MAY 2025
SUPPLEMENT OF CIO&LEADER

BEHIND THE FIREWALL PG 29

Guarding the digital frontier...

Agnelo Dsouza, CISO, Adani Airport Holdings Ltd

CISOFORUM

Security For Growth And Governance

GUARDING THE GRID: NAVIGATING OT CYBER RISKS IN THE AGE OF AI

With critical infrastructure in the crosshairs, **Pradipta Patro, Head of Cyber Security & IT Platform at KEC International Limited** breaks down the threats and shares a roadmap for resilient, AI-powered OT security. PG. 12

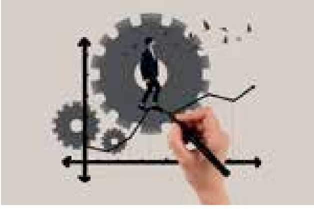
A 9.9 GROUP PUBLICATION
www.csoforum.in
csoforum-in csoforum-in

NEWS & VIEWS

OPINION

INTERVIEW

INSIGHTS



BEHIND THE FIREWALL

CISOFORUM
Security For Growth And Governance
www.cisoforum.in

MANAGEMENT
Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher / CEO & Editorial Director (B2B Tech):
Vikas Gupta
COO & Associate Publisher (B2B Tech):
Sachin Nandkishor Mhashilkar (+91 99203 48755)

EDITORIAL
Group Editor - 9.9 Group: **R Giridhar**
Executive Editor - B2B Tech: **Jatinder Singh**
Correspondent - B2B Tech: **Jagrati Rakheja**
Editorial Intern: **Shikha Pandey**

DESIGN
Creative Director: **Shokeen Saifi**
Senior Designer: **Vipin Rai**

SALES & MARKETING
Director - B2B Tech:
Vandana Chauhan (+91 99589 84581)
National Sales Head - B2B Tech:
Hafeez Shaikh (+91 98331 03611)
Head - Brand & Strategy:
Rajiv Pathak (+91 80107 57100)

COMMUNITY ENGAGEMENT & DEVELOPMENT
Head - Community Relations: **Dipanjan Mitra**
Head - Databases: **Neelam Adhangale**
Community Manager: **Vaishali Banerjee**
Community Manager: **Snehal Thosar**
Community Manager: **Reetu Pande**
Community Manager: **Nitika Karyet**
Assistant Manager Community Development:
Shabana Shariff

OPERATIONS
General Manager - Events & Conferences:
Naveen Kumar
General Manager - Events & Conferences:
Himanshu Kumar
Senior Manager - Digital Operations:
Jagdish Bhainsora
Assistant Manager - Events & Conferences:
Sampath Kumar
Video Editor: **Sunil Kumar**

PRODUCTION & LOGISTICS
Senior Manager - Operations: **Mahendra Kumar Singh**

OFFICE ADDRESS
9.9 GROUP PVT. LTD.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published and Printed by Vikas Gupta for and on behalf of the owners, 9.9 Group Pvt Ltd (formerly known as Nine Dot Nine Mediaworx Pvt Ltd). Published at 121, Patparganj, Mayur Vihar Phase-1, Near Mandir Masjid, Delhi-110091 and printed at G. H. Prints Private Limited, A-256 Okhla Industrial Area, Phase-I, New Delhi - 110020.

Editor: **Vikas Gupta**

9.9 GROUP

AI Arms Race: How India's Tech Hubs Became Cybersecurity Battlegrounds

Vishal Salvi discusses India's evolving cyber threats, emphasizing AI-driven security solutions, behavior-based detection, and the need for zero-trust frameworks as organizations combat increasingly sophisticated attacks in 2025.

By **Jagrati Rakheja** | jagrati.rakheja@9dot9.in

AS INDIA battles an unprecedented wave of cyber attacks, with a staggering 369 million malware detections across the nation, organizations face increasingly sophisticated threats designed to evade traditional security measures. In this exclusive interview with CISO Forum, Vishal Salvi, Chief Executive Officer of Quick Heal Technologies Ltd, reveals the alarming reality behind these statistics and shares how his company's Seqrite solutions are leveraging artificial intelligence to transform cyber defense. From the 974% surge in behavior-based malware to the targeting of critical sectors like healthcare and finance, Salvi provides a sobering assessment of India's cybersecurity landscape while offering strategic insights on how enterprises can build resilience against the next generation of AI-powered threats. As regional technology hubs become prime targets and hacktivism escalates alongside geopolitical tensions, Salvi explains why conventional security approaches are failing and how Quick Heal is pioneering AI-driven solutions to stay ahead in this evolving digital battlefield.

CISO Forum: India is witnessing a surge in cyber threats, with over 369 million detections. What are the primary reasons behind this increase, and how has the threat landscape evolved in recent years?

VISHAL SALVI: India's cyber threat landscape has intensified dramatically, as highlighted in our India Cyber Threat Report 2025, prepared by our researchers at Seqrite Labs, India's largest malware analysis facility, in association with DSCI. Their in-depth analysis revealed 369.01 million malware detections across 8.44 million installations, emphasizing the alarming rise in cyber threats from four primary factors; first, rapid digital transformation has expanded the attack surface, particularly in healthcare, hospitality, and financial sectors, which experienced detection rates of 21.82%, 19.57%, and 17.38% respectively per endpoint.

> "AI-powered cyber threats like Black-Mamba represent a paradigm shift in security. They use AI for evasion and payload generation to create polymorphic malware that adapts to defenses in real-time."

Second, we're witnessing regionalization of threats, with technology corridors in Telangana (15.03%), Tamil Nadu (11.97%), and Delhi (11.79%) facing the highest concentration of attacks. Third, attack methodologies have evolved significantly, with behavior-based malware detections increasing by 974.6% since 2021, jumping from 5 million to 53.73 million. Geopolitical tensions are fueling cyber warfare, as 150+ hacktivist groups targeted Indian entities in 2023, with daily attacks exceeding 50 incidents, often linked to the Israel- Palestine and Russia- Ukraine conflicts. These findings highlight the urgent need for AI-driven threat intelligence and stronger cybersecurity measures to protect India's digital infrastructure.

CISO Forum: With Trojans accounting for 43.38% of all detections, what risks do they pose to enterprises, and how can organizations effectively protect themselves against such targeted attacks?

VISHAL SALVI: When we look at Trojans, the danger lies in their versatility. These aren't simple viruses. They create backdoors that persist in your systems, move laterally across networks, and steal valuable credentials. Let me give you a real example we've investigated. We've tracked variants like Trojan. Sys scan that brute-forces their way into systems to create hidden administrator accounts. Recently, in Karnataka, attackers used this exact approach. They gained initial access and then pivoted to extract entire sensitive databases.

Enterprises can adopt a multi-layered approach to cybersecurity. First, behavior-based detection is essential. It accounts for about 14.5% of our detections and catches threats that traditional signature-based systems miss. We also strongly advocate for zero-trust security frameworks. At Seqrite, we've integrated these principles with our advanced threat detection and network access tools to validate every access request. Combine this with good email filtering and network segmentation, and you'll significantly limit the impact of any breach.

CISO Forum: Many organizations still struggle with cybersecurity preparedness. In your view, what are the key gaps in enterprise security strategies, and how should companies address them?

VISHAL SALVI: AI-powered cyber threats like the BlackMamba keylogger represent a paradigm shift in security. They use AI for evasion and payload generation to create polymorphic malware that adapts to defenses in real-time. To combat these threats, organizations must move beyond signature-based detection, which represents 85% of current detections but cannot keep pace with evolving attack patterns.

To counter this, organizations must prioritize behavior-based detection, which identifies malicious activity based on patterns rather than static signatures. Our data shows a 974.6% surge in behavior-based detections since 2021, highlighting its growing necessity. AI-driven predictive analytics further strengthen security by detecting emerging risks before they escalate.

The human element remains critical, with awareness training evolving to counter AI-generated social engineering attacks. At Seqrite, our XDR solutions leverage machine learning (ML) models to effectively detect and neutralize AI-driven cyber threats. Beyond this, we are developing unsupervised ML models that learn autonomously from vast datasets of malicious activity, enabling real-time anomaly detection.

Looking ahead, we are advancing "AI for AI"—experimental AI models designed to detect and neutralize AI-generated attacks, ensuring proactive defense against the next generation of cyber threats.

CISO Forum: Seqrite is leveraging AI and ML for threat detection and response. Can you share insights on how AI-driven automation enhances cybersecurity resilience?

VISHAL SALVI: At Seqrite, we are making substantial investments in AI and machine learning. These technologies hold immense potential for transforming how we protect our customers. Our research team analyzes threat patterns across our base of 10 million endpoints. This gives us incredible insight into emerging threats and helps us dramatically reduce false positives, a huge pain point for security teams. More importantly, it allows us to identify zero-day threats before they have been widely recognized.

Seqrite's comprehensive security solutions, powered by the self-aware malware-hunting technology GoDeep. AI, auto-remediate threats in real-time, shrinking response windows from hours to seconds. Furthermore, our Malware Analysis Platform combines static, dynamic, and manual analysis to neutralize suspicious files preemptively. AI in cybersecurity also alleviates alert fatigue by prioritizing critical incidents, freeing SOC teams to focus on strategic work rather than sifting through endless alerts.

CISO Forum: Given the increasing sophistication of cyberattacks, what are the primary cybersecurity trends you foresee in India over the next five years?

VISHAL SALVI: Looking ahead at India's cybersecurity landscape over the next five years, several critical trends are emerging that business leaders should prepare for today. First and most concerning of all is how generative AI will transform threats. We already see early signs of hyper-personalized phishing attacks and deepfake-driven social engineering. This is why we're heavily investing in AI-augmented defense capabilities at Seqrite.

For India specifically, we expect cryptojacking to remain a persistent threat. As our country expands its computing infrastructure, these attacks will follow the resources. Similarly, ransomware will continue targeting our critical sectors, with healthcare being particularly vulnerable because of its essential nature and often limited security resources.

The perimeter-based security model is rapidly becoming obsolete. We advise all our enterprise customers to move toward identity-centric security and zero-trust frameworks. Also, compliance will drive significant investment as India continues to evolve its data protection laws. Companies that prepare early will have an advantage. To help our customers adhere to the new, strengthened laws, we have ensured that all our products comply with the recently released DPDP Draft Rules.

“Looking ahead at India's cybersecurity landscape over the next five years, several critical trends are emerging that business leaders should prepare for today."

CISO Forum: Employee training and awareness are critical in mitigating cyber threats. What initiatives does Quick Heal Technologies Limited undertake to help enterprises build a stronger cybersecurity culture?

VISHAL SALVI: We have always believed that technology alone can't solve cybersecurity challenges at Quick Heal Technologies Limited. It's the human element that makes all the difference. That's why we have invested heavily in building Quick Heal Academy as a cornerstone of our cyber education initiatives. We have also developed specialized corporate training programs for enterprises that combine technical depth with real-world scenarios.

We are also addressing the talent

pipeline challenge through our industrial training course. To that end, we have also joined forces with Chitkara University and Quantum University to offer long-term cybersecurity courses. We have introduced short-term learning modules for enterprises looking to build continuous learning cultures that employees can access from anywhere, anytime. These daily drills cover everything from spotting deepfake videos to secure BYOD practices. We introduce new courses to help organizations update their employees with the latest technical know-how and cybersecurity best practices.

CISO Forum: How does Seqrite balance global threat intelligence with localized insights to provide enterprises with tailored cybersecurity solutions?
VISHAL SALVI: At Seqrite, our approach to threat intelligence balances global insights with deep local understanding, which gives us a unique advantage in protecting Indian businesses. We collect telemetry from our global sensor network and combine it with India-specific data from over 10 million nationwide endpoints. This combination is powerful because threats often have regional variations or targeting patterns.

Let me share a concrete example. We recently conducted an in-depth threat study in Karnataka that revealed that Bengaluru experienced approximately 9.5 million threat detections - four times higher than the state average. This granular, localized insight helps us tailor our protections for businesses in different regions.

We have also established valuable partnerships with Indian and international organizations like the DSCI and the NIST, which significantly enriches our understanding of the local threat landscape. At the same time, we ensure our threat intelligence uses standardized protocols that easily integrate with the security tools our customers already have in place. This dual focus lets us predict global threat waves while preempting region-specific campaigns, like cryptojacking surges targeting Indian enterprises.

CISO Forum: What innovations are you currently working on, and how do they address the pressing concerns faced by CISOs today?
VISHAL SALVI: We take immense pride in the several innovations we have developed at Seqrite. First, there's our Malware Analysis Platform (SMAP). We built this to solve two critical problems: the risk of zero-day threats and the overwhelming volume of alerts security teams face. SMAP performs deep analysis of suspicious files and combines this with real-time threat data to identify previously unknown threats.

Our unified EDR-ZTNA security solutions combine advanced threat detection with zero-trust network access. This is particularly important now that most organizations operate in hybrid environments with employees working from anywhere. I'm particularly proud of our work with AI and machine learning models that automatically prioritize security incidents. This addresses the alert fatigue problem I mentioned earlier and helps security teams focus on what truly matters, significantly reducing response times.

We understand that organizations have different infrastructure needs, so we have designed our solutions to be flexible. They can be deployed in the cloud, on-premises, or hybrid configurations. This flexibility ensures that security doesn't hinder your preferred IT strategy. Another pain point we're addressing is compliance reporting. We've built automated reporting capabilities that significantly reduce the burden during audits.

The common thread across all these innovations is our focus on simplifying complexity, enhancing visibility, and aligning security with business outcomes. We firmly believe that security shouldn't be an obstacle to business - it should be an enabler.

CISO Forum: What should be the top priorities for CISOs in 2025?
VISHAL SALVI: First and foremost, security leaders need to translate cyber risks into business terms better. Quantifying risks using metrics like 'time-to-contain breaches' or 'potential financial impact' dramatically improves leadership buy-in and funding support. At Seqrite, we also strongly advocate for the adoption of behavioral analytics. As credential theft becomes increasingly sophisticated, traditional password protections aren't enough. Systems that automatically flag anomalous login patterns - like an employee suddenly accessing systems at 3 AM from an unusual location - provide an essential layer of protection.

Zero Trust security frameworks are gradually becoming non-negotiable as remote and hybrid work becomes permanent. We need to validate every access request regardless of where it originates. Automation should also be a top priority. Security teams are overwhelmed, and automation of routine SOC workflows increases efficiency by creating the capacity to address more strategic security challenges. At the same time, we must shift focus from prevention to ensuring business continuity during and after attacks. This means regular drills and clear recovery protocols.

Lastly, identity security—protecting human and machine identities—will become increasingly critical as organizations expand their use of SaaS applications and IoT devices. By focusing on these priorities, CISOs can better align security efforts with organizational growth objectives, turning security from a perceived obstacle into a business enabler in this challenging threat environment. ■