware analysis facilities—recorded 265.52 million detections, averaging around 505 threats every minute.

The report also highlighted that sectors such as education, healthcare, and manufacturing accounted for nearly 47% of all detections. Ransomware groups including KillSec and Babuk2 were among the most active attackers targeting Indian enterprises, often exploiting vulnerabilities in third-party software and vendor ecosystems.

Seqrite emphasized that organizations must adopt a proactive security approach to mitigate supply chain risks. This includes regularly auditing vendor security policies, restricting third-party access, monitoring software updates, and implementing multi-factor authentication for both internal and external systems.

The company also highlighted the importance of strong data protection measures, especially as breaches often expose sensitive information such as personal data, financial records, and customer details.

With the implementation of India's Digital Personal Data Protection Act, 2023, the regulatory stakes have increased significantly. Under the law, data fiduciaries can face penalties of up to ₹250 crore for serious data protection violations. Seqrite said its enterprise security solutions are designed to help organizations strengthen cybersecurity defenses while ensuring compliance with the country's evolving data protection regulations.