AUGUST 2025
SUPPLEMENT OF CIO&LEADER

OPINION PG 16

Cybersecurity in the AI era

Dipesh Patel, DVP- Unit Head - Cloud Network and Security Engineering, HDFC Bank

CISOFORUM

Security For Growth And Governance

Trust in Transit

Rethinking API Security in a Microservices World

PG 10

Mayank Mehta
Magma General Insurance

Deepak Bhosale
Asian Paints

Uday Deshpande
Larsen & Toubro

Dr. Pawan K Sharma
Tata Motors

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

17th edition of

THE CISO FORUM

India's Leading Cybersecurity Conference

The Strategic CISO – Leading in the Age of AI

21–22 November 2025

Tropicana Resort & Spa, Alibaug, Maharashtra

In today's enterprises, the CISO are the guardian on trust, resilience, and business continuity. At the CISO Forum Conference & Awards 2025, 70+ India's top CISOs & security leaders across verticals will come together to exchange insights, strategies, and experiences that are shaping the future of enterprise security at the serene beauty of Alibaug.

Keynotes | Panel Discussions | Ideas Café | Roundtables | Case-Study Workshops | Cook-a-thon | NextCISO Awards

Celebrity Speakers @17th edition

David J. Gee
Board Risk Advisor, | Chairman, Leadership Collective Australia.

Dr. Sanket Bhosale
Indian comedian, actor, doctor, and television presenter

Sugandha Santosh Mishra
Indian actress, playback singer, television presenter, comedian, and radio jockey

Prominent Sports Personality

Indian Celebrity Chef

For Partnership Opportunities

Hafeez Shaikh
National Sales Head, B2B Tech
hafeez.shaikh@9dot9.in
+91 98331 03611

Sourabh Dixit
Regional Sales Head - North, B2B Tech
sourabh.dixit@9dot9.in
+91 99714 75342

Subhadeep Sen
Senior Sales Manager, B2B Tech
subhadeep.sen@9dot9.in
+91 96113 07365

Aanchal Gupta
Senior Sales Manager, B2B Tech
aanchal.gupta@9dot9.in
+91 96518 41119

The Trust Revolution

THE ROLE of the Chief Information Security Officer is undergoing a significant transformation. What began as a technical function focused on network and infrastructure defense has evolved into a strategic leadership role that sits at the heart of business value creation.

Driving this change is the profound transformation of the enterprise landscape and business environment. The traditional enterprise perimeter has dissolved. Cloud-first infrastructures, remote workforces, and API-driven ecosystems demand a new security paradigm—one built on trust relationships rather than defensive barriers.

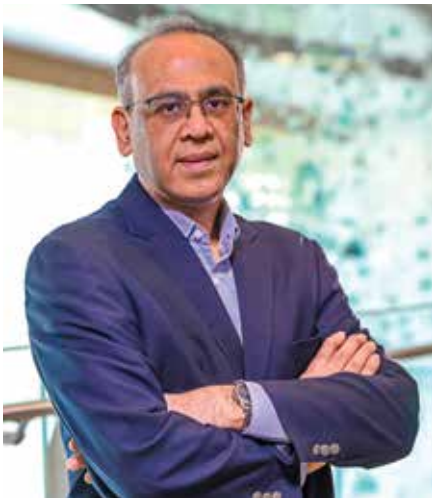
Trust has become a quantifiable business asset. Organizations that master trust-building are achieving superior outcomes: higher customer retention rates, premium market perception, and improved access to capital markets.

And technology leaders are already adapting. They're expanding their mandate beyond threat mitigation to encompass ethical technology deployment. They're building governance frameworks that enable responsible innovation while maintaining competitive advantage. They're becoming the architects of organizational integrity in an age where reputation risk can destroy decades of value creation overnight.

Consider the strategic implications of emerging technologies. AI and machine learning present tremendous opportunities for operational efficiency and market differentiation. Yet they also introduce complex ethical considerations that demand executive-level oversight. The leaders who can navigate this complexity—and deploy AI systems that are both powerful and principled—will define the next decade of competitive advantage.

The regulatory environment is also accelerating this transformation. Privacy legislation continues to proliferate across jurisdictions. Board-level scrutiny of technology governance is intensifying. These aren't obstacles to innovation—they're market forces that reward organizations with mature trust frameworks.

For CISOs, the message is clear. The leaders who will thrive in this new paradigm will be those who can seamlessly integrate technical excellence with ethical leadership, strategic thinking, and stakeholder engagement. This is your moment to redefine what technology leadership means in the digital age.



"Trust is no longer optional—it's the new currency of business and the CISO is its chief architect."

R. Giridhar
Group Editor, B2B Tech
r.giridhar@9dot9.in

CONTENTS AUGUST 2025

COVER STORY

10-15 Rethinking API Security in a Microservices World

APIs power India's innovation, yet expose enterprises to systemic cyber risks demanding strong CISO oversight.

Cover Design by:
Manish Kumar

 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.

OPINION

INTERVIEW

INSIGHTS

FEATURE

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: **R Giridhar**
Editor: **Jatinder Singh**
Senior Correspondent & Editorial Coordinator - CISO Forum: **Jagrati Rakheja**
Principal Correspondent: **Musharrat Shahin**

DESIGN
Creative Director: **Shokeen Saifi**
Assistant Manager- Graphic Designer: **Manish Kumar**

SALES & MARKETING
Senior Director-Community & Brand **Vandana Chauhan (+91 99589 84581)**
National Sales Head - B2B Tech: **Hafeez Shaikh (+91 98331 03611)**
Reginal Sales Head - North: **Sourabh Dixit (+91 9971475342)**
Head - Brand & Strategy: **Rajiv Pathak (+91 80107 57100)**

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

OPERATIONS
General Manager - Events & Conferences: **Himanshu Kumar**
Senior Manager - Digital Operations: **Jagdish Bhainsora**
Manager - Events & Conferences: **Sampath Kumar**
Senior Producer: **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

Sudeep Dey appointed as CIO & CISO at Aster DM Healthcare, India

Sudeep Dey has been appointed CIO & CISO at Aster DM Healthcare, India. With 20+ years in digital transformation, IT, and cybersecurity, he will lead digital, data, and security strategies to drive tech-enabled patient care. His experience spans top healthcare organisations, healthtech advisory roles, and building secure, scalable, and future-ready infrastructures.

Amit Kumar joins Niva Bupa Health Insurance as VP & CISO

Amit Kumar has been appointed Vice President & CISO at Niva Bupa Health Insurance. With nearly 20 years' expertise in cybersecurity, threat management, and governance, he will strengthen the company's security posture. His leadership experience spans GST Network, Orange Business Services, and earlier roles at Ogilvy & Mather and HCL Infosystems.

Manish Sehgal joins JSW as Head – Information Security

Manish Sehgal has been appointed Head – Information Security at JSW, overseeing cybersecurity across its diverse businesses. With 20+ years' experience at firms including CloudSEK, AU Small Finance Bank, and HPE, he is known for building robust, business-aligned security frameworks and driving governance, automation, and compliance to make cybersecurity a growth enabler.

Mayank Mehta appointed CISO at Magma General Insurance Limited

Mayank Mehta has been appointed CISO at Magma General Insurance. With 15+ years in cybersecurity, IT governance, and risk management, he has held leadership roles at Bajaj Allianz Life, Summit Digitel, Axis Finance, and more. He will strengthen Magma's security strategy, compliance, and resilience against evolving threats.

Rajendra Bhalerao appointed as CISO at the Central Bank of India

Rajendra Bhalerao has been appointed CISO at the Central Bank of India. With 20+ years in cybersecurity, risk management, and digital infrastructure, he has led major security programs at Scotiabank, SBM Bank, Paytm Payments Bank, and NPCI, and will strengthen the bank's cyber resilience and governance.

Rohan Haldankar joins BNP Paribas as VP & CISO

Rohan Haldankar has been appointed Vice President & CISO at BNP Paribas. With 20+ years in cybersecurity, IT governance, risk, and compliance, he has held leadership roles at Credit Suisse, Abhyudaya Cooperative Bank, and TCS. He will drive the bank's security strategy and strengthen its regional cyber resilience.

Elastic launches AI SOC Engine to strengthen threat detection in existing tools

Elastic's new AI SOC Engine adds AI-powered threat detection and triage to existing SIEM and EDR systems.

By **CISO Forum** | editor@cisoforum.com

ELASTIC HAS introduced the Elastic AI SOC Engine (EASE), a serverless security package designed to add AI-powered detection and triage capabilities to existing Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) platforms, without requiring immediate migration.

AI-driven alert management

EASE integrates Elastic's Attack Discovery technology to correlate, prioritise, and summarise alerts, reducing SOC analysts' workload and alert fatigue, while an AI Assistant delivers context-aware insights, natural language queries, and enterprise-wide search across Jira, GitHub, and SharePoint.

Fast deployment, broad compatibility

The solution works with Splunk, Microsoft Sentinel, CrowdStrike, and other tools through agentless integrations. This allows organisations to ingest and analyse alerts immediately, applying AI without installing new agents or replacing systems.

> "EASE brings Elastic's proven AI capabilities into the tools teams already use."
>
> **Santosh Krishnan,** GM Observability & Security, Elastic

Transparency and flexibility

EASE supports both customer-managed and Elastic-managed large language models (LLMs). All AI responses are cited, with complete logging of queries, responses, and token usage, ensuring traceability.

Operational metrics

Built-in dashboards provide measurable insights into time savings, improved detection, and return on investment, enabling security leaders to demonstrate business value.

Industry perspective

"SOC analysts are overwhelmed by high alert volumes and lack the AI support they need from their existing SIEM and EDR solutions," said Santosh Krishnan, general manager, Observability & Security at Elastic. "EASE brings Elastic's proven AI capabilities into the tools teams already use, to automatically prioritise threats, correlate alerts, and accelerate investigations."

Michelle Abraham, senior research director at IDC, said the product addresses a key challenge—introducing open and transparent AI into SOCs without rebuilding infrastructure.

By embedding AI-driven detection, alert correlation, and investigation, Elastic helps organisations uncover threats faster and strengthen defences while protecting investments. ■

Tenable launches AI Exposure solution to manage enterprise AI risks

Tenable launches AI Exposure to discover, manage, and secure enterprise generative AI use.

By **CISO Forum** | editor@cisoforum.com

TENABLE HAS expanded its Tenable One exposure management platform with Tenable AI Exposure, a new solution designed to identify, manage, and control risks arising from generative AI use in enterprises. The product, launched at Black Hat USA 2025, supports platforms such as ChatGPT Enterprise and Microsoft Copilot.

Addressing a hidden risk frontier

As companies rapidly adopt generative AI to boost productivity, they often lack visibility into how employees use these tools, what sensitive data could be exposed, and how the systems might be exploited. Tenable AI Exposure aims to close this gap with an end-to-end approach that combines discovery, risk management, and policy enforcement.

Beyond discovery to full governance

"Simply discovering shadow AI isn't enough," said Steve Vintz, Co-CEO and CFO, Tenable. "We're giving organisations the visibility and control they need to safely embrace the promise of generative AI without introducing unacceptable risk."

The agentless system deploys within minutes, offering:

- Comprehensive AI Discovery – Unifies data from Tenable AI Aware and AI Security Posture Management (AI-SPM) to detect sanctioned and unsanctioned AI use, with continuous monitoring of user interactions, data flows, and risk-prone activities.
- Risk Management and Prioritisation – Identifies and ranks risks from sensitive data leakage, misconfigurations, and unsafe integrations with external tools.
- Governance and Control – Enforces organisational policies to guide AI use, blocking threats such as prompt injections, jailbreaks, and malicious output manipulation.

> "Simply discovering shadow AI isn't enough... we deliver visibility and control."
>
> **Steve Vintz,** Co-CEO and CFO, Tenable

Unified risk view

The capabilities integrate into the Tenable One platform, giving security teams a consolidated view of risks across the attack surface. With Tenable AI Aware, AI-SPM, and new governance features, enterprises can discover, assess, and secure AI use without introducing operational delays.

Availability

Tenable AI Exposure is currently in a private customer preview, with general availability planned by the end of 2025.

By combining rapid discovery with governance and risk prioritisation, Tenable is positioning AI Exposure as a comprehensive safeguard for organisations navigating the benefits and security challenges of enterprise AI adoption. ■

F5 adds AI data leak prevention to secure enterprise AI workloads

F5 adds AI-driven tools to prevent data leaks and manage AI risks in enterprises.

By **CISO Forum** | editor@cisoforum.com

F5 HAS introduced new AI-driven capabilities for its **Application Delivery and Security Platform (ADSP)** to help organisations protect sensitive data in AI-powered applications and hybrid multicloud environments. The updates focus on preventing data leakage, managing AI risks, and enforcing compliance policies in real time.

Securing AI and encrypted traffic

The enhancements include expanded functionality in **F5 AI Gateway** to detect, classify, and stop sensitive data from leaking during AI interactions. This includes scanning AI prompts and responses for personal information and applying customer-defined rules to redact, block, or log the data. The technology, powered by F5's recent LeakSignal acquisition, will be available later this quarter.

F5 is also planning to extend **BIG-IP SSL Orchestrator** capabilities by late 2025 to manage AI risks in encrypted traffic. This will allow security teams to decrypt, inspect, and block unauthorized AI use—known as Shadow AI—while maintaining performance and centralising audit and compliance reporting.

> "We're giving leaders the controls to stop data leakage and govern AI use."
>
> **Kunal Anand,** Chief Innovation Officer, F5

Addressing modern AI security gaps

With AI adoption accelerating, sensitive data often flows through encrypted channels or unapproved AI tools, creating blind spots for traditional security methods. F5's new tools aim to close these gaps by:

- Detecting and blocking sensitive data leaks in AI-driven and encrypted traffic.
- Preventing risks from unauthorised AI applications.
- Applying consistent policies across applications, APIs, and AI services.

Balancing innovation and protection

"The core tension in every boardroom today is the race to adopt AI versus the mandate to protect the firm's data," said Kunal Anand, Chief Innovation Officer at F5. "By providing deep visibility into encrypted AI conversations, we're giving leaders the controls to stop data leakage and govern AI use."

Compliance and visibility benefits

"The new features integrate with Security Information and Event Management (SIEM) tools, offering real-time alerts, policy enforcement, and detailed audit logs. This unified approach is designed to reduce compliance risks while enabling secure AI innovation across hybrid and multicloud infrastructures.

By combining AI security, encrypted traffic inspection, and policy enforcement, F5 aims to position its platform as a comprehensive solution for enterprises seeking to embrace AI without compromising data protection. ■

Quick Heal warns of scams targeting Kedarnath helicopter bookings

Quick Heal warns of fake Kedarnath helicopter booking scams targeting Char Dham pilgrims.

By **CISO Forum** | editor@cisoforum.com

QUICK HEAL Technologies Limited has issued a warning over a surge in fraudulent helicopter booking schemes preying on devotees travelling to Kedarnath during the Char Dham Yatra season.

Fake operators exploiting high demand

Researchers at Seqrite Labs, Quick Heal's malware analysis facility, uncovered a network of fake websites and social media profiles impersonating legitimate operators such as Himalayan Heli and IRCTC. These scams, often targeting senior citizens and families, offer steep discounts to entice advance payments before disappearing.

Victims left stranded

In one case, pilgrims paid ₹15,000 per person for a Guptkashi–Kedarnath flight, only to be asked for another ₹30,000. No tickets were issued, and the agency became unreachable, leaving victims financially hit and unable to complete their journey.

Emotional and long-term risks

The scams not only disrupt travel but also harvest personal details—such as phone numbers, bank data, and addresses—placing victims at risk of further fraud. The impact is heightened for those who have spent months or years planning their pilgrimage.

"These scams exploit both faith and urgency, leaving pilgrims financially and emotionally distressed."

Defensive measures with AntiFraud.AI

Quick Heal's AntiFraud.AI platform offers multi-layered protection, including real-time suspicious link alerts, blocking unauthorised screen sharing on financial apps, detecting call forwarding, confirming payee names for QR payments, and monitoring online banking for fraud attempts.

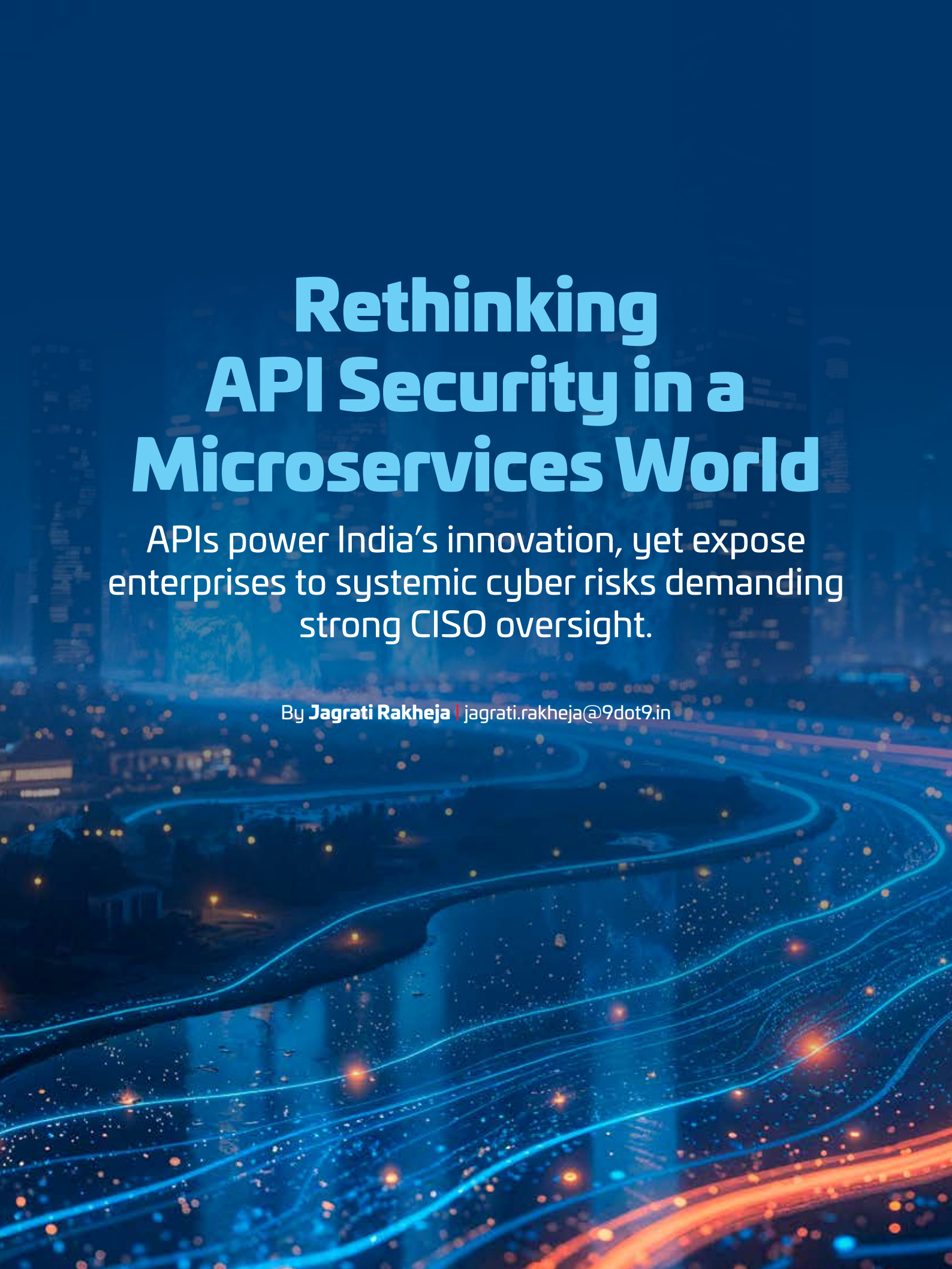
Safety guidelines for pilgrims

The company urges booking only via the official IRCTC HeliYatra Portal (heliyatra.irctc.co.in) and verifying URLs before making payments. Devotees should be cautious with social media offers, avoid sharing sensitive credentials, and only download apps from trusted stores.

"These scams exploit both faith and urgency, leaving pilgrims financially and emotionally distressed," Quick Heal said in a statement.

Quick Heal also recommends reporting suspicious profiles and ads immediately and installing security tools like AntiFraud.AI to safeguard the booking process and travel period.

By highlighting this threat, the company aims to prevent further financial and emotional harm during one of India's most significant pilgrimage seasons. ■



Rethinking API Security in a Microservices World

APIs power India's innovation, yet expose enterprises to systemic cyber risks demanding strong CISO oversight.

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

ON A Monday morning in Mumbai's bustling Santa Cruz corporate hub, Deepak Bhosale walks into the Asian Paints office carrying a rare mix of accomplishment and vigilance. As Associate Vice President of IT, he has steered the 80-year-old paint giant into a digital-first enterprise where technology underpins every service and customer interaction. Today, Asian Paints orchestrates a vast ecosystem that extends far beyond paint—spanning kitchens, bathrooms, and home improvement solutions—all seamlessly connected through a web of APIs that link partners, suppliers, and end-users.

This transformation is emblematic of India's sweeping digital ambitions as the nation races towards a projected $1 trillion digital economy by 2025. Yet, beneath this undeniable progress lies a persistent challenge: APIs—the very arteries driving innovation—have also become vulnerable gateways for cyber attacks. "On one hand, businesses want fearless innovation; on the other, security cannot be compromised," Bhosale reflects. His words capture the essence of a dilemma facing every CIO and CISO today—the daily balancing act between enabling rapid technological advances and safeguarding critical data assets.

APIs have quietly emerged as the highways of India's digital economy. They shuttle data between mobile apps, cloud services, and connected devices, making platforms more agile and consumer experiences more seamless. But like all roads, the more they proliferate, the greater the opportunity for breakdowns, accidents, and targeted attacks. API security incidents in India have more than doubled in the past year, a stark indicator of the risks accompanying explosive growth. Most corporate decision makers remain unaware of the sheer number of APIs—many operating outside traditional security perimeters—through which their businesses now communicate.

"Most API security tools are not mature enough today—they don't give a complete east-west, north-south view in a single pane. That's why maintaining an inventory of active APIs and eliminating zombie APIs is critical."

Mayank Mehta
CISO, Magma General Insurance

Numbers from industry research paint a concerning picture: nearly 80% of API breaches in India stem from weak authentication, an avoidable flaw with potentially devastating financial, reputational, and regulatory repercussions. Akamai's recent study provides further context—85% of Asia-Pacific businesses reported at least one API breach last year, with each incident costing over US $580,000 on average. Even more troubling is the perceptual gap: while most C-suite leaders believe they have

full oversight of their API landscape, less than half of security teams share that confidence; only a small fraction feel capable of identifying APIs that actually expose sensitive data.

This disconnect magnifies enterprise exposure and underscores the urgent need for purpose-built API security, not patchwork solutions. Many organizations still rely on application support and monitoring tools for protection, but these are mere band-aids—not comprehensive fortifications. As the adoption of microservices, cloud, and edge architectures continues to accelerate, CISOs across India are awakening to a new reality: API security must be embedded from the outset, woven into the design and fabric of every digital project.

The Microservices Revolution

The shift from monolithic enterprise applications to microservices-based architectures has rewritten both business models and security strategies. Each microservice carries its own APIs, and when multiplied across internal, external, and third-party services, the result is an exponential surge in vulnerability points. This proliferation spawns shadow APIs that escape documentation and governance, zombie APIs left un-retired, and inconsistent security practices around authentication and encryption. Complicating matters, agile development cycles mean rapid, frequent updates—sometimes at the expense of robust security vetting.

Integration with third-party platforms further compounds risks, making security contingent on external standards that may not align with the enterprise's own policies. The talent crunch in API security, along with cultural friction between developer speed and security discipline, and nascent governance frameworks, presents additional hurdles for CISOs. Thus, the challenge for security leaders encompasses not just technical threats but also strategic and operational dimensions that shape overall business resilience.

"APIs are now the primary highways for enterprise data—and without purpose-built controls, they risk becoming open shortcuts for attackers."

Why Traditional Security Falls Short

Traditional security tools were designed for simpler times, when applications sat behind walls with tightly controlled entry points. APIs have shattered that assumption, routing data across internal networks, third-party platforms, and customer applications in a continuous and often invisible flow. Traffic rarely passes through perimeter defenses such as firewalls, leaving gaps that criminals are quick to exploit.

Shadow and zombie APIs exemplify these risks. In rapidly evolving projects, developers may launch APIs without proper documentation, or neglect to shut down obsolete ones—creating endpoints that often lack basic authentication and monitoring. For example, a banking app upgrade might leave an old balance-check API running unnoticed, vulnerable to exploitation. Third-party dependencies extend risk beyond direct control; an insurer may secure its claims platform, but if an aggregator lacks encryption, data in transit can be intercepted. The fast pace and frequent updates of DevOps can also lead to authentication oversights, potentially exposing user information with just one missed detail.

The harsh lesson: Security methods built for stable environments falter in the API era, where boundaries are blurred, change is constant, and the attack surface is sprawling. APIs are now not just business enablers—they are potential open shortcuts for attackers, demanding a new breed of security strategy.

As Mayank Mehta, CISO at Magma General Insurance notes, "Most API security tools are not mature enough today—they don't give a complete

"We built a platform of innovation that exposed business as a service, underpinned by secure APIs. But since we expose huge amounts of data externally, security at both process and people level has become a huge focus in the last 5–6 years."

Deepak Bhosale
Associate Vice President–IT,
Asian Paints

east-west, north-south view in a single pane. That's why maintaining an inventory of active APIs and eliminating zombie APIs is critical.'"

The Hidden Scale of API Attacks

Unlike headline-grabbing malware outbreaks, most API breaches exploit subtle design flaws or simple misconfigurations. Attackers use compromised credentials or legitimate-looking requests to blend in with normal traffic, making detection difficult. These intrusions are often incremental; data is siphoned off slowly from services APIs, financial databases, or HR systems, all while business appears to function normally.

As Uday Deshpande, CISO at Larsen & Toubro, explains, "The biggest problem is weak authentication and authorization. That's why we are adopting Zero Trust principles and AI/ML for anomaly detection in API traffic. Discipline is essential—the earlier you detect, the earlier you mitigate."

To appreciate the scale of today's API security challenge, consider the underlying digital shift. MuleSoft's 2024 Connectivity Benchmark Report finds that the typical large enterprise now operates approximately 900 distinct applications, yet less than one-third are integrated—a coverage gap that enables hundreds of potential exposures. Every smartphone tap, online transaction, or video stream triggers countless API calls. Mobile banking is a vivid example: a balance check may activate APIs for fraud detection, credit review, payments, notifications, and regulatory reporting—all before giving the user feedback. AI-powered services further compound complexity, generating multi-layered API calls across disparate backend platforms.

Gartner's research highlights that 74% of global organizations now use microservices, leaving monolithic platforms behind. This architectural leap creates a "city" of thousands of interconnected APIs, delivering agility at the cost of exponentially multiplying possible entry points for attackers.

While most C-suite leaders in India believe they have full visibility into their APIs, less than half of security teams agree—and only a fraction feel confident about spotting APIs that expose sensitive data.

India's Sectoral Battleground for API Security

India's rapid digital revolution, visible in sectors such as fintech, manufacturing, and healthcare, makes the risks ever more tangible. Consider the Unified Payments Interface (UPI). Each month, over 10 billion payments are completed via APIs linking banks, payment processors, fintech startups, and regulatory agencies. A single compromised API could impact millions of users, prompting RBI to enforce real-time API security standards and robust breach notification protocols.

Similarly, the fintech domain—now valued at $31 billion in 2024—depends almost entirely on APIs for daily operations. Platforms like Razorpay, Paytm, and PhonePe juggle millions of transactions, their interconnectivity creating an extensive attack surface. The Digital Personal Data Protection Act (DPDPA) 2023 mandates not just data privacy but explicit controls at the API layer, including granular consent management and data localization.

"Every day we discover something new on our firewall—APIs insecurely hosted, unpatched, vulnerable, or even exposing sensitive data. Shadow IT makes it worse, with businesses collaborating with third parties without oversight."

Uday Deshpande
CISO, Larsen & Toubro

Manufacturing's embrace of Industry 4.0, typified by Asian Paints' integration of APIs across business and service platforms, opens new avenues for both growth and vulnerability. Healthcare leverages APIs to connect hospitals, diagnostics, and telemedicine, making patient data more accessible—and more exposed—than ever. The sector has witnessed a spike in targeted attacks, pushing providers to upgrade API monitoring and compliance practices.

Sectoral Impact of APIs in India

APIs have become the backbone of India's digital economy, powering everything from payments and identity verification to e-commerce and health records. While they enable rapid innovation and scale, insecure APIs expose critical data and infrastructure to breaches, fraud, and systemic disruption, making their security a national priority.

- **Banking and Financial Services:** With UPI, IMPS, and Aadhaar-enabled payments, India has become the world's most API-driven financial ecosystem. In 2023, CERT-In reported rising cases of API abuse in digital lending apps and unauthorized UPI requests. The RBI has tightened norms around authentication, and the Data Protection Act 2023 creates liability for financial data leakage. The 2024 Finastra incident globally underscores risks, but India's own cases — such as the Paytm Payments Bank compliance issues — show how exposed APIs can disrupt services at scale.
- **Manufacturing and Industrial IoT:** Make in India and Industry 4.0 programs have accelerated IoT adoption, with APIs linking ERP systems, shop-floor robotics, and suppliers. Weak authentication remains common, and CERT-In advisories in 2022 flagged vulnerabilities in exposed OT APIs in energy and steel plants. Compromise of APIs here risks not only IP theft but operational sabotage — a live concern given geopolitical cyber tensions.
- **Healthcare and Pharmaceuticals:** The Ayushman Bharat Digital Mission (ABDM) relies heavily on health data APIs linking hospitals, insurers, and patients. Misconfigured APIs could expose electronic health records (EHRs), which are increasingly traded in underground markets. In 2022, a major Indian pathology lab leak was traced to insecure APIs exposing millions of patient reports. The Digital Information Security in Healthcare Act (DISHA, draft) and DPDP Act highlight the urgency of securing health APIs.
- **Retail and E-Commerce:** APIs drive checkout, delivery, inventory, and payment in India's e-commerce and Q-commerce giants. Vulnerabilities have enabled price manipulation and loyalty-point theft. In 2021, a food delivery platform suffered API abuse that exposed user data, including addresses and order history. With ONDC (Open Network for Digital Commerce), secure APIs are even more critical, as thousands of small sellers connect to national-scale infrastructure.
- **Telecommunications:** Telcos like Jio, Airtel, and Vi expose APIs for billing, KYC, and partner services. SIM-swap fraud, often linked to weak API authorization, remains a rising threat. In 2023, TRAI raised concerns around APIs used in spam/OTP generation and mandated stricter testing of Distributed Ledger Technology (DLT)-based SMS APIs. Outages linked to misconfigured APIs in interconnect billing have shown systemic fragility.
- **Energy and Utilities:** Smart meters and EV charging stations are heavily API-dependent. Insecure APIs can enable energy theft or denial of service in distribution networks. Researchers have demonstrated how EV charging APIs could be manipulated to disrupt availability. With India's Critical Information Infrastructure (CII) framework under NCIIPC, utilities are expected to harden API endpoints as a national security priority.
- **Government and Public Services:** India Stack — with Aadhaar, DigiLocker, and e-Sign APIs — is the most ambitious public digital infrastructure globally. But Aadhaar has repeatedly been in the news for leaks via unsecured APIs of third-party service providers. The new DPDP Act 2023 imposes penalties on entities failing to secure APIs while handling citizen data. Several state-level e-governance platforms have also suffered scraping and brute-force API attacks.
- **Media and Entertainment:** OTT platforms like Hotstar, SonyLIV, and JioCinema rely on APIs for streaming, subscriptions, and ad delivery. Credential stuffing on login APIs is a frequent risk, with breached accounts resold on darknet forums. In 2023, a gaming API exposure led to leaks of personal data from over 1.5 million Indian users. Regulatory focus is growing, with MeitY examining consumer protection in digital entertainment ecosystems.
- **Transportation and Logistics:** From IRCTC's ticketing APIs to ride-hailing apps like Ola and Uber, APIs underpin India's mobility sector. In 2022, a Bengaluru-based bus ticketing aggregator suffered a breach via poorly secured booking APIs, exposing travel details of millions. Logistics APIs, including those in e-commerce supply chains, are highly targeted — disruptions cascade into national commerce and trade flow. DPDP compliance will require securing these APIs against unauthorized access.

Three Pillars of Next-Gen Security

Today, Indian CISOs recognize that security cannot be an afterthought. The most forward-looking organizations use three robust pillars to secure their APIs:

1. AI-Powered Behavioral Analysis:

Emerging threats often hide in normal traffic. AI tools are now indispensable—learning typical patterns, flagging unexpected deviations, and continually updating to reflect business changes. "AI/ML tools are helping us detect anomalies where traditional methods throw too many false positives," notes Deshpande.

2. Zero Trust by Design:
Security must assume "trust nothing, verify everything." Zero Trust models enforce authentication and least-privilege access for every session and transaction, starting with the most exposed APIs and expanding inward.

3. Security Across the API Lifecycle:
APIs evolve constantly; security must start with design, continue through deployment, and include post-incident review. Shift-left approaches bake in prevention early, while ongoing monitoring and governance maintain effective resilience. "Security at both process and people level has become a huge focus in the last 5–6 years," says Bhosale.

Turning Principles into Practice: A Roadmap

For CISOs, putting concepts into action means structuring security maturity with clear, phased steps:

Phase 1: Discovery & Foundation (Months 1–3): Map every API, including undocumented and legacy endpoints, and institute baseline controls like encryption and rate limiting.

Phase 2: Integration & Governance (Months 4–8): Deploy secure gateways, run security tests in CI/CD pipelines, enforce MFA and OAuth, and align with DPDPA governance.

Phase 3: Advanced Capabilities (Months 9–18): Implement AI anomaly detection, refine incident response, and ensure continuous compliance with board-level visibility.

This approach enables organizations to quickly address exposures while building lasting resilience—crucial in a landscape where threats evolve as quickly as business models.

Delay Costs, Leadership Pays

The financial penalties for API-related outages and security breaches in India are staggering. A single hour of downtime or exposure can cost an enterprise up to ₹1 crore, while serious violations under the Digital Personal Data Protection Act (DPDPA) could attract fines as high as ₹250 crore. These aren't just hypothetical figures; recent incidents across banking, manufacturing, and healthcare have led to swift regulatory scrutiny and significant business disruption, with ripple effects felt in market reputation and customer trust.

But the consequences extend far beyond the immediate monetary impact. Cyberattacks often trigger mandatory public disclosures, potentially eroding years of brand equity in just days. Regulatory investigations can stall critical business projects and delay product rollouts, directly impeding an organization's ambition to innovate rapidly or scale up in a competitive market. Moreover, loss of sensitive customer data can see companies battling legal claims, litigation, and long-term trust deficits in their stakeholder communities.

On the flip side, organizations that decide to future-proof their API security infrastructure reap measurable rewards. Robust protection practices translate into 40% faster time-to-market, a 60% reduction in development delays, and demonstrably stronger customer relationships built on transparency and reliability. Such firms not only avoid costly breaches and penalties—they also become models for industry best practice, attracting business partnerships and regulatory goodwill vital for long-term growth and digital leadership.

What's Next?

In conclusion, as India's digital economy accelerates on the back of APIs, securing them is no longer a narrow technical task—it is a leadership mandate. Tools alone are not enough; enterprises need disciplined governance, continuous API lifecycle visibility, and a culture where developers and security teams work seamlessly together. From ecosystem risks to zombie APIs and shadow IT, the threats are real and rising. Yet, with strong hygiene, shift-left practices, and AI-enabled monitoring, CISOs can transform APIs from the weakest link into the resilient foundation of innovation. ■

The API Security Maturity Path

Assess where your enterprise sits today—and where regulators, customers, and partners expect you to be tomorrow.

- **Level 1 – Reactive:** APIs monitored only after incidents. No central inventory.
- **Level 2 – Defined:** API gateways deployed, partial inventory exists.
- **Level 3 – Integrated:** APIs covered by DevSecOps testing and runtime controls.
- **Level 4 – Proactive:** APIs monitored only after incidents. No central inventory.
- **Level 5 – Adaptive:** AI-driven anomaly detection, automated remediation, API security embedded in enterprise risk DNA.

Emerging API Risks

What feels like a niche API concern today could be a headline risk tomorrow.

- **AI Workloads:** APIs serving AI/ML models could be poisoned or exploited.
- **5G & IoT:** API will underpin billions of devices in critical infrastructure.
- **API Marketplaces:** Monetization platforms become new hunting grounds.
- **Autonomous Attack Bots:** APIs will face AI-driven adversaries; human monitoring won't scale.

Cybersecurity in the AI era: Protecting the protectors

AI's power in cybersecurity comes with vulnerabilities, demanding strong safeguards to protect the protectors.

By **Dipesh Patel**

THE USE of AI in cybersecurity offers immense advantages for rapid threat detection, faster response, and improved resilience. However, it also introduces critical vulnerabilities. AI tools, while acting as powerful defenders, have paradoxically become attractive targets for sophisticated adversaries. This dual nature is especially evident in online verification and security processes, where AI's innovative capabilities collide with the potential for manipulation.

Unlike traditional systems, AI consolidates sensitive data and decision-making, making it a prime target. For CISOs, the challenge is "Protecting the Protectors" by securing AI itself. Malicious actors exploiting AI algorithms can compromise its benefits, leading to severe consequences.

Addressing these risks requires robust protection strategies, adaptive safeguards, and comprehensive frameworks to ensure trust and preserve AI's true potential.

Got it! Here's the refined 150-word version in points while keeping the original style and context intact:

Latest irends / impact of AI on Modern Security (protector)

Smarter threat detection:

- AI-driven machine learning surpasses traditional rule-based systems, uncovering subtle and complex threat patterns through advanced anomaly detection.
- AI analyses network traffic and user behaviour to identify deviations that may indicate potential attacks.
- AI examines malware code and behaviour to detect novel and unknown threats.
- AI scrutinizes emails and websites to uncover sophisticated phishing attempts.

Proactive defence:

- AI's predictive analytics enhances threat intelligence, enabling organizations to anticipate and prevent attacks.
- AI reduces false positives, delivering accurate and timely alerts on emerging threats.

Enhanced access control:

- AI strengthens identity and access management through biometric and behavioural analysis..

Faster incident response:

- AI automates incident response, ensuring rapid containment and mitigation.
- AI prioritizes incidents and provides actionable insights, improving response efficiency.

Streamlined security operations:

- AI-powered copilots accelerate detection, investigation, and response.
- AI processes large datasets to forecast potential attacks and anomalies.
- AI automates routine tasks, freeing analysts to focus on complex issues.

Best practices for securing AI systems (protecting the protector):

Data centric security:

- Implement robust data encryption (at rest and in transit).
- Enforce strict access controls (RBAC, least privilege).
- Utilize data anonymization and differential privacy techniques.
- Establish clear data lineage and provenance tracking.

Model security:

- Develop adversarial robustness through adversarial training.
- Ensure model integrity with digital signatures and hashing.
- Implement explainable AI (XAI) for transparency and bias detection.

Dipesh Patel
DVP- Unit Head - Cloud Network and Security Engineering HDFC Bank

- Establish continuous model monitoring and auditing.

System and infrastructure security:

- Secure cloud and on-premises infrastructure with firewalls and intrusion detection.
- Implement secure API gateways with authentication and authorization.
- Conduct regular vulnerability scanning and penetration testing.
- Adopt secure coding practices and input/output validation.

Governance and ethical AI:

- Develop comprehensive AI ethics guidelines and policies.
- Establish a responsible AI development framework.
- Implement bias detection and mitigation strategies.
- Maintain human oversight and control.
- Create an incident response plan for AI security breaches..

GenAI and agentic AI specific security:

- Implement robust prompt injection defences.
- Address model hallucinations through grounding and verification.
- Protect against data poisoning and copyright infringement.
- Monitor for and mitigate misinformation and disinformation.
- Prompt Engineering best practices and guardrails.
- Implement the principle of least privilege for AI agents.
- Monitor agent behaviour for anomalies and suspicious activities
- Maintain detailed audit trails of agent actions and interactions
- Deploy AI agents in sandboxed environments to limit their access to sensitive systems.

CISO's practical guide with AI security - (protecting the protector)

1. Establish an AI security framework:

2. AI security posture management (ASPM)

- **Asset inventory:** Create a comprehensive inventory of all AI assets, including models, data, infrastructure, and applications.
- **Risk assessments:** Conduct regular AI-specific risk assessments, focusing on adversarial attacks, data poisoning, bias, and ethical concerns.
- Use threat modelling techniques to identify potential attack vectors.
- **Continuous monitoring:** Implement continuous monitoring of AI security controls and model performance.
- Integrate AI security monitoring into existing security information and event management (SIEM) systems.
- **Policy enforcement:** Automate policy enforcement using AI security tools and platforms.

3. AI runtime protection:

- **Anomaly detectio:** Deploy anomaly detection systems to identify unusual AI model behaviour and potential attacks.

Leadership	Focus	Key aspects covered
NIST AI Risk Management Framework (AI RMF)	Managing risks associated with AI development, deployment, and use	Govern, Map, Measure, Manage (fairness, transparency, security, privacy)
ISO 42001	Establishing, implementing, maintaining, and continuously improving an Artificial Intelligence Management System (AIMS)	Policies, procedures, and controls to address AI risks across the organization
OWASP Top 10 LLM Security Risks	Security vulnerabilities specific to Large Language Models (LLMs)	Prompt Injection, Insecure Output Handling, Training Data Poisoning, Model Denial of Service, Supply Chain Vulnerabilities, Sensitive Information Disclosure, Insecure Plugin Design, Excessive Agency, Overreliance, Model Theft
Google's Secure AI Framework (SAIF)	Enhancing security across AI operations	Securing AI algorithms and their operational environment, encryption, secure user access, anomaly detection
ENISA's Framework for AI Cybersecurity Practices (FAICP)	AI good cybersecurity practices necessary for securing ICT infrastructures and hosted AI	Basic cybersecurity relevant to AI, AI-specific cybersecurity, sector-specific cybersecurity for AI
DHS's Roles and	Safe and secure development and	Roles and responsibilities for cloud providers, AI developers,
Responsibilities Framework for AI in Critical Infrastructur	Deployment of AI in critical infrastructure	Infrastructure owners/ operators, civil society, and the public sector
Internal Frameworks	Internal to Organization	Develop internal AI security policies and procedures that align with industry best practices and regulatory requirements

- **Input/output validation:** Implement real-time input and output.
- **Containerization:** Use containerization technologies (e.g., Docker, Kubernetes) to isolate and secure AI models.
- **API security:** Secure AI APIs with authentication, authorization, and rate limiting.

4. AI vulnerability and penetration testing: :

- **AI-specific testing:** Conduct penetration testing that specifically targets AI vulnerabilities, such as adversarial attacks, model inversion, and data poisoning.
- **Vulnerability scanning:** Use specialized AI vulnerability scanning tools to identify known vulnerabilities in AI libraries and frameworks.
- **Red teaming:** Conduct red team exercises to simulate real-world AI attacks and test the effectiveness of security controls.
- **Prompt injection testing:** Ensure that all genAI systems are tested for prompt injection vulnerabilities.

5. Governance and ethical AI:

- **AI ethics committee:** Establish an AI ethics committee to oversee the development and deployment of AI systems.
- **Bias mitigation:** Implement bias detection and mitigation techniques throughout the AI lifecycle.
- **Transparency and explainability:** Promote transparency and explainability in AI decision-making.
- **Human oversight:** Maintain human oversight of critical AI systems.

6. Vendor risk management:

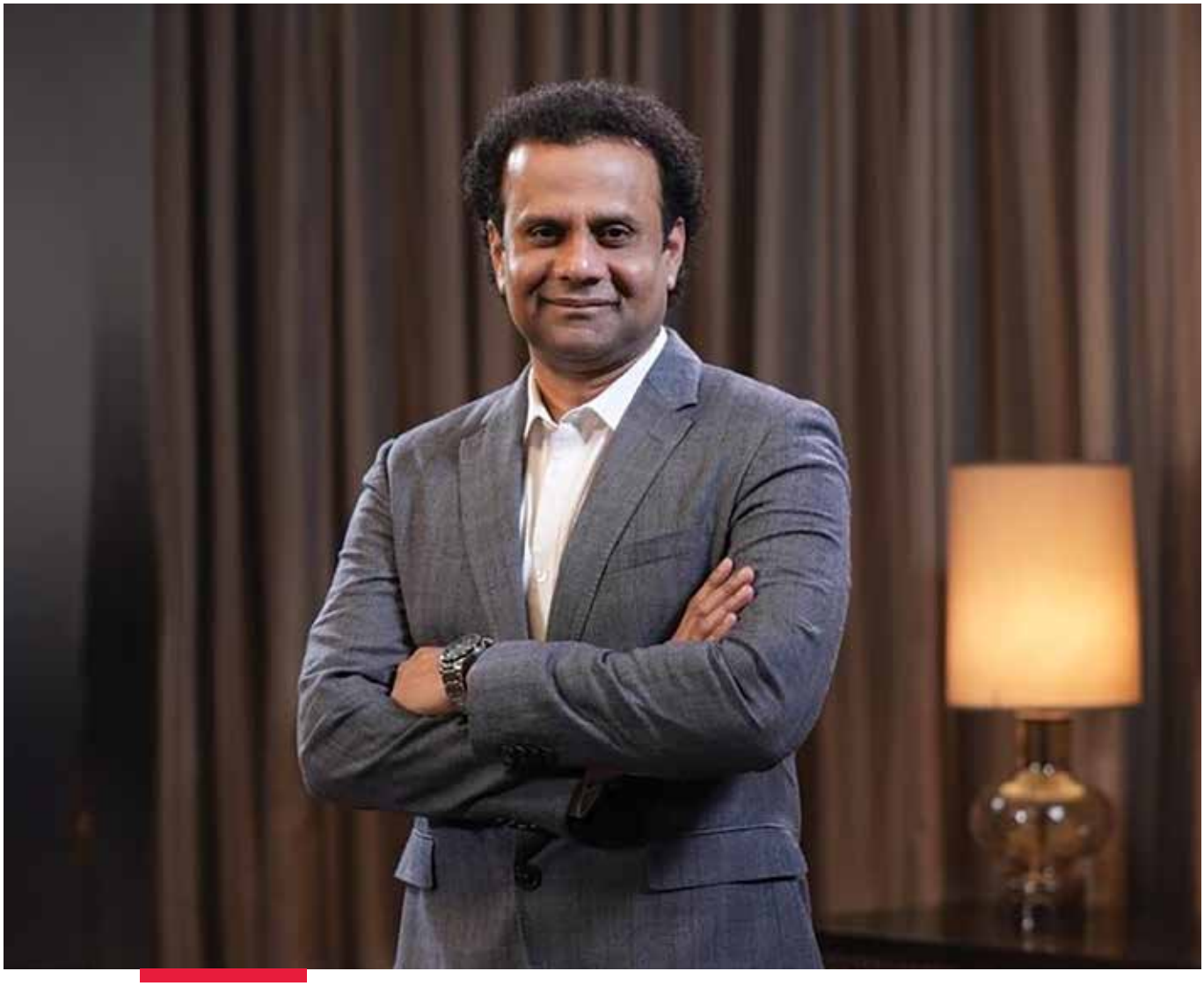
- **Due diligence:** Conduct thorough due diligence on AI vendors, including security assessments and audits.
- **Contractual agreements:** Ensure that vendor contracts include strong security and privacy provisions.
- **Data sharing agreements:** Establish clear data sharing agreements with AI vendors.

7. Continuous improvement:

- **Threat intelligence:** Stay up-to-date on emerging AI security threats and vulnerabilities.
- **Training and awareness:** Provide regular AI security training and awareness programs for employees.
- **Incident response:** Develop and maintain an AI-specific incident response plan.

Conclusion

The AI era demands a paradigm shift in cybersecurity. As AI powers both attack and defence, protecting these systems is critical. Fortifying models, ensuring data integrity, and establishing ethical frameworks require continuous monitoring, adaptive measures, and AI-driven tools—safeguarding not just technology, but trust in an AI-dependent society.■



From crisis to constant: How CISOs must adapt to AI-powered cyber threats

Fortinet's Vishak Raman urges CISOs to adopt AI-driven, integrated platforms for predictive, resilient cyber defense.

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

AS ARTIFICIAL INTELLIGENCE transforms both cyber offense and defense, Chief Information Security Officers across India and Southeast Asia find themselves at the epicenter of an unprecedented security evolution. The traditional reactive approach to cybersecurity is rapidly becoming obsolete, replaced by an urgent need for predictive, intelligence-driven strategies that can counter AI-powered attacks, such as deepfakes, polymorphic malware, and automated reconnaissance.

At the forefront of this transformation is Vishak Raman, Vice President of Sales for India, SAARC, SEA & ANZ at Fortinet, who brings a unique perspective on navigating hybrid cloud environments, Zero Trust architectures, and evolving regulatory frameworks, such as India's Digital Personal Data Protection Act.

In this exclusive interview, Raman shares critical insights on the most pressing cybersecurity challenges facing modern enterprises, from managing fragmented security tools across multi-cloud environments to transforming Security Operations Centers through intelligent automation. With cyber threats becoming increasingly covert and coordinated, his vision for platform-based security solutions offers a roadmap for organizations seeking to build adaptive, resilient defenses in an era where cyber risk has evolved from crisis to constant.

CISO Forum: How is Fortinet leveraging artificial intelligence to proactively detect and mitigate emerging threats such as deepfakes and AI-driven cyberattacks?

Vishak Raman: AI is no longer just a capability — it's becoming foundational to both cyber offense and defence. At Fortinet, we've embedded AI across our platform to help customers detect, prioritize, and respond to threats in real time. This includes stopping AI-powered attacks, such as deepfake-driven fraud, polymorphic malware, and automated reconnaissance, which are growing at an alarming rate.

Our FortiAI capabilities are built into the Security Fabric, so instead of relying on isolated tools, we offer an integrated approach that spans prevention, detection, response, and learning. Whether it's tracing the origins of an attack, reducing false positives, or strengthening API and SaaS security, our AI works across the environment to improve protection and resilience.

CISO Forum: What are the most critical cybersecurity challenges facing CISOs in managing hybrid and multi-cloud environments today?

Vishak Raman: Hybrid and multi-cloud environments offer agility, but they also introduce complexity, and that's where the biggest cybersecurity challenges emerge. CISOs are grappling with fragmented security controls across different cloud providers, inconsistent visibility, and the operational burden of managing multiple tools that don't speak to each other.

Misconfigurations remain a top concern, often resulting in the unintended exposure of critical assets. Meanwhile, the speed at which cloud services are spun up — sometimes outside of IT's direct control — makes governance even harder. Add to that a flood of security alerts from disconnected systems, and security teams quickly face burnout and blind spots.

What's needed is a platform approach that consolidates these fragmented tools and provides unified visibility and control across all environments. Fortinet's cloud-native platform brings security, networking, and AI-powered intelligence together — helping organizations detect, prioritize, and respond to threats faster, while keeping pace with the scale and speed of modern development cycles.

CISO Forum: In what ways can CISOs transition from reactive security practices to a predictive, intelligence-driven approach to threat management?

Vishak Raman: To move from reactive to predictive security, CISOs need to shift from siloed point solutions to an integrated platform strategy — one that's built on AI and automation. The volume, speed, and sophistication of today's threats make it impossible for manual processes or disconnected tools to keep up.

By consolidating their security stack and embracing AI-powered solutions that work across the network, endpoint, cloud, and identity layers, CISOs can detect anomalies earlier, reduce false positives, and respond faster. The goal is to build a security infrastructure that not only detects more but also learns and adapts in real-time, turning intelligence into immediate action. Convergence and automation enable lean teams to stay ahead of complex, multi-vector threats.

CISO Forum: How mature is the adoption of Zero Trust architectures across India and Southeast Asia, and what common pitfalls should security leaders be aware of?

Vishak Raman: Zero-trust adoption is accelerating, especially with hybrid work and distributed applications becoming the norm. But maturity levels vary. Many organizations underestimate the complexity of enforcing Zero Trust across cloud, on-prem, and SaaS environments — or try to implement it piecemeal with disparate tools.

The key is integration. At Fortinet,

"AI is no longer just a capability — it's becoming foundational to both cyber offense and defence."

we're helping organizations converge networking, access, and security into one fabric, making it easier to enforce least-privilege policies consistently. Without this convergence, Zero Trust can become a buzzword rather than a functional security posture.

CISO Forum: With increasing regulatory requirements such as India's DPDP Act, how can CISOs effectively align their security strategies with evolving compliance demands?

Vishak Raman: Regulations are a strategic opportunity to strengthen the resilience of individual organizations and the entire industry. India's DPDP Act underscores the importance of data stewardship, risk management, and visibility across digital operations. For CISOs, this is an opportunity to align compliance with broader resilience goals.

We see organizations increasingly using compliance as a springboard to modernize processes, from automating data protection to tightening identity access controls. Fortinet's integrated platform helps simplify audit readiness while embedding security into business workflows, ensuring teams stay both secure and compliant.

CISO Forum: What role does automation play in transforming Security Operations Centres (SOCs), and how should organizations balance this with the need for skilled human analysts?

Vishak Raman: Automation plays a critical role in modernizing SOCs — not by replacing human analysts, but by helping them scale. Most organizations today face a dual challenge: a growing volume of alerts and a shortage of skilled cybersecurity talent. In India, for example, only 13% of IT staff are focused on cybersecurity, and just 6% of organizations have specialized SOC teams.

That's where automation becomes essential. Fortinet's AI-powered SecOps capabilities — including automated threat detection, triage, and response — have helped reduce incident response times by up to 99%, according to ESG's economic validation. One customer reduced time spent on incidents by over 200 person-hours per week, while improving accuracy and threat coverage.

This doesn't eliminate the need for skilled analysts — instead, it allows them to focus on high-value investigations, threat hunting, and strategic decision-making. The future SOC is not just about more tools or more people — it's about smarter, integrated operations that combine human expertise with machine-driven speed and precision.

CISO Forum: Looking ahead to 2025, what key priorities should

"Hybrid and multi-cloud environments offer agility, but they also introduce complexity — and that's where the biggest cybersecurity challenges emerge."

CISOs focus on to defend against persistent and multi-vector cyber threats?

Vishak Raman: In 2025, CISOs will need to rethink their priorities as cyber threats become more covert, complex, and coordinated. The attack surface is expanding rapidly, with AI-generated phishing, supply chain compromises, cloud misconfigurations, and IT/OT convergence all presenting significant risk. These aren't isolated events anymore; they're part of multi-vector campaigns designed to bypass siloed defences and exploit blind spots across infrastructure layers.

To stay ahead, CISOs must prioritize reducing fragmentation and accelerating detection and response. That starts with consolidating vendors to simplify operations and close integration gaps. AI-powered platforms that can correlate signals across endpoints, networks, identities, and cloud workloads are becoming essential. Identity security, SASE adoption, and cloud-native application protection are all emerging as strategic investment areas.

Additionally, visibility into OT environments is becoming increasingly crucial. As cyberattacks extend into physical systems, organizations need tools that can monitor and secure industrial networks with the same rigor as IT environments. The overarching goal is to build an adaptive, intelligence-driven security posture that's built for scale, speed, and resilience — because in today's environment, cyber risk is no longer a crisis; it's a constant.

CISO Forum: How does Fortinet's acquisition of Israeli SaaS security firm Suridata enhance its AI-driven threat management capabilities, and what implications does this have for the integration of advanced SaaS security solutions within the Fortinet Security Fabric?

Vishak Raman: Suridata strengthens our Unified SASE portfolio by providing deep visibility and control over SaaS applications, which remain a significant blind spot for many organizations. As more businesses adopt SaaS-first strategies, SSPM becomes essential for managing misconfigurations, enforcing policies, and detecting risks at scale.

Suridata's AI-driven SaaS Security Posture Management integrates seamlessly into the Fortinet Security Fabric, enhancing our CASB capabilities and ensuring consistent protection across users, apps, and data. This is a strategic step in our commitment to deliver end-to-end, platform-based security for today's hybrid enterprises. ■

Securing the industrial backbone: OT cyber security matures in 2025

OT cybersecurity is maturing, with executive leadership driving fewer intrusions and better resilience against advanced threats.

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

IMAGINE A world where a factory floor halts not due to faulty machinery, but because of a malicious code slipped into a vulnerable network. That world is now. Operational Technology (OT)—the backbone of industries such as manufacturing, utilities, and logistics—is under siege from sophisticated cyber threats. Yet, according to Fortinet's 2025 State of OT and Cybersecurity Report, there is hope. Organizations are maturing. Strategies are evolving. And crucially, responsibility is shifting to the top.

Cybersecurity goes to the C-Suite

The report reveals a significant trend: OT security is no longer just an IT issue—it's a boardroom priority. In 2025, over half (52%) of organizations have placed OT cybersecurity under the CISO, up from a mere 16% in 2022. This shift reflects a growing awareness of OT's strategic importance and the potential consequences of cyber incidents.

Maturity brings results

Cyber maturity is rising. Nearly half of all respondents now rate their cybersecurity processes at Level 4, where feedback loops, threat intelligence, and incident response are continuously optimized. Intrusions are declining too. In 2025, 52% of organizations reported zero intrusions, compared to just 6% in 2022. Mature organizations that utilize advanced controls experience significantly fewer incidents compared to those that lag in this area.

Threats still loom large

While progress is evident, so are the dangers. Cyberattacks remain a persistent threat, especially for less mature organizations. The manufacturing sector, the most targeted, continues to face risks from ransomware and malware. Additionally, AI-powered attacks are making phishing and malware detection and prevention more challenging.

Best practices that work

Organizations making headway are embracing proven strategies:

- **Segmentation and Visibility:** Creating network zones to limit the spread of threats.
- **SOT-Specific Threat Intelligence:** Enabling faster detection of sector-specific exploits..
- **Platform-Based Security:** Simplifying architecture while improving response.
- **Vendor Consolidation:** 78% now work with just 1–4 OT vendors, enhancing control and reducing cost.
- **Executive-Level Incident Reporting:** More firms are transitioning from routine compliance reporting to comprehensive security assessments, such as penetration tests.

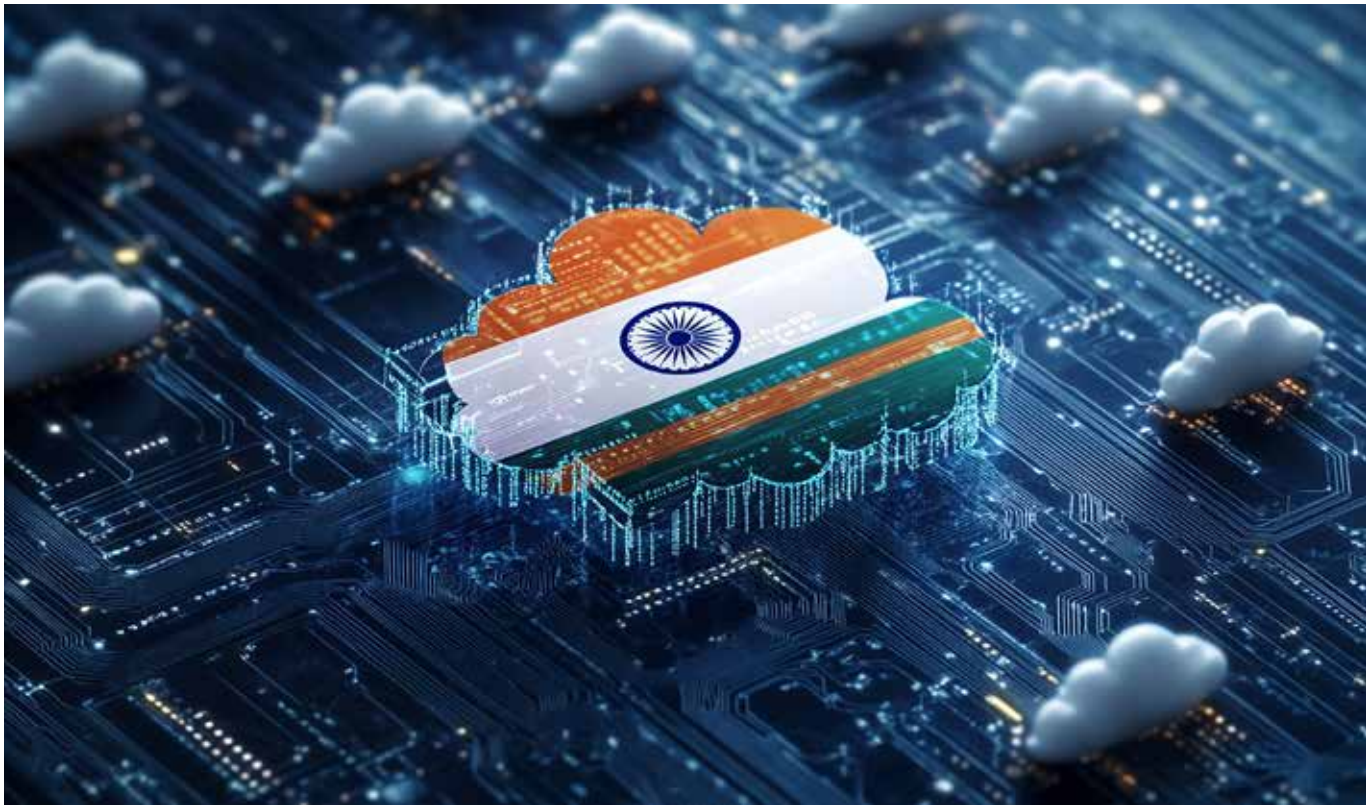
Security maturity is rising—and it's reducing intrusions.

A safer future hinges on strategy

Despite the aging infrastructure—most OT systems are 6–10 years old—companies are investing in modernization and virtual patching. With 66% of organizations expecting tighter regulations within five years, proactive security planning is no longer optional.

The message from Fortinet's global survey of 550+ OT professionals is clear: cybersecurity maturity pays off. As the digital-physical boundary fades, securing the operational core of modern enterprises has never been more urgent—or more achievable. ■

India's cybersecurity faces rising AI threats and cloud risks



India faces a surge in sophisticated cyber threats, demanding AI-driven defenses and urgent cloud, sectoral, and behavioral security upgrades.

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

IN AN era of rapid digital growth, the India Cyber Threat Report 2025, jointly published by the Data Security Council of India (DSCI) and Seqrite, sheds light on the escalating threat landscape, urging organizations to reassess their cybersecurity strategies.

A surge in cyber threats

India witnessed over 369 million malware detections across 8.44 million endpoints, averaging 702 threats per minute. These staggering numbers indicate that attacks are not only increasing in volume but also becoming more sophisticated. Major cities, such as Surat, Bengaluru, and Hyderabad, are particularly vulnerable, with Tier 2 and Tier 3 cities also experiencing a sharp rise in cyber incidents.

Top targets: Healthcare, BFSI, and hospitality

The healthcare sector emerged as the most attacked, accounting for 21.82% of all malware detections. BFSI (17.38%) and hospitality (19.57%) also faced a high volume of threats. These industries store sensitive personal and financial data, making them attractive targets for cybercriminals.

The cloud is under fire

With 62% of all malware detections occurring in cloud environments, cloud platforms have become the new battleground. The report warns that misconfigured cloud settings and insecure APIs are leading causes of breaches. As more businesses move to the cloud, security gaps need immediate attention.

AI: Double-edged sword

AI-powered malware is on the rise. Generative AI tools are enabling attackers to craft more sophisticated phishing emails, impersonate individuals, and circumvent traditional security systems. However, the same AI technologies are being used by defenders to enhance behavior-based detection, which has increased from 12.5% to 14.5% in one year, helping to identify threats that evade signature-based systems.

Malware breakdown: Trojans and ransomware dominate

Trojans remain the most detected malware type (43.25%), followed by infectors and worms. Ransomware, although accounting for only 0.3% of total detections, remains highly damaging. Attackers use these to encrypt data and demand a ransom, resulting in significant operational and financial losses.

Cybersecurity is not just an IT issue—it's a boardroom priority impacting business continuity and reputation.

WhatsApp and APK scams: A growing concern

One alarming trend is the rise of fake APK files sent via WhatsApp, often disguised as messages from government departments or banks. A family of malware called RewardSteal tricks users into accepting offers such as subsidies or KYC updates, then silently steals their financial data and personal information.

Hacktivism and geopolitical threats

Geopolitical tensions—such as the Russia-Ukraine war—have influenced an increase in state-sponsored attacks. Groups like Anon Black Flag Indonesia and The Anonymous Bangladesh were responsible for thousands of hacktivist attacks targeting Indian infrastructure and institutions.

Recommendations for a safer digital future

The report recommends investing in behavioral detection tools, AI-based security platforms, and robust cloud protection strategies. Regular updates, employee training, and industry collaboration are essential. It also emphasizes that cybersecurity is not just an IT issue—it's a boardroom priority impacting business continuity and reputation.

Conclusion

As India's digital economy grows, so does its attack surface. The report calls for a unified, adaptive, and proactive approach to cybersecurity—one that's grounded in technology, awareness, and continuous improvement. ■

Cloud misconfigurations put sensitive data at risk, 2025 report warns

Cloud misconfigurations expose sensitive data and secrets; security must become a core business priority, not an afterthought.

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

IMAGINE LEAVING your house keys in a public parking lot, your wallet on a restaurant table, and your passport in a library book. That's what many organizations are doing with their cloud data right now.

The latest Tenable Cloud Security Risk Report for 2025 has unveiled some eye-opening truths about how companies are managing their cloud environments. While the digital transformation has brought incredible benefits, it has also created new vulnerabilities that many organizations haven't yet fully grasped.

The shocking truth about public data

Here's a statistic that should make every IT professional pause: 9% of publicly accessible cloud storage contains sensitive data. That means nearly 1 in 10 public storage resources analyzed held confidential or restricted information that anyone on the internet could access.

Even more alarming? Of that sensitive data found in public locations, 97% was classified as either restricted or confidential—the highest risk categories. This isn't just about minor privacy concerns; we're talking about data that could cause severe legal, financial, or reputational damage if it falls into the wrong hands.

Secrets are scattered everywhere

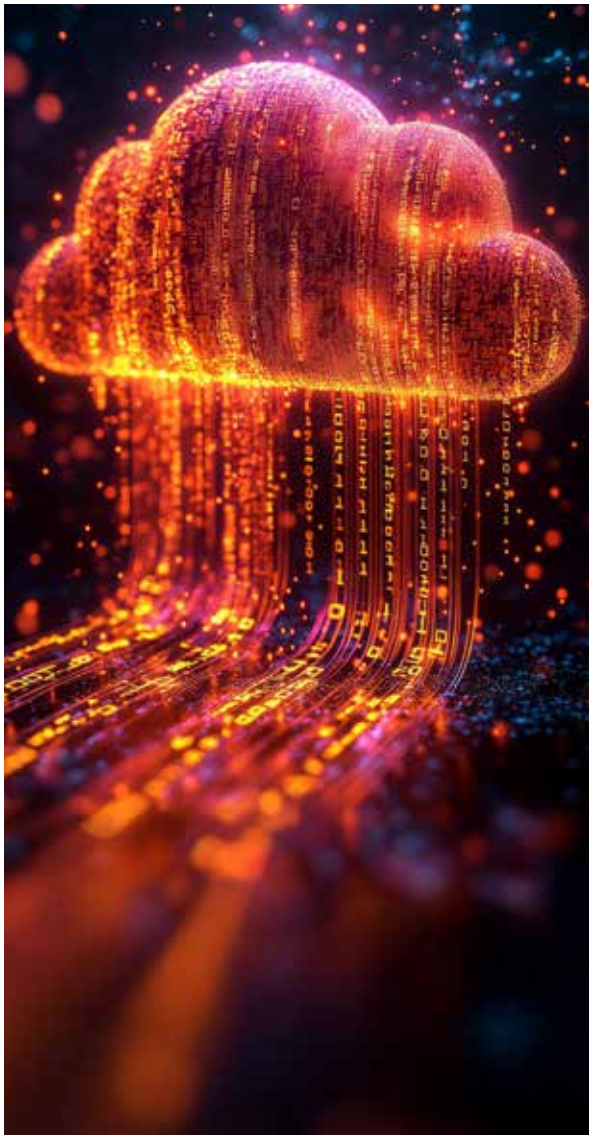
The report reveals another troubling trend: secrets, such as passwords, API keys, and access tokens, are being stored in insecure locations. Over half of organizations using Amazon Web Services have at least one secret embedded in their container configurations, while 52% of Google Cloud users have similar issues.

Perhaps most concerning is that 3.5% of AWS EC2 instances—one of the most widely used cloud services—contain secrets in their user data. Given EC2's popularity, this small percentage represents a massive security risk across the internet.

Some good news on the horizon

It's not all doom and gloom. The report indicates that organizations are improving in certain areas. The number of "toxic cloud trilogies"—systems that are publicly exposed, critically vulnerable, and highly privileged—dropped from 38% to 29% of organizations.

Additionally, 83% of AWS users have configured identity providers, which is a best practice for managing access to cloud resources.



Organizations need to treat cloud security not as an afterthought, but as a fundamental business priority.

The bottom line

As artificial intelligence and cloud computing continue to expand, the stakes are getting higher. Organizations need to treat cloud security not as an afterthought, but as a fundamental business priority. The convenience of cloud computing shouldn't come at the cost of security.

The message is clear: it's time for organizations to audit their cloud environments, secure their secrets, and ensure sensitive data isn't accidentally left in public view. ■

Why Cyber Resilience Matters More Than Ever?

Tata Motors' CISO Dr. Pawan K Sharma highlights cyber resilience as a strategic advantage, blending global frameworks, agility, and employee awareness.

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

AS CYBERATTACKS become increasingly complex and widespread, modern enterprises must think beyond protection—they must prepare to adapt, respond, and recover in real-time. For Dr. Pawan Sharma, Chief Information Security Officer at Tata Motors, cyber resilience isn't just a technical imperative—it's a business enabler. With a legacy brand operating across global markets and intricate supply chains, Tata Motors requires a security strategy that is both agile and robust.

In this exclusive conversation with CISO Forum, Dr. Sharma shares how the company measures and nurtures cyber resilience by combining global standards, such as NIST and ISO, with hands-on threat intelligence, rapid response systems, and a deeply embedded culture of employee awareness. From managing third-party risks and incident response to transforming human capital into a "human firewall," his approach reflects the maturity and foresight required in today's high-stakes cybersecurity environment. Dr. Sharma's insights offer a rare behind-the-scenes look into how one of India's automotive giants stays secure, prepared, and relentlessly resilient.

CISO Forum: How do you define and measure cyber resilience in your organisation, and what frameworks guide your approach?

Dr. Pawan K Sharma: Cyber resilience is our ability to sustain operations despite cyber threats. It goes beyond prevention and focuses on early detection, timely response, swift recovery, and continuous adaptation to evolving risks. We measure it using key metrics, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), as well as employee awareness indicators, including training completion rates and phishing simulation outcomes. Our approach is guided by global standards, including the NIST Cybersecurity Framework, ISO 27001, and ISO 22301.existing cryptographic algorithms with quantum-safe alternatives without requiring extensive system overhauls.

CISO Forum: When systems are compromised, what's your strategy for maintaining business continuity while ensuring complete threat eradication?

Dr. Pawan K Sharma: We isolate affected systems immediately to prevent spread, while activating backup environments to maintain continuity. A detailed root cause analysis follows, leading to targeted remediation—patching, cleansing, and reinforcing controls. Regular drills and simulations ensure readiness, and incident response plans are continually refined based on lessons learned. Stakeholder communication remains clear and consistent throughout.ISO 27001, and ISO 22301.existing cryptographic algorithms with quantum-safe alternatives without requiring extensive system overhauls.

"Cyber resilience goes beyond prevention—it's about early detection, timely response, swift recovery, and continuous adaptation,"

CISO Forum: How do you build security programs that can quickly adapt to new attack methods and unknown threats?

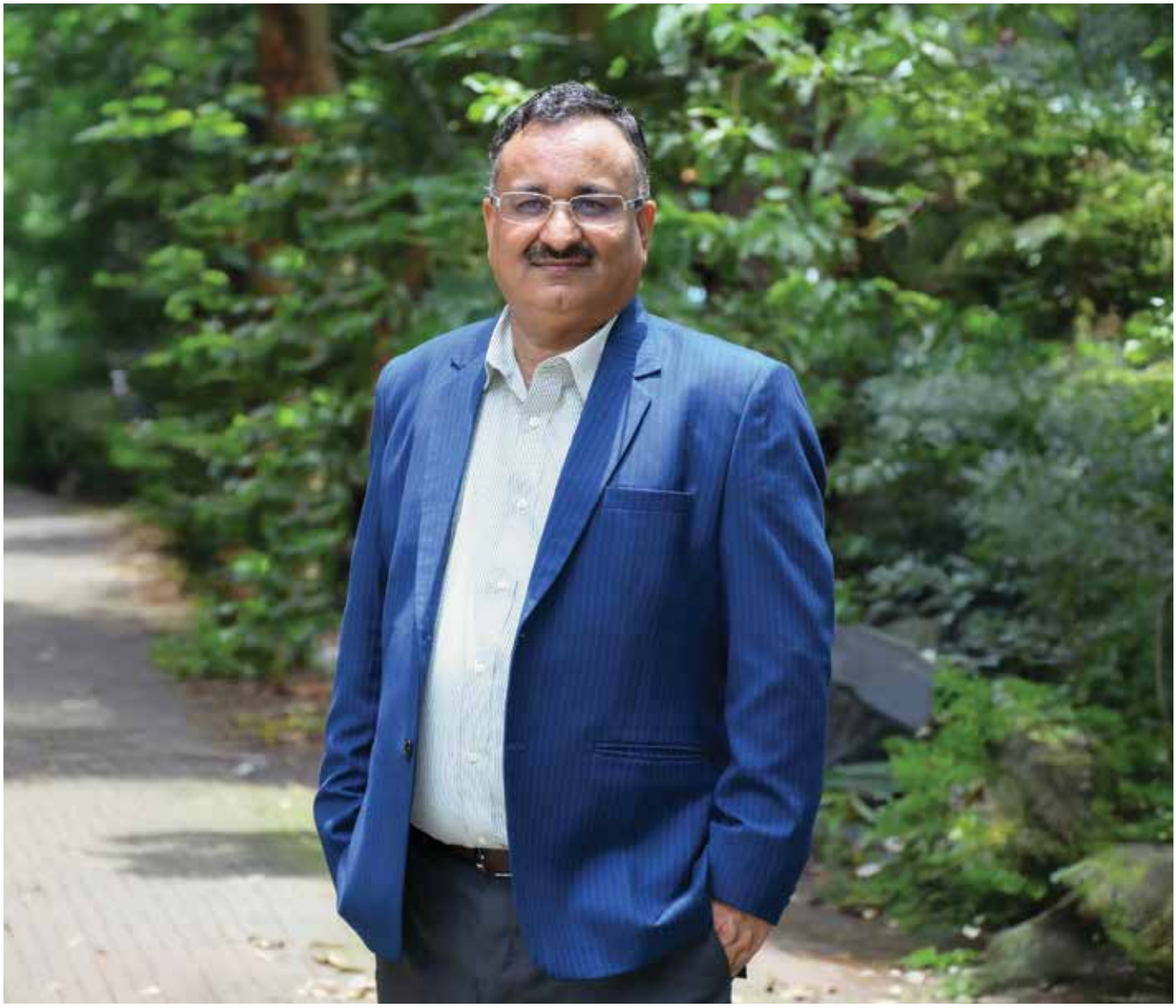
Dr. Pawan K Sharma: We take a proactive and agile approach to security. Real-time monitoring and up-to-date threat intelligence enable early detection and rapid response to threats. Regular reviews of security controls and incident response plans ensure alignment with evolving risks and threats, thereby maintaining optimal security posture. Employee training reinforces awareness, while our flexible architecture allows for quick reconfiguration as new threats emerge.

CISO Forum: How are you building resilience against threats that arise from vendors, partners, and third-party dependencies?

Dr. Pawan K Sharma: We follow a structured, risk-based approach to third-party security. This includes pre-engagement assessments, clearly defined cybersecurity requirements, and contractual safeguards like audit rights. Access to systems is strictly need-based, and we conduct regular audits to ensure compliance. We also monitor the supply chain for vulnerabilities, extend awareness programs to our partners, and maintain contingency plans to ensure business continuity in the event of a breach.

CISO Forum: What role do your employees play in your resilience strategy, and how do you prepare them for their part in cyber defense?

Dr. Pawan K Sharma: Employees play a critical role in an organisation's resilience strategy, particularly in the context of cybersecurity. As the first line of defense, their awareness and day-to-day actions can significantly influence the organisation's ability to prevent, detect, and respond to security threats.



Dr. Pawan K Sharma
CISO at Tata Motors

We invest in ongoing edu cation and training programs to equip employees with the knowledge and tools needed to identify and report suspicious activity. This includes simulated phishing exercises, role-based security training, and regular updates on emerging threats and best practices. Clear guidelines are in place to ensure the secure handling of sensitive information, and we foster a culture of cyber awareness across all levels of the organisation. By embedding cybersecurity into daily routines and decision-making, we build a strong human firewall that complements our technical safeguards. This integrated approach ensures that every employee contributes meaningfully to our overall cyber resilience.

CISO Forum: How do you learn from security incidents and near-misses to strengthen your organisation's overall cyber resilience?

Dr. Pawan K Sharma: We treat every incident and near-miss as a learning opportunity. Post-event reviews help us identify root causes, assess response effectiveness, and uncover gaps in systems, processes, or user behaviour. These insights drive updates to policies, tools, and training.

Real-life examples are used in employee awareness programs, while regular drills and simulations ensure that employees are prepared. We also track patterns, encourage open reporting, and collaborate with industry peers to stay ahead of emerging threats. This continuous feedback loop strengthens our overall cyber resilience. ■

Scaling AI: Why Trust Is the True Competitive Edge

ARTIFICIAL INTELLIGENCE has moved far beyond pilots and proofs of concept. It is now embedded in everyday business, shaping how organizations compete, serve customers, and make decisions. The question is no longer whether to adopt AI, but how to scale it—faster, more effectively, and without compromising trust.

The State of Enterprise Technology Survey 2025, conducted by CIO&Leader, the sister publication of CISO Forum, highlights this paradox. Drawing insights from over 350 senior technology and cybersecurity leaders, the report shows that while enterprises recognize AI's immense value, scaling it remains difficult. Skill gaps, cultural resistance, and identifying the right use cases pose hurdles, but the single biggest roadblock is security and privacy. A striking 91.7% of Indian enterprises cite these risks as their top concern.

The threat landscape reinforces this anxiety. Traditional risks like phishing, ransomware, and identity-based attacks continue to dominate, even as AI-driven threats—such as model poisoning, adversarial manipulation, and data leakage—are rapidly emerging.

The survey also highlights how enterprises are responding. Zero-trust frameworks, cloud-native controls, AI-powered detection tools, SOC modernization, and privileged access management are becoming central to enterprise defense strategies. These shifts underscore a critical truth: scaling AI is not just about scaling technology, it is about scaling trust.

For CISOs, this creates both a responsibility and an opportunity. In the AI era, they are no longer just defenders of infrastructure, they are the architects of trust. Their leadership will shape how confidently enterprises can harness AI.

To succeed, CISOs must drive the agenda on several fronts:

- **Governance & compliance:** Establishing strong AI gover nance frameworks, clear guidelines, and ensuring regulatory compliance.
- **Workforce readiness:** Building AI-aware teams by deploying the right tools, promoting ethical use, and nurturing a culture of risk awareness.
- **Continuous oversight:** Implementing monitoring systems that detect vulnerabilities and flag emerging security risks in real time.
- **Stakeholder collaboration:** Working closely with business lead ers, data scientists, and regulators to align security priorities with enterprise ambitions.

In the end, AI will scale in enterprises only at the pace at which trust scales. And CISOs, standing at the intersection of risk, technology, and business, hold the keys to that future.■

"More than 91.7% of Indian enterprises cite data security and privacy risks as their most significant obstacle to scaling AI and analytics."

Jatinder Singh
Editor, CISO Forum
jatinder.singh@9dot9.in

AMD PRESENTS

26th Annual Conference CIO&LEADER

AI: From Pilot to Production

1st-3rd August, 2025 • Ritz Carlton, Pune

CO-PRESENTED BY NxtGen

Thank You

for making 26th Annual CIO&Leader Conference a Grand Success.

Our Partners

PRESENTING PARTNER: AMD

CO-PRESENTING PARTNER: NxtGen

POWERED BY PARTNER: sify

CO-POWERED BY PARTNERS: freshworks, Google Cloud, TATA COMMUNICATIONS, VERTIV

GOLD PARTNERS: InfoBeans, servicenow, SentinelOne, UNICOM, neat.

ASSOCIATE PARTNERS: allied digital, Barracuda, CHECK POINT, CRESTRON, Sigma AVIT, DELTA, DevRev, GENESYS, LAUREN GROUP, IBM, L&T-Cloudfinity, NetApp, neysa, opentext, rubrik, SAP, sas, Red Hat, ST Telemedia Global Data Centres, SymphonyAI, UiPath

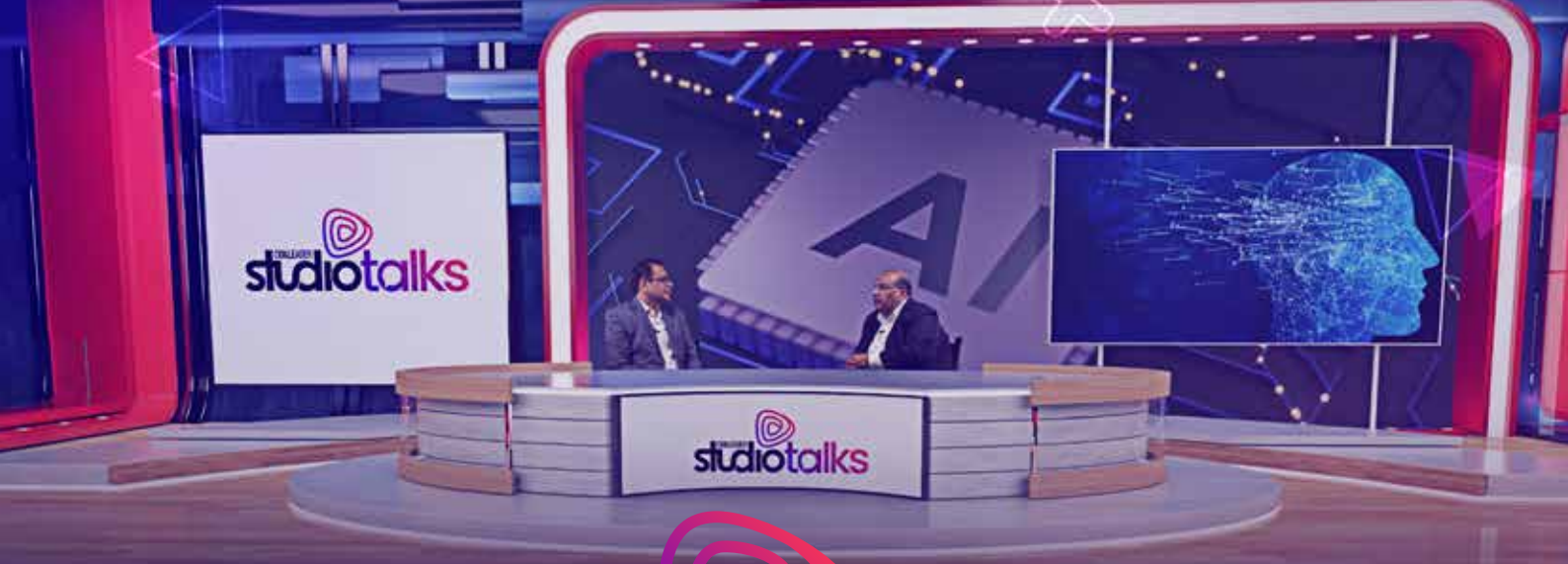
EXHIBIT PARTNERS: acecloud by rtds, esds, HCLTech, IceWarp, infraon, motherson, NeoSOFT, SPOG.AI

EVENT TECH PARTNER: CONECT

MEDIA PARTNER: CNBC TV18

CONCEPT BY: CIO&LEADER, IT NEXT

#CIOandLeaderConference



CIO&LEADER studiotalks

CIO&LEADER STUDIOTALKS—
WHERE TECHNOLOGY MEETS THE SPOTLIGHT!

CIO&Leader proudly presents StudioTalks—a premium platform where India's most influential CIOs and CTOs take center stage. Captured with high-production aesthetics, sleek visuals, and dynamic backdrops, StudioTalks transforms leadership insights into an engaging cinematic experience, and brings India's most influential CIOs and CTOs into the spotlight.
This exclusive series explores visionary leadership, emerging technologies, and strategic transformation—all presented in a format that blends deep insights with the visual polish of a professional studio production.

WHY JOIN STUDIOTALKS?

Engage in powerful conversations that shape the future of enterprise IT.

Share your expertise in a high-impact, TV-style format.

Be featured among India's top technology leaders.

Be the voice of transformation. Be part of CIO&Leader StudioTalks.

SECURE YOUR SPOT NOW!

For more information
Jatinder Singh
Executive Editor - Enterprise Tech
jatinder.singh@9dot9.in, +919718154231

For Business Proposal
Hafeez Shaikh
National Sales Head, B2B Tech,
hafeez.shaikh@9dot9.in, +91 9833103611

Follow us: @CIOandLeader