@entitworld @enterpriseitworld @enterpariseitworld

RS 20 | PAGES 40 | VOLUME 10 | ISSUE 05 WWW.ENTERPRISEITWORLD.COM

Enterprise IT WORLD

FOR THE CIOs. BY THE CIOs.

SEPTEMBER 2025

BEYOND AI BUZZ: HOW VEHERE IS REWRITING THE RULES OF GLOBAL CYBERSECURITY

The untold story of Vehere's bold vision for AI-first cybersecurity in a connected world.

PRAVEEN JAISWAL
FOUNDER AND COO
VEHERE

NAVEEN JAISWAL
FOUNDER AND CTO
VEHERE

micron

6400MT/s DDR5 Server DRAM

For AI and deep learning

Relieve the bandwidth-per-core crunch
to pull peak computing performance

Best for

- Maximizing DDR5 server
- Workstation performance
- Artificial intelligence
- Intensive simulations

Speed

Up to 6400MT/s

Capacity

Up to 128GB

Warranty

3-year limited

Key features

- Increase performance by up to 85% over DDR4
- Speeds up to 6400MT/s
- New higher RDIMM density of 128GB using single die packaging
- Optimized for the latest Intel® and AMD® server and workstation platforms
- 3-year limited warranty
- 100% component and module tested
- Operating voltage reduced to 1.1V from DDR4's 1.2V
- Manufactured by Micron®

Contact us - expert talk

Mr. Sanjeeo Singh
Manager - Enterprise Sales
Contact: +91 8800507776

CIO500 & ACCELERATOR **X AWARDS 2025 – A NATIONWIDE CELEBRATION** OF TECH LEADERSHIP, POWERED BY SNS, **EVENTUS, AND SOPHOS**

The CIO500 & Accelerator X Awards 2025 has successfully connected over 1500 CIOs and IT heads across ten major cities—Chennai, Hyderabad, Bangalore, Kolkata, Ahmedabad, Delhi, Pune, Kochi, Coimbatore, and Mumbai—creating a powerful platform for collaboration, recognition, and regional insight into India's evolving digital landscape.

This year's edition was especially significant as SNS celebrated its 25th anniversary, marking a legacy of innovation and leadership in the technology space. SNS played a pivotal role as the presenting partner in 8 out of the 10 cities, bringing its deep expertise and customer-centric approach to the forefront of discussions around infrastructure modernization, cybersecurity, and digital transformation.

Each city stop was tailored to reflect local market dynamics and sectoral challenges, allowing CIOs to engage in meaningful dialogue around:

- Regional innovation priorities
- Digital maturity across industries
- Talent and resource constraints
- Cyber resilience and AI adoption

The Mumbai finale was a grand culmination of this journey, and special thanks go to Eventus, who stepped in as the presenting partner for the Mumbai chapter. Their support helped elevate the experience, enabling high-impact sessions and seamless execution that matched the scale and ambition of the event.

In Ahmedabad, Sophos took the lead as the presenting partner, bringing its global cybersecurity expertise to the local stage. Their presence sparked valuable conversations around threat intelligence, endpoint protection, and building resilient IT ecosystems in Gujarat's rapidly growing industrial and financial sectors.

Over 80 CIOs were honored in Mumbai, and the sessions featured thought leaders like Apoorba Kumar Patranabish and Akash Sureka, who addressed the evolving role of CIOs in boardroom strategy and crisis management. Across all ten cities, the awards recognized leaders who are driving transformation in manufacturing, healthcare, BFSI, retail, and beyond. Sanjay Mohapatra, Editor of Enterprise IT World, reflected on the journey:

"Connecting 1500 CIOs across India has given us a panoramic view of the country's digital ambitions. With SNS celebrating 25 years and leading the charge in 8 cities, and with Eventus and Sophos powering key chapters, this initiative became a true celebration of leadership, legacy, and the future of technology."

As India accelerates toward its $7.3 trillion GDP vision by 2030, the insights, connections, and collaborations forged through this initiative will serve as a powerful catalyst. The CIO500 & Accelerator X Awards 2025, powered by the legacy of SNS and the strategic support of Eventus and Sophos, has reaffirmed that India's digital future is not only ambitious—it's collaborative, inclusive, and achievable. ENT

Mohapatra

SANJAY MOHAPATRA
SANJAY@ACCENTINFOMEDIA.COM

NEXT MONTH SPECIAL

COVER STORY

AUTOMATION STRATEGIES

The next issue is dedicated to the Automation Strategies. We would like to take feedback from the CIOs and OEMs and create our judgment on the same.

SUPPLEMENT

QUOTES FROM TOP CIOS

The supplement story of the magazine would have relevant quotes from the top CIOs in India.

PLUS

Interviews and Case Studies

Catch interviews, guest articles and case studies of recent applications from the Industry stakeholders, IT/ITES Vendors and IT leaders and CIOs from the Enterprise IT World CIO Community.

Send in your inputs to sanjay@accentinfomedia.com

CONTENTS

VOLUME 10 | ISSUE 05 | SEPTEMBER 2025 | WWW.ENTERPRISEITWORLD.COM

FEATURE STORY

20 **BALANCING INNOVATION, COST, AND SECURITY: INSIGHTS FROM INDUSTRY LEADERS**

Enterprises must drive innovation with agility while maintaining disciplined cost structures, ensuring that transformation does not come at the expense of financial resilience.

27

GUEST TALK

RICK VANOVER

"Guarding the Gateways: Why Supply Chain Security Demands a New Approach"

36

SECURITY

AMIT SHASTRI

"Digitate's OpenTelemetry Integration Brings CIOs Closer to Self-Healing IT"

Enterprise IT WORLD
FOR THE CIOs. BY THE CIOs.

Publisher: Sanjib Mohapatra
Chief Editor: Sanjay Mohapatra
Associate Editor: Balaka Baruah Agarwal
Managing Editor: Anisha Nayar Dhawan
Designer : Deepak kumar
Web Designer: Sangeet Kumar
Technical Writer: Manas Ranjan
Lead Visualizer: DPR Choudhary

MARKETING
Print & Advertising: Annie Garg
Marketing Manager: Sangram Barpanda

SALES CONTACTS
Delhi 6/102, Kaushalya Park, Hauz Khas
New Delhi-110016
Phone: 91-11-40587445
E-mail: info@accentinfomedia.com

EDITORIAL OFFICE
Delhi: 6/103, (GF) Kaushalya Park, Hauz Khas
New Delhi-110016,
Phone: 91-40587445
info@accentinfomedia.com

Printed, Published and Owned by Sanjib Mohapatra
Place of Publication: 6/103, (GF) Kaushalya Park,
Hauz Khas
New Delhi-110016
Phone: 91-11-46151993 / 41055458
Printed at Karan Printers, F-29/2, 1st floor, Okhla Industrial Area, Phase-2, New Delhi 110020, India.

Subscription: Rs.200 (12 issues)
All payments favouring: Accent Info Media Pvt. Ltd.

MORE INSIDE

Editorial ~~~~~~~~~~~~~~~~~~~~~~~~~~~ 03
News ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ 06

Look Ahead

Introducing **HID Amico**™

Facial Recognition Readers

HID Amico combines advanced facial recognition technology with a user-friendly experience to streamline entry points while enhancing security.

- **Fast and accurate recognition** to reduce delays at entry points.
- **Multiple authentication methods** for heightened security.
- **Flexible integration options** with out-of-the-box support for OSDP and Wiegand.

HID

ITWORLD ROUND UP

SAP Launches Sovereign Cloud in India to Power Secure and Compliant Innovation

SAP, a global leader in enterprise application software and business AI, has launched its SAP Sovereign Cloud in India, a significant step toward strengthening the nation's digital sovereignty. Unveiled at SAP Labs India Innovation Park in Bengaluru, the offering is designed in full compliance with the National Information Security Policy & Guidelines (NISPG) to help governments and regulated industries modernize securely with cloud and AI while retaining full control over their sensitive data.

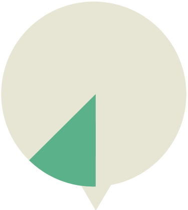
The SAP Sovereign Cloud delivers sovereignty across four key dimensions—data, operational, technical, and legal—enabling Indian enterprises in regulated sectors to build secure, future-ready digital ecosystems. Customers will have flexibility to deploy on-site within their own data centers or through a hyperscaler-based model in partnership with Amazon Web Services (AWS).

As part of the initiative, SAP also inaugurated a Secure Operational Facility at its Bengaluru campus to meet the requirements of India's National Security Authorities. The facility will serve as a hub for compliance, innovation, and co-creation with Indian customers.

"With SAP Sovereign Cloud in India, we are proud to support the country's path as a growing hub for innovation—offering customers freedom of choice to embrace cloud and AI while retaining full control over data and operations," said Martin Merz, President, SAP Sovereign Cloud.

"By ensuring data remains secure, compliant, and within sovereign boundaries, we are enabling India's regulated industries to innovate fearlessly," added Manish Prasad, President & Managing Director, SAP Indian Subcontinent.

DATA BRIEF



Gartner Says Worldwide GenAI Smartphone End-User Spending to Total $298 Billion by the End of 2025

BharatGen Secures INR 988.6 Crore Funding Under IndiaAI Mission to Lead India's Sovereign AI Push

BharatGen, India's first government-backed multimodal sovereign AI initiative, has been awarded INR 988.6 crore under the IndiaAI Mission, making it the largest beneficiary of the Ministry of Electronics and Information Technology's (MeitY) INR 1,500 crore allocation. The announcement was made by Hon'ble Union Minister of Electronics & IT, Shri Ashwini Vaishnaw, at an event held at The Ashok, New Delhi, on September 18.

The funding underscores BharatGen's central role in building India's sovereign AI ecosystem and will accelerate the development of multilingual, multimodal AI models, including Large Language Models (LLMs) with up to one trillion parameters. These models will power AI-driven applications across critical sectors such as agriculture, governance, finance, healthcare, and education.

Earlier this year, BharatGen launched Param-1, a bilingual LLM with 2.9 billion parameters, pretrained on 5 trillion tokens in English and Hindi. The next phase aims to expand coverage to all 22 scheduled Indian languages, ensuring equitable access and inclusive innovation.

The BharatGen consortium includes leading academic institutions such as IIT Bombay, IIT Madras, IIT Kanpur, IIIT Hyderabad, IIT Hyderabad, IIT Mandi, IIT Kharagpur, IIIT Delhi, and IIM Indore, reflecting a collaborative national effort.

"This allocation will empower BharatGen to advance foundational models, strengthen AI infrastructure, and drive adoption while ensuring inclusive access across India's diverse linguistic and cultural landscape," said Prof.

TCS Partners with NVIDIA to Accelerate AI Adoption in Retail

Tata Consultancy Services (TCS) has announced a strategic partnership with NVIDIA to integrate accelerated computing and AI Enterprise software into its retail solutions, helping global retailers drive operational efficiency, reduce costs, and scale innovation.

TCS has embedded NVIDIA technologies across its flagship retail platforms, including TCS Optumera™ and TCS Omnistore™, enabling enterprises to harness advanced AI, multimodal data, and domain-specific accelerators. The partnership will allow retailers to adopt next-generation AI capabilities at speed and at significantly lower costs.

"At TCS, we help retailers gain a competitive advantage and unlock new sources of growth by combining our deep domain experience with next-generation technology," said Krishnan Ramanujam, President, Consumer Business Group, TCS. "Together with NVIDIA, we are setting a new standard for AI excellence, superior store operations, and dynamic supply chain management."

Key solutions include Generative AI adoption with TCS AI WisdomNext™, Stores of the Future

CIO EVENTS

10-12 SEP, 2025

SEMICON Taiwan, One of the biggest trade shows in semiconductors & microelectronics in Asia. Key for hardware / chip manufacturing, packaging, test technologies.

PLACE: **TAIPEI, TAIWAN**

05-09 SEP, 2025

IFA Berlin 2025, Major consumer electronics & home appliances show. Great for seeing the latest in gadgets, consumer tech, display tech, IoT etc.

PLACE: **BERLIN, GERMANY**

12-14 SEP, 2025

CogX Festival 2025 , Big gathering around AI, emerging technologies, ethics, government policy. Good mix of academic, industry and public-sector perspectives.

PLACE: **LONDON, UK**

09-12 SEP, 2025

Oracle CloudWorld, One of the flagship cloud gatherings: infrastructure, cloud services, enterprise solutions, updates from Oracle & ecosystem. Important for cloud / enterprise tech trends.

PLACE: **LAS VEGAS, USA**

D-Link®

MTCTE CERTIFIED

TEC

☑ EMI ☑ SAFETY ☑ SECURITY

BUILD SMARTER NETWORKS WITH NEXT-GEN Wi-Fi 6

Next-Gen Wi-Fi for Next-Level Environments-High Density, High Demand, No Compromise

- Flexible AP Solutions
- WPA3 — Centralized Management with Wi-Fi controller
- Enterprise Securtiy
- 160 — *160 Mhz Channels
- 2.5 GBPS — *Multi-Gigabit Port
- 3 GBPS — *Aggregated Throughput
- Centralized Management With Nuclias Connect
- Intelligent & Secure Performance
- User Authentication & Seamless Roaming
- IP68 Weather Proof Housing in Outdoor AP
- Multiple Operational Modes
- MU-MIMO & Beam-Forming

*60 Mhz, 2.5 Gbps, 3 Gbps Supported In DAP-X3060 Series Only

sales@in.dlink.com www.dlink.com 080 691 33 999 Follow us:

Smarter Security: Akamai and Seraphic Join Forces to Simplify SSE with Secure Enterprise Browsing

Enterprise IT WORLD
Search...
Smarter Security: Akamai and Seraphic Join Forces to Simplify SSE with Secure Enterprise Browsing
www.enterpriseitworld.com

Akamai Technologies has entered into a strategic partnership with Seraphic Security to integrate secure enterprise browser (SEB) technology into its Zero Trust portfolio, marking a major step toward simplifying security service edge (SSE) architectures.

With enterprises rapidly adopting SaaS, private applications, and AI tools, employees expect seamless access—yet security teams must combat new risks such as data leakage, malicious AI prompts, and unmanaged browsers. Traditional network-based security has struggled to close these gaps, prompting demand for browser-level protection as part of modern Zero Trust frameworks.

"Enterprises are realising that unmanaged browsers and risky AI tools create gaps traditional network security can't cover. Partnering with Akamai allows us to extend secure browsing into a broader Zero Trust framework, ensuring organisations can adopt new technologies confidently while keeping users and data safe," said Ilan Yeshua, CEO and Co-Founder, Seraphic Security.

By embedding Seraphic's SEB with Akamai's Enterprise Application Access—its Zero Trust Network Access solution—the partnership provides secure, frictionless access to apps and data without relying on heavy proxy-based architectures.

"With Seraphic, we're able to go beyond the limits of legacy SSE," said Ofer Wolf, Senior Vice President and General Manager, Enterprise Security at Akamai. "By combining Seraphic's enterprise secure browsing with our ZTNA solution we deliver a simpler way to secure apps, SaaS, and AI tools on any device, without the heavy infrastructure and complexity of traditional proxies."

The joint solution leverages Akamai's global network for high performance while offering unified policy controls, device posture checks,

S/HE SAID IT

THOMAS KURIAN, CEO, GOOGLE CLOUD

"We help organizations unify their data across multiple clouds and silos, combining structured and unstructured data and making data every employee's superpower."

"Today, India holds the fourth-largest foreign exchange reserves in the world at about USD 690 billion. Our inflation has remained below four per cent for the last three months. The Reserve Bank has done a commendable job balancing liquidity and currency management. "We are well on track with our bilateral trade agreement with the United States of America (USA) and making fast progress with the European Union's 27-nation bloc."

PIYUSH GOYAL, INDIA'S UNION MINISTER FOR COMMERCE AND INDUSTRY

QUICK BYTE ON SECURITY

Acronis Report Reveals India Tops Global Malware Charts as AI Fuels Ransomware Surge

Acronis, a global leader in cybersecurity and data protection, has released its Cyberthreats Report H1 2025, revealing alarming trends in the global threat landscape. The report highlights India as the most targeted country worldwide, with 12.4% of monitored endpoints affected, underscoring the nation's growing exposure to AI-powered phishing, impersonation, and ransomware attacks.

The report, based on data from over 1 million unique Windows endpoints globally, shows that ransomware remains the top threat to large and midsized

Vertiv to Acquire Great Lakes Data Racks & Cabinets for $200 **Million**

Vertiv has signed an agreement to acquire Great Lakes Data Racks & Cabinets (Great Lakes) for $200 million, in a move aimed at strengthening its AI-ready infrastructure portfolio.

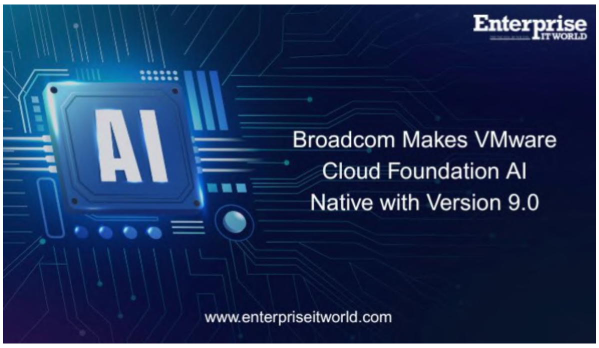
Founded in 1985 and headquartered in Edinboro, Pennsylvania, Great Lakes is a leading manufacturer of custom and standard racks, integrated cabinets, seismic solutions, and advanced cable management systems. With operations in the U.S. and Europe, the company has earned a strong reputation for delivering engineered, tailored infrastructure for both retrofit and new data center projects.

"Great Lakes is a leading rack manufacturer with an extensive portfolio of high-end solutions and innovation capabilities that are essential in an increasingly demanding high-density AI infrastructure environment," said Gio Albertazzi, CEO, Vertiv.

By combining Great Lakes' expertise with Vertiv's global power and cooling solutions, the acquisition will allow Vertiv to deliver end-to-end, integrated data center solutions. Customers are expected to benefit from consolidated sourcing, faster deployment of pre-engineered systems, enhanced scalability for AI workloads, and stronger service support worldwide.

The transaction, valued at about 11.5x expected 2026 EBITDA after synergies, is subject to regulatory approvals and customary closing conditions. Completion is expected in Q3 2025.

Broadcom Makes VMware Cloud Foundation AI Native **with Version 9.0**


Enterprise IT WORLD
AI
Broadcom Makes VMware Cloud Foundation AI Native with Version 9.0
www.enterpriseitworld.com

Broadcom has announced the general availability of VMware Cloud Foundation (VCF) 9.0, transforming the platform into an AI native private cloud solution. The release integrates VMware Private AI Services as a standard component, enabling enterprises to securely run, fine-tune, and govern AI models with GPU precision.

With more than 100 million cores of VCF licensed globally and adoption by nine of the top 10 Fortune 500 companies, VCF continues to see strong momentum as enterprises re-architect their cloud strategies.

"To support the next wave of AI innovation, Broadcom is making Private AI a standard part of the modern private cloud," said Krish Prasad, SVP & GM, VMware Cloud Foundation Division, Broadcom. "Infrastructure teams gain virtualization benefits for AI workloads without compromising performance, while developers get direct access to AI services."

From Q1 FY26, every VCF subscription will include Private AI Services — covering GPU monitoring, model runtime, vector databases, and agent builders — without the need for add-ons. Future innovations will introduce AI-driven Intelligent Assist for support, Model Context Protocol integration with platforms like ServiceNow and GitHub, and multi-tenant Models-as-a-Service with full data isolation.

EXECUTIVE MOVEMENT

Firstsource Appoints Kumaran Shanmuhan as Chief Strategy Officer

Tenable Appoints Matthew Brown as Chief Financial Officer

Eventus Security Appoints Vikas Somani as Vice President – Sales to Accelerate Growth and Enterprise Expansion in India

Abdur Rafi Joins RICE Adamas Group as Group Head IT

VIBS Infosol Appoints Vikas Khandelwal as Chief Information Officer

Wiise Appoints Sullivan McIntyre as Chief Product Officer to Drive AI-Led ERP Innovation

GLOBAL UPDATE

SentinelOne's Observo AI Acquisition Signals Rising Urgency in Telemetry Data Management

Enterprises are accelerating their shift towards unified telemetry frameworks as fragmented data pipelines drive cost, complexity, and operational risk. SentinelOne's acquisition of Observo AI underscores this urgency, marking a significant step in the convergence of security and observability.

Modern organizations typically rely on dozens of tools for monitoring, analytics, and cybersecurity — each generating massive streams of telemetry data, including logs, metrics, and traces. Managing these pipelines in isolation has become expensive and increasingly unsustainable. SentinelOne's move highlights the growing need to consolidate security data pipelines, where risks are highest.

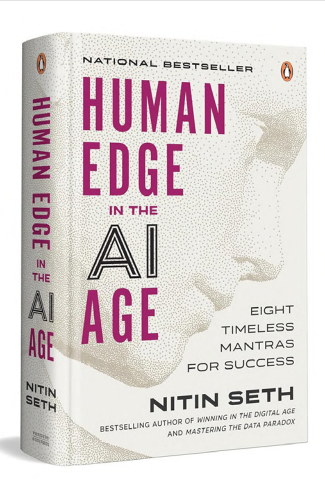
"Enterprises are realizing that telemetry pipelines are the new backbone of digital operations," said Michael Kelly, CEO of Bindplane. "But without consolidation, they become the weakest link. This acquisition is a clear sign the market is moving towards holistic solutions."

Industry experts point to OpenTelemetry as the path forward. As the most widely adopted open-source framework, it provides a standardized method to collect, process, and export telemetry across diverse platforms. Beyond technical efficiency, it reduces duplicate infrastructure costs, accelerates threat detection, and improves resilience.

While SentinelOne's acquisition is strategic for its security business, it also reflects

BOOK SHELF

Human Edge in the AI Age



PRICE:
INR 539 (HARD COVER)
WHERE
AMAZON.IN

Author :
NITIN SETH

About The Book

In Human Edge in the AI Age, Nitin Seth delivers a timely and deeply reflective guide for navigating the accelerating influence of artificial intelligence. As AI reshapes industries, job roles, and even emotional domains, Seth asks a profound question: What remains uniquely human when machines can do almost everything else?

The book is structured around the POSSIBLE framework, an eight-dimensional model that highlights timeless human traits—Problem-Solving, Openness, Spirituality, Sports, Impact, Balance, Leadership, and Entrepreneurship. These traits, Seth argues, are not just philosophical ideals but practical tools for thriving in an AI-driven world. Each chapter ends with actionable insights, encouraging readers to cultivate emotional intelligence, ethical clarity, and adaptability—qualities that machines

Okta Acquires Axiom Security to Strengthen Privileged Access in AI-Driven Enterprises

Okta has signed a definitive agreement to acquire Axiom Security, a modern Privileged Access Management (PAM) provider designed for cloud, SaaS, and database environments. The move expands Okta's capabilities in privileged access and strengthens its identity-first security strategy at a time when enterprises face rising risks from AI adoption.

Privileged accounts, which hold the keys to critical systems and sensitive data, have become prime targets for cybercriminals and insider threats. Traditional PAM solutions, often built for on-premises infrastructure, are struggling to keep pace with today's cloud-first, hybrid, and AI-driven environments. By integrating Axiom's technology into Okta Privileged Access, customers will gain modern capabilities such as contextual controls, real-time monitoring, and granular policies without added complexity.

The combined platform will enable enterprises to:

Enforce consistent privileged access policies across on-premises, cloud, and SaaS systems.

Gain unified visibility into identity and access risks.

Mitigate emerging threats linked to AI and data misuse.

Okta emphasized that PAM is no longer a niche tool but a core requirement for enterprise security and compliance, particularly as regulations tighten. The integration of Axiom into Okta Privileged Access will be rolled out in phases, with Okta assuring customers of a seamless transition.

With this acquisition, Okta reinforces its role as a trusted partner for enterprises navigating the AI era — where identity is the new perimeter and

Whatfix Unveils AI Agents to Drive Enterprise **Productivity**

Whatfix, a global leader in Digital Adoption Platforms (DAP), has launched a new suite of AI-powered agents designed to simplify enterprise software usage and accelerate business outcomes. Powered by its proprietary ScreenSense technology, the new Whatfix AI Agents interpret user context and real-time intent to deliver intelligent, timely assistance across workflows.

The launch addresses a growing challenge in enterprise IT: translating rising investments in AI and software into measurable productivity. Gartner forecasts double-digit growth in enterprise software spending in 2025, driven by generative AI. Yet, user adoption remains a hurdle.

"Whatfix AI Agents flip the equation — they adapt technology to users, not the other way around," said Khadim Batti, CEO and Co-Founder of Whatfix.

The first three agents — Authoring, Insights, and Guidance — are now live. The Authoring Agent enables non-technical teams to create in-app walkthroughs using natural language. The Insights Agent offers conversational access to analytics, while the Guidance Agent delivers contextual answers from enterprise documentation within workflows.

Early adopters are already seeing impact. "With Whatfix AI, we're heading toward a world where

ManageEngine Adds Digital Employee Experience to Endpoint Central, Paving the Way for Autonomous Endpoint Management

"Our North Star is autonomous endpoint management delivered through a unified platform that proactively ensures all endpoints remain secure and high performing." — Mathivanan Venkatachalam, Vice President, ManageEngine

ManageEngine, the enterprise IT division of Zoho Corporation, has introduced digital employee experience (DEX) capabilities into its flagship Endpoint Central platform, advancing its vision of autonomous endpoint management.

The new features aim to help IT teams detect, diagnose, and remediate endpoint issues proactively, reducing support tickets and boosting employee productivity. Everyday problems such as slow boot times, login delays, or application crashes often remain unnoticed until they impact workflows. With DEX, IT teams gain real-time visibility and automation to address performance concerns before they escalate.

Key capabilities include experience monitoring, root cause analysis, prioritized alerts, automated remediation, and benchmarking to measure endpoint health. Together, these enable IT teams to move from reactive troubleshooting to proactive engagement.

Industry experts highlight hybrid work as a driver for integrated visibility and auto-

CyCognito Study Reveals Gaps in **Enterprise WAF Coverage**

A new study by CyCognito, a leader in external attack surface management, has uncovered alarming gaps in enterprise web application firewall (WAF) protection. Despite WAFs being a foundational layer of application security, the report reveals that over half of enterprise assets remain exposed, including high-traffic applications handling sensitive personal data.

Analyzing more than 500,000 internet-facing assets from Forbes Global 2000 companies, CyCognito found that 52.3% of cloud-hosted and 66.4% of off-cloud assets lacked WAF coverage. Many of these unprotected systems include login portals, registration forms, and checkout pages — prime targets for cyberattacks.

"It's not that enterprises lack WAFs, they lack consistent implementation," said Zohar Venturero, Data Scientist at CyCognito. The study highlights fragmented deployments, siloed security teams, and unknown assets as key contributors to the problem.

On average, enterprises operate 12 different WAF products, with some using over 30. This fragmented approach leads to inconsistent protection and exploitable gaps. A manual review across sectors like finance, retail, and media revealed critical applications running without WAFs, even alongside fully protected flagship systems.

CyCognito warns that years of decentralized procurement and security management have created an illusion of complete coverage. "WAFs still play a critical role in protecting enterprise applications and data," Venturero added. "These

DIGEST

ACRONIS AND INTEL JOIN FORCES FOR AI-POWERED ENDPOINT SECURITY

Acronis has announced a strategic partnership with Intel to deliver AI-driven endpoint threat detection, integrating Acronis Cyber Protect Cloud with Intel® Core™ Ultra processors. The collaboration aims to enhance cybersecurity while optimizing system performance for enterprises and managed service providers (MSPs).

The joint solution leverages Intel's neural processing units (NPUs) to offload resource-heavy security tasks from the CPU, enabling real-time threat detection and remediation directly on endpoint devices. Internal testing shows up to 92% reduction in processor load, allowing organizations to maintain productivity without compromising security.

CRESTRON TO SHOWCASE SIGHTLINE EXPERIENCE AND ONE-TOUCH MEETING AT INFOCOMM INDIA 2025

Crestron, a global leader in smart workplace technology, will unveil its latest innovations — Sightline Experience and One-Touch Meeting — at InfoComm India 2025, booth H01. These solutions are designed to simplify collaboration, enhance connectivity, and deliver seamless user experiences across hybrid workspaces.

The Sightline Experience leverages Visual AI, speaker tracking, and multi-camera intelligence to create immersive, equitable meetings. Powered by Automate VX, it ensures remote and in-room participants engage naturally, with dynamic framing and full-room awareness.

NETGEAR LAUNCHES COMPACT WIFI 6 ACCESS POINT FOR HOSPITALITY AND EDUCATION

NETGEAR has introduced the WAX610W, its most compact WiFi 6 access point yet, tailored for hospitality venues, multi-dwelling units (MDUs), and classrooms. Combining enterprise-grade performance with a sleek wall-mount design, the WAX610W delivers high-speed connectivity and simplified deployment for high-density environments.

Capable of 1.8 Gbps throughput across dual bands, the device supports seamless roaming, WPA2/WPA3 security protocols, and centralized cloud management via the NETGEAR Insight platform. It features one Gigabit PoE-In port for power and uplink, plus four Gigabit LAN ports for connecting IP phones, smart TVs, and other devices — ideal for guest rooms and shared spaces.

"The WAX610W blends unobtrusive design with enterprise-grade performance," said Nat Chidambaram, Senior Director of Product Management at NETGEAR.

MANAGEMENT MANTRA

"Constantly think about how you could be doing things better and questioning yourself."

Elon Musk, ceo, Tesla, SpaceX

Atlassian Opens New R&D Centre in Bengaluru, Expands India Operations

Atlassian, the global collaboration and productivity software company, has inaugurated a new R&D Centre in Bengaluru, marking a significant milestone in its India growth strategy. Spanning over 2 lakh square feet, the facility is four times larger than its previous office and is designed to accommodate 1,000+ employees across two levels.

India has rapidly become one of Atlassian's fastest-growing innovation hubs. Since entering the market in 2018 with a team of 60, the company now boasts over 2,500 employees, with nearly 75% engaged in R&D across areas such as enterprise search, data residency, and customer success.

"This new R&D Centre is a symbol of our investment in the future of work and India's exceptional talent," said Rajeev Rajan, CTO at Atlassian.

The facility supports Atlassian's Team Anywhere policy, offering flexible workstations, collaboration zones, wellness areas, and hybrid-ready infrastructure. It reflects the company's commitment to distributed teamwork and modern workplace design.

"Our new R&D Centre is a destination for the incredible talent we have in India," added Avani Prabhakar, Chief People Officer. "It's designed for how we work today and how we will work tomorrow."

Indus Towers Begins Global Expansion with Entry into African Markets

Indus Towers Limited, India's leading telecom infrastructure provider, has announced its strategic entry into Africa, marking the company's first international expansion. The board has approved operations in Nigeria, Uganda, and Zambia, leveraging its expertise and long-standing partnership with Bharti Airtel to tap into Africa's fast-growing telecom sector.

"The Board's approval to enter international markets in Africa unlocks our vision for long-term sustainable growth and value creation for our shareholders," said Prachur Sah, Managing Director & CEO, Indus Towers. "We are well-positioned to differentiate ourselves through innovative and cost-effective solutions."

This move aligns with the Government of India's vision to encourage Indian enterprises to become global players. Indus Towers aims to diversify its revenue streams and capitalize on emerging market opportunities, especially in regions where Airtel already has a strong footprint.

The new markets offer significant growth potential, driven by increasing mobile penetration and demand for robust telecom infrastructure. Indus Towers plans to bring its proven operational

Sophos Endpoint Now Natively Integrated with Taegis MDR and XDR

Sophos has announced the native integration of Sophos Endpoint into all Taegis MDR and XDR subscriptions, marking a major step in delivering unified cybersecurity solutions with improved ROI. The move follows Sophos' acquisition of Secureworks earlier this year and aims to streamline threat prevention, detection, and response for enterprise customers.

With Sophos Endpoint now automatically included, organizations gain access to advanced ransomware protection, real-time telemetry, and automated response capabilities—all within a single platform. This integration simplifies deployment, reduces licensing costs, and enhances threat mitigation across diverse IT environments.

"Not all endpoint products are built to stop today's hands-on-keyboard attacks," said Raja Patel, Chief Product Officer at Sophos. "Sophos Endpoint's prevention-first capabilities, like CryptoGuard and Adaptive Attack Protection, shut down attacks before they escalate."

The integration also opens new opportunities for partners. "It expands the value and flexibility we deliver to customers and partners," added Chris Bell, SVP of Global Channel & Alliances. "It enables tool consolidation, drives renewals, and strengthens enterprise relationships."

Taegis remains an open platform, supporting third-party endpoint solutions while maximizing operational efficiency. The unified approach helps organizations reduce complexity, improve threat visibility, and respond faster to evolving cyber threats.

Sophos' latest move reinforces its commitment to delivering high-ROI cybersecurity that's both powerful and practical—empowering IT teams to stay ahead of attackers with fewer resources and greater confidence.

Enterprise IT WORLD
AI
AI
AI
Concentric AI Integrates with OpenAI's ChatGPT Enterprise Compliance API to Enhance Data Security Governance
www.enterpriseitworld.com

Concentric AI Integrates with OpenAI's ChatGPT Enterprise Compliance API to Strengthen Data Governance

Concentric AI has announced a strategic integration with OpenAI's ChatGPT Enterprise Compliance API, enhancing data security governance for enterprises leveraging generative AI. This collaboration brings Concentric AI's context-aware Semantic Intelligence™ platform to ChatGPT Enterprise, offering deeper visibility and control over sensitive data.

ChatGPT Enterprise, widely adopted across industries, accesses diverse data sources including proprietary models, user uploads, and enterprise connectors. Concentric AI's platform augments this by accurately identifying and classifying sensitive information—ranging from regulated data like PII, PCI, and PHI to intellectual property and critical business documents often missed by traditional tools.

"With this integration, organizations can fully embrace ChatGPT Enterprise's capabilities while ensuring robust data protection," said Karthik Krishnan, Founder & CEO of Concentric AI.

The integration enables continuous monitoring for risks such as misclassified data, excessive permissions, and improper storage. Automated remediation actions help reduce human error and bolster compliance efforts. Additionally, Semantic Intelligence ingests user prompts and metadata to detect potential insider threats and data leakage.

By eliminating the need for rigid rules or complex regex, Concentric AI's patented approach delivers

5Tattva Joins K. R. Mangalam University's Corporate Advisory Board to Advance Cybersecurity Education

In a strategic move to bridge academia and industry, cybersecurity firm 5Tattva has joined the Corporate Advisory Board (CAB) of K. R. Mangalam University. The partnership aims to strengthen cybersecurity education and prepare students for the growing challenges of the digital age.

As a CAB member, 5Tattva will contribute to curriculum development, mentorship, and aligning academic programs with global industry standards. The company brings deep expertise in cybersecurity consulting, compliance, and implementation, helping students gain real-world insights into threat mitigation and digital resilience.

"This collaboration allows us to mentor students closely and collectively shape the next generation of cybersecurity leaders," said Atul Luthra, Co-Founder of 5Tattva and CEO of Zeroday Ops.

Dr. Vibha Thakur, Director of the Career Development Center at K. R. Mangalam University, welcomed the partnership, emphasizing its potential to empower students with industry-relevant skills and exposure.

Atul Luthra will actively engage with students, offering mentorship and sharing his extensive experience in cybersecurity operations. The collaboration promises hands-on learning through workshops, case studies, and interactive sessions, ensuring students gain both theoretical knowledge and practical expertise.

5Tattva specializes in certifications such as PCI DSS, HIPAA,

Fortinet Named a Leader in 2025 Gartner Magic Quadrant for Hybrid Mesh Firewall

Fortinet has been recognized as a Leader in the 2025 Gartner Magic Quadrant for Hybrid Mesh Firewall (HMF), earning the highest position for Ability to Execute. This marks Fortinet's leadership in 12 Gartner Magic Quadrant reports, reinforcing its strength in converged networking and cybersecurity.

Powered by custom-built ASICs and unified under FortiOS, Fortinet's hybrid mesh firewalls deliver high-performance protection across hardware, virtual, and cloud-native environments. The recognition highlights Fortinet's commitment to innovation, operational flexibility, and integrated security.

"Being recognized as a Leader in the inaugural Gartner Magic Quadrant for Hybrid Mesh Firewall validates our commitment to delivering convergence and best-of-breed security everywhere," said Nirav Shah, SVP of Products and Solutions at Fortinet.

Fortinet's leadership is built on three pillars:

Integrated Security: FortiOS, FortiGuard Labs, and AI-powered defenses form a unified Security Fabric for faster threat detection and response.

AI and Post-Quantum Innovation: FortiAI-Assist combines GenAI, agentic AI, and AIOps, while early adoption of post-quantum cryptography protects sensitive data from future threats.

Operational Flexibility: FortiFlex licensing enables seamless transitions between hardware, virtual, and cloud firewalls with pay-as-you-go agility.

Fortinet also unveiled its vision for next-gen SASE firewalls, converging SD-WAN, ZTNA, CASB, and firewall capabilities within FortiOS for consistent protection across hybrid environments.

This recognition further solidifies Fortinet's role in simplifying cybersecurity adoption, reducing costs, and enhancing user experiences in

GITEX GLOBAL

13-17 OCT 2025
DUBAI WORLD TRADE CENTRE

FEATURING

Global Data Centres · GQX GITEX QUANTUM EXPO · GITEX DIGI HEALTH & BIOTECH · GITEX CYBER VALLEY · GITEX GREEN IMPACT · GLOBAL DEV SLAM

THE WORLD'S LARGEST TECH, AI & STARTUP SHOW

200,000	180	40%	6,500	1,733	400+
TECH EXECUTIVES	COUNTRIES	OF ATTENDEES ARE C-LEVEL	EXHIBITING COMPANIES	STARTUPS	GOVERNMENT ENTITIES

Scan the QR code to

GET INVOLVED

#GITEXGLOBAL
gitex.com

ORGANISED BY
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

BEYOND AI BUZZ: HOW VEHERE IS REWRITING THE RULES OF GLOBAL CYBERSECURITY

The untold story of Vehere's bold vision for AI-first cybersecurity in a connected world.

BY SANJAY@ACCENTINFOMEDIA.COM

The past decade has seen a digital surge like no other. From India's thriving mobile-first economy to the global shift toward cloud-native enterprises, technology now underpins every critical function of business and governance. But this progress has come with a dark shadow: cyberattacks that are multiplying in scale, sophistication, and impact. In the first quarter of 2025 alone, organizations faced an average of 1,925 cyberattacks per week—a staggering 47% increase from the previous year, according to Check Point Research. Ransomware has surged by 126% globally, with North America accounting for over half of these incidents.

The rise of mobile-first ecosystems has only widened the attack surface. Consider this: according to the Wikipedia page on mobile security by December 2023, 5.4 million mobile cyberattacks per month were being recorded worldwide—a 147% year-over-year increase. Meanwhile, the number of connected devices is skyrocketing. IoT endpoints are projected to nearly double—from 18.8 billion in 2024 to 40 billion by 2030, per — each one a potential entry point for attackers.

The consequences are devastating. Global cybercrime costs are forecast to reach $10.5 trillion annually by 2025. Deepfake-enabled social engineering adds another layer of risk—51% of security leaders report incidents of executive-targeted attacks leveraging AI-generated impersonations according to reports.

"Cybersecurity is no longer a back-office IT concern—it's boardroom strategy. In a connected world, the fallout from a single breach doesn't stay local. It cascades across supply chains, economies, and even national security," says Praveen Jaiswal, Founder & COO of Vehere.

The Evolving Role of Cybersecurity

Traditionally, enterprises leaned heavily on firewalls, antivirus software, and endpoint detection. But these tools are increasingly outpaced by modern adversaries. Attackers are exploiting encrypted traffic, lateral east–west movement within networks, and human error with alarming precision.

"Most defenses today remain focused on the perimeter, but the real risk lies inside the network," explains Naveen Jaiswal, Founder & CTO of Vehere. "Our mission is to deliver deep visibility into network activity so organizations can detect, investigate, and stop sophisticated threats in real time."

Vehere, founded in 2006, began by building high-performance intelligence systems for governments. Today, it applies that same battlefield-grade insight to enterprises through its AI-powered Network Detection and Response (NDR) platform.

Seeing the Unseen: Vehere's Edge in Cyber Defense

The modern battlefield is not only physical—it lives in invisible data streams coursing through fiber optics and mobile networks. The challenge is no longer about stopping intruders at the gate—it is about spotting subtle anomalies hidden in encrypted traffic before they escalate.

This is where Vehere thrives. Its AI Network Security platform functions like an embedded intelligence officer inside an organization's infrastructure. It inspects every packet, decrypts meaning from encrypted flows, and flags deviations from normal patterns. The result: ransomware halted before files lock, and rogue IoT devices stopped before they can open a backdoor.

Vehere's government-focused AI Counter-Terrorism suite extends this capability at national scale—sifting through torrents of communication data in real time to surface risks that could otherwise slip through. Its Zero-Day Defender tool provides sandboxing to analyze previously unseen malware, ensuring analysts can preemptively counter threats.

At the core of these capabilities is Gladius-X, Vehere's proprietary engine. Comparable to a radar in modern air defense, it scans the digital horizon for faint blips—early signs of compromise invisible to conventional systems.

Banks rely on it to uncover hidden fraud inside encrypted traffic. Manufacturers use it to stop attackers moving laterally across supply chains and Governments deploy it to shield critical infrastructure while balancing scale with privacy.

AI: A Double-Edged Sword

AI is reshaping cybersecurity on both sides of the battlefield: it strengthens protection, but it also fuels more sophisticated threats. Adversaries are deploying AI to generate polymorphic malware, automate phishing, and craft sophisticated deepfake lures. "We see this as the start of AI vs. AI warfare in cyberspace," warns Praveen Jaiswal.

Explaining how AI is disrupting cyber security, Praven says, "From generating polymorphic malware to automating phishing and evasion techniques, AI is being weaponized to outmanoeuvre traditional defenses. At Vehere, our strategy is twofold: first, using AI-driven analytics that can spot patterns. For example, anomalies in encrypted traffic or lateral movement hidden in east–west flows. Second, building adaptive defenses that continuously learn from evolving attack techniques, ensuring our models are not static and can be responsive in real time."

Vehere supervised Deep Neural Network (DNN) platform embeds AI/ML at every layer to spot anomalies that human analysts or signature-based systems may miss. The model does not require any baselining, and can analyze traffic immediately on deployment, ensuring that even never-before-seen attack patterns are caught. Its Entity Behavior Anomaly (EBA) models continuously adapt in real time, learning and evolving with each data flow.

Praveen cites the example of a global financial institution that was nearly compromised through slow, encrypted data exfiltration. Conventional defenses saw nothing suspicious while Vehere's AI model picked up subtle irregularities in flow timing and packet behavior, uncovering a hidden command-and-control channel just in time. "This is not AI as a buzzword," stresses Naveen. "For us, AI directly translates into protection—spotting what legacy tools overlook and stopping real-world threats before they escalate."

"Our platform doesn't just detect anomalies — it provides rich forensic visibility into traffic flows, communications, and patterns of compromise. This enables security teams to rapidly reconstruct incidents, trace attacker movement across east–west traffic, and respond with speed and precision. By combining detection with investigation and response, we help customers reduce dwell time and strengthen resilience against even the most advanced adversaries," adds Naveen.

Unlike conventional solutions that falter against encryption, Vehere's encryption-agnostic traffic analysis penetrates secure channels to uncover hidden threats. And by harnessing the power of Large Language Models (LLMs), its autonomous security framework cuts through the noise of false positives, guiding analysts directly to the threats that matter most. This integration of advanced AI models positions Vehere not just as a technology provider, but as a pioneer shaping the future of cyber defense in an AI-driven world.

PRAVEEN JAISWAL

Founder and COO, Vehere

> "Our mission is to deliver deep visibility into network activity, helping organizations detect, investigate **and stop sophisticated threats in real time. With two decades of experience and a global presence,** Vehere is bridging the worlds of national security and enterprise cybersecurity."

Winning Digital by Fortifying Cyber Security

Cybersecurity today is at an inflection point. Attacks are no longer confined to isolated systems—they move laterally across hybrid networks, hide inside encrypted traffic, and exploit the speed at which businesses embrace digital transformation. With ransomware

NAVEEN JAISWAL
Founder and CTO, Vehere

> “We are actively working to strengthen ease of deployment and automation at scale for enterprises. We **are heavily focused on making our platforms more automated, intuitive,** and analyst-friendly, so that our customers get faster time-to-value.”

damages projected to hit USD 265 billion by 2031 (Cybersecurity Ventures) and 43% of global breaches now traced to cloud or hybrid environments, the urgency to rethink cyber defense has never been greater.

For most enterprises, the challenges are compounded by two hard truths: first, the shortage of skilled cyber analysts, with an estimated shortage of four million security roles worldwide; second, the limitations of legacy tools that drown teams in alerts but miss the stealthier, more sophisticated threats. Add to this a mobile-first, always-connected world, where every device becomes a potential vulnerability, and it's clear that traditional defense approaches simply don't measure up.

This is the landscape which Vehere seeks to disrupt—unlike conventional tools that just flag anomalies, Vehere's platforms allow enterprises to reconstruct entire attack chains in near real time by tracing an adversary's footsteps, identifying lateral movements, and neutralizing the threat before it spirals into a breach. In effect, Vehere has introduced solutions with deep forensics that only state intelligence agencies could afford.

Vehere's roots in national defense technology have given it an edge. Its solutions were battle-tested in high-stakes environments where precision and speed were non-negotiable. That same rigor is now embedded in enterprise deployments, giving organizations access to capabilities hardened in the crucible of defense, but tailored for the realities of business.

With a global-first mindset, Valere solutions are compliant with global regulatory requirements and protocols. It has strong network of local partnerships, and the leadership is spread across the U.S, Singapore, Dubai, Saudi Arabia, and India. That means the company gets visibility into threats across borders and an understanding of compliance requirements to adapt the technology. It does not simply export the technology but brings its understanding from different markets and the local context to design solutions while operating with global strength.

The company is among the few actively preparing for the quantum era, where encryption could be broken in seconds. Its quantum-safe visibility tools and autonomous AI defense systems empowers to protect against today's threats and be prepared for the battles ahead. By leveraging LLM-powered AI, Vehere also cuts through the “alert fatigue” plaguing SOC teams, guiding analysts to focus only on the signals that matter most.

“Our strength lies in combining India's engineering excellence with global go-to-market expertise,” says Praveen Jaiswal, Co-founder of Vehere. “We're not just competing with international players—we are defining the next wave of cybersecurity innovation.”

In a market crowded with products promising next-gen security, Vehere stands out because it doesn't just promise resilience—it builds it into the fabric of enterprise defense. By marrying intelligence-grade technology with real-world enterprise needs, Vehere is continuously innovating to embed resilience in cyber security.

Beyond AI Buzzwords: Vehere's Distinct Approach

In cybersecurity, AI has become an overused terminology as vendors promise machine learning breakthroughs and revolutionary anomaly detection, even though the results do not match the claims when confronted with real-world threats. The problem is that AI will not work unless it is woven into the heart of security strategy.

Vehere approach to security is unique weaving AI into everything. Says Naveen, “AI and ML are at the core of Vehere's approach to cyber defense. AI directly translates into protection — spotting what legacy tools overlook and preventing threats before they escalate. What sets us apart are our network forensics and incident response capabilities. Our platform doesn't just detect anomalies—it provides forensic visibility into traffic flows, communications, and patterns of compromise. This enables security teams to rapidly reconstruct incidents and respond with speed and precision. By combining detection with investigation and response, we help customers reduce time and strengthen resilience against even the most advanced adversaries.”

That difference comes to life in the way Vehere engineers its platform. At its core are deep neural networks that learn continuously, picking up subtle deviations in behavior and the EBA model which adapt dynamically to evolving user and device activities.

Vehere's encryption-agnostic traffic analysis offers visibility into secure channels to expose attackers using encryption to cover malware and lateral movements. To cut through the fog of endless alerts Vehere integrates large language models that act like an intelligent filter, directing analysts to the small number of incidents that matter most.

The company's technology empowers teams to detect and reconstruct incidents in detail and shut down attacks with surgical precision. That capability is built on years of deep work with government and intelligence agencies, where technologies refined for national defense have been seamlessly adapted to meet the complex needs of enterprises.

The Road Ahead: Cybersecurity as Strategic Resilience

Cyber threats today are existential, not incidental. In 2025, the average cost of a U.S. data breach reached $5.18 million, while downtime costs soared to $21,250 per minute. For businesses and governments alike, the stakes in cybersecurity has increased becoming synonymous with resilience—a matter of preserving trust, continuity, and national stability.

Vehere's mandate is clear—it seeks to weld intelligence-grade visibility with adaptive AI and work as a strategic partner in safeguarding the future, rather than just a technology vendor. And so, as the digital battlefield shifts into an era of AI vs. AI, Vehere is working systematically to empower defenders with speed, foresight, and precision to see first, act fast, and protect what matters most.

INDIA'S JOB MARKET COOLS IN JULY, BUT TECH ROLES POWER AHEAD

Formal employment slows, pay transparency dips, but high-skill demand drives resilience

India's job market experienced a noticeable cooling in July, with job postings on global hiring platform Indeed dropping by 5.8% month-on-month and 14.9% year-on-year. Despite this decline, the market remains significantly stronger than pre-pandemic levels, with postings still 70% higher than in early 2020. This suggests that while the hiring pace has moderated, the foundation of formal employment remains resilient.

According to the latest report from the Indeed Hiring Lab, the current slowdown follows a peak in January 2023. Since then, job postings have declined by 21%, reflecting a cyclical adjustment in the labor market. However, the data also reveals a deeper transformation: a shift toward high-skilled, formal roles, particularly in the technology sector.

Enterprise IT WORLD
India's Job Market Cools in July, but Tech Roles Power Ahead: Indeed Hiring Lab
www.enterpriseitworld.com

CALLAM PICKERING
APAC SENIOR ECONOMIST, INDEED

> "Even when overall hiring slows, **tech remains the heartbeat** of India's job market."

Tech Roles Defy the Downturn

Technology continues to be the engine of India's job market. One in every five job postings in July was for software development roles, underscoring the sector's dominance. Additionally, postings in data and analytics surged by 15.4% over the past three months, followed closely by logistics support (+14.3%), therapy (+13.7%), and dental roles (+13.6%).

This trend highlights a growing demand for specialized skills, even as broader hiring slows. "Even when overall hiring slows, tech remains the heartbeat of India's job market," said Callam Pickering, APAC Senior Economist at Indeed. "The challenge isn't demand — it's whether we can build a workforce skilled enough to meet it."

In contrast, several sectors saw notable declines. Medical information roles dropped by 12.3%, pharmacy by 10.7%, education by 8.0%, and physicians and surgeons by 7.8%. These figures point to a market increasingly tilted toward digital and high-skill professions.

Transparency Takes a Hit

Another key trend in July was a decline in pay transparency. Earlier in the year, over 50% of job listings included salary information. That figure has now slipped to 45%, raising concerns about candidate trust and hiring efficiency. Interestingly, transparency varied widely by sector. Childcare and dental roles were the most transparent, with 88% of listings disclosing pay. On the other hand, data and analytics (9.4%) and software development (18.3%) were among the least transparent.

"Employers who share pay details hold a clear competitive advantage, as transparency helps candidates make faster, informed decisions," the report noted. The drop in transparency could hinder hiring in already competitive sectors like tech, where skilled professionals often have multiple offers.

Skills Gap Widens

Despite a large labor force, India continues to face a significant skills mismatch. The demand for tech and management professionals far exceeds supply, reinforcing the urgent need for upskilling and workforce development initiatives.
The July data paints a picture of a labor market in transition — moving away from informal, low-skill roles toward structured, high-skill employment. Technology is not just surviving the slowdown; it's driving the next phase of growth.

As India navigates this evolving landscape, the focus must shift to building a future-ready workforce. With the right investments in education, training, and transparency, the country can turn this moment of moderation into a launchpad for long-term resilience. ENT

BALANCING INNOVATION, COST, AND SECURITY: INSIGHTS FROM INDUSTRY LEADERS

Enterprises must drive innovation with agility while maintaining disciplined cost structures, ensuring that transformation does not come at the expense of financial resilience.

BY SANJAY@ACCENTINFOMEDIA.COM

Enterprises operate in an environment of relentless change and business leaders are under constant pressure to innovate, adopt new technologies, and deliver superior customer experiences. Yet they must do so while managing costs, complying with regulations, and safeguarding operations against growing cyber risks. Striking the right balance between these competing priorities has become one of the defining challenges of digital transformation.

These challenges were the focus of a recent industry discussion moderated by Saumil Shah, Partner – Operations Transformation at Grant Thornton Bharat, where an eminent panel of IT and business leaders came together to share their perspectives. The discussion featured Anil Kumar Sharma, Group Head – Systems at Sabardairy (Amul Group); Dipen Chauhan, Senior Vice President (IT & ERP) at Gujarat Gas Limited; Juned Kasmani, Associate Director – Sales at Shivaami; Gaurav Vyas, Head IT at Stovec Industries Limited (SPG Prints); and Dr. Mukund KS, AVP & Group Head IT at Eris Lifesciences Ltd.

The discussion explored how organizations are navigating this balancing act in practical terms. From redefining how return on innovation is measured, reskilling workforces for future readiness, to balancing risk with speed of execution, the conversation reflected real trade-offs enterprises face every day. Cloud adoption and AI are reshaping IT strategy, while low-code/no-code platforms and blockchain promise cost-optimized pathways to modernization. At the same time, geopolitical tensions are driving enterprises to rethink cloud sovereignty and data ownership.

The panel explored how enterprises can strike the right balance to manage the complexities

JUNED KASMANI
ASSOCIATE DIRECTOR – SALES AT SHIVAAMI

"WHILE OPEN SYSTEMS ALLOW YOU TO BUILD AI FOR SPECIFIC PURPOSES, THE BROADER AND MORE SUSTAINABLE APPROACH IS TO ADOPT AI-AS-A-SERVICE. WITH TECHNOLOGY EVOLVING RAPIDLY AND INNOVATIONS LIKE BLOCKCHAIN TRANSFORMING INDUSTRIES SUCH AS SUPPLY CHAIN, BUSINESSES MUST FOCUS ON SOLUTIONS THAT ENSURE SCALABILITY, TRANSPARENCY, AND CUSTOMER TRUST."

of legacy versus modern systems, strengthen business and IT alignment, and address growing concerns around cloud security and cybersecurity. Their insights, drawn from real-world experience, highlight what it takes to build resilient, future-ready organizations in an increasingly digital-first economy.

Clearly innovation cannot be pursued in isolation—it must be grounded in business strategy, supported by measurable outcomes, and implemented in ways that secure both resilience and scalability. Below are the key themes that shaped the dialogue.

Finding the Sweet Spot Between Innovation and Cost

While innovation is often hailed as the lifeblood of competitive advantage, turning ideas into measurable busines value is far from straightforward. Many promising initiatives fail to deliver impact because they overlook feasibility, scalability, or cost considerations. The example of Netflix's million-dollar recommendation engine—an advanced solution that was ultimately abandoned because it was over-engineered and impractical to implement—highlights the danger of chasing innovation without considering feasibility and ROI.

For CIOs, the challenge is not simply to foster innovation but to balance it with cost control and operational realities. This requires a mindset that blends vision with pragmatism. Leaders must avoid the trap of endlessly refining pilot projects that never scale. Instead, adopt lean methodologies and design thinking to streamline the innovation cycle. By focusing on empathy, ideation, rapid prototyping, and iterative testing, organizations can reduce waste, fail fast, and quickly identify ideas that are truly worth scaling.

The 'sweet spot' lies at the intersection of four dimensions: practicality, cost, technology, and value. Practicality ensures solutions can be adopted and sustained within the organization; cost discipline keeps experimentation aligned with financial realities; technology provides the tools to enable transformation; and value guarantees that innovation drives tangible business outcomes. CIOs who successfully balance these dimensions evolve beyond technologists into business leaders—acting as visionaries shaping the future while being pragmatic to ensure that present remains stable.

Modernizing Legacy Systems: Bridging Technology and Business

One of the most difficult challenges in digital transformation is in modernizing legacy systems. In many industries, the resistance to change is often greater than the technical constraints themselves. Employees accustomed to traditional platforms may hesitate to adopt new systems, fearing disruption or loss of control. Overcoming this inertia requires a pragmatic, phased approach—starting small with pilot projects, layering modular systems on top of legacy environments, and using APIs to integrate old and new. By gradually demonstrating ROI, organizations can build user confidence and secure management buy-in for larger transformation initiatives.

At the same time, modernization is no longer just a technical exercise, but it is increasingly a business imperative. The traditional divide between IT and business is merging as technology now sits at the core of enterprise strategy. Boards

DR. MUKUND KS
AVP & GROUP HEAD IT AT ERIS LIFESCIENCES LTD

"THE DEFINITION OF ROI IS EVOLVING—FROM RETURN ON INVESTMENT TO RETURN ON IMAGINATION AND, ULTIMATELY, RETURN ON INNOVATION. MEASURING SUCCESS TODAY MEANS TRACKING HOW DIVERSE IDEAS ARE, HOW FAST THEY MOVE FROM CONCEPT TO REALITY, AND WHETHER EMPLOYEES TRULY ADOPT THEM. BY BUDGETING FOR EXPERIMENTATION AND LEARNING TO FAIL FAST, ORGANIZATIONS CAN TURN IMAGINATION INTO INNOVATION AND INNOVATION INTO REAL BUSINESS VALUE"

ANIL KUMAR SHARMA
GROUP HEAD – SYSTEMS AT SABARDAIRY (AMUL GROUP)

"THE BIGGEST BARRIER TO MODERNIZATION ISN'T TECHNOLOGY—IT'S RESISTANCE TO CHANGE. WHEN MOVING FROM LEGACY TO NEW SYSTEMS, THE KEY IS TO START SMALL: PILOT MODULAR SOLUTIONS, INTEGRATE GRADUALLY, AND SHOW ROI EARLY. THIS APPROACH NOT ONLY EASES USER ADOPTION BUT ALSO HELPS SECURE MANAGEMENT BUY-IN FOR BROADER TRANSFORMATION."

and CEOs expect IT to keep systems running while also driving innovation, reducing costs, and enhancing productivity. Business leaders are learning the language of technology, while IT leaders are aligning more closely with business outcomes. This convergence is transforming modernization efforts into a shared venture where technology directly enables new business models, smarter operations, and sustained growth. In this context, updating legacy systems is not just about replacing outdated infrastructure but about reimagining the way business and IT work together to unlock long-term value.

Securing the Cloud: From Resistance to Readiness

Cloud adoption, once resisted over concerns of data security and control, is now seen as a key enabler of digital transformation. Modern cloud platforms are designed with compliance and security at their core, offering robust device management, access controls, and data loss prevention (DLP). Hybrid models that combine on-premise and cloud flexibility, giving organizations control over sensitive data while enabling secure, scalable collaboration across geographies.

For regulated sectors like oil and gas, cybersecurity has become an operational necessity rather than a discretionary cost. The panel underscored that compliance with regulatory mandates and preparedness for geopolitical risks are central to cybersecurity strategy.

Just as airbags are now mandatory in cars, cybersecurity is becoming a basic requirement for doing business. As cyber threats evolves daily, proactive investments in security are vital for business continuity.

Measuring ROI from Innovation

Even as innovation is celebrated as the lifeblood of competitive advantage, converting ideas into measurable business value is a far more complex task. In many organizations, the definition of ROI is evolving beyond a narrow financial lens into a layered framework that captures the return on imagination, return on innovation, and ultimately, return on investment. This shift recognizes that ideas alone are not enough; they must be executed effectively, adopted widely, and aligned with strategic goals to create impact.

One of the biggest lessons for enterprises is the danger of over-engineering. The example of Netflix's abandoned million-dollar recommendation engine illustrates this point clearly. While technologically advanced, the solution proved impractical to implement and failed to deliver real business value. For CIOs, this underscores the importance of balancing vision with pragmatism. Innovation cannot be pursued for its own sake—it must be evaluated against feasibility, cost, and ROI.

To achieve this balance, organizations are increasingly turning to structured metrics. These include tracking the diversification of ideas across different business functions, measuring the speed of execution from concept to deployment, and monitoring stage-gate success rates to understand where pilots fail. Equally important is calculating the cost per idea, which allows businesses to identify weak concepts early and exit them before they drain resources. Employee adoption is also a critical measure, since engagement without real usage fails to translate into value.

A disciplined financial approach underpins

GAURAV VYAS
HEAD IT AT STOVEC INDUSTRIES LIMITED (SPG PRINTS)

"THE DAYS WHEN IT WAS JUST ABOUT UPTIME AND SECURITY ARE OVER—TODAY, IT IS THE BUSINESS. BOARDS NOW EXPECT TECHNOLOGY TO DRIVE INNOVATION, BOOST PRODUCTIVITY, AND REDUCE COSTS. IT'S NO LONGER ABOUT TECH VERSUS BUSINESS; IT'S A SHARED VENTURE WHERE IT LEADERS SPEAK THE LANGUAGE OF BUSINESS, AND BUSINESS LEADERS EMBRACE THE LANGUAGE OF TECHNOLOGY."

DIPEN CHAUHAN
SENIOR VICE PRESIDENT (IT & ERP) AT GUJARAT GAS LIMITED

> **"IN A REGULATED INDUSTRY LIKE OURS, CYBERSECURITY IS NO LONGER OPTIONAL–IT'S A BASIC REQUIREMENT OF DOING BUSINESS. WITH OVERSIGHT FROM REGULATORS AND THE CONSTANT SHADOW OF GEOPOLITICAL RISKS, WE MUST CONTINUOUSLY RAISE OUR DEFENSES. JUST AS CARS NOW COME WITH MANDATORY AIRBAGS, ENTERPRISES MUST TREAT CYBERSECURITY AS A BUILT-IN SAFEGUARD, NOT A COST CENTER."**

these efforts. Many organizations now allocate a fixed percentage of their IT budgets—often between 3% and 10%—specifically for experimentation. This innovation buffer provides room to test and fail fast, while ensuring that investments remain aligned with business priorities. It prevents pilots from dragging on indefinitely and gives leaders clear data on when to scale and when to cut losses.

Ultimately, measuring ROI from innovation requires CIOs to act as both visionaries and pragmatists. They must encourage bold ideas while demanding accountability through metrics. In doing so, enterprises can build a culture of innovation that is not only imaginative but also disciplined, ensuring that every experiment contributes to long-term business value.

Reskilling the Workforce to Enable Innovation

Cost pressures and talent shortages are pushing companies to focus on reskilling their existing workforce. Reskilled employees not only reduce reliance on external consultants but also become more motivated and productive, creating a virtuous cycle of innovation and efficiency. By equipping teams with new skills in emerging technologies, businesses can spread critical knowledge across departments and reduce single points of dependency. This not only drives cost savings but also builds resilience and agility in adapting to future demands.

Balancing Risk, Compliance, and Speed

Innovation cannot come at the cost of business continuity. Companies are drawing clear lines between core processes—such as ERP systems, billing, and cybersecurity—that must remain stable and uncompromised, and support functions where innovation can be piloted with lower risk. Many organizations are adopting a phased approach, testing new technologies in smaller units or specific geographies before scaling it enterprise-wide. This risk-managed innovation strategy ensures that while speed remains a priority, compliance and operational stability are never compromised.

Cloud Adoption and the Role of AI

Cloud adoption, once met with skepticism, has now become mainstream. Enterprises are realizing that the real cost advantage of cloud goes beyond infrastructure savings—it lies in simplified management, device-independent access, and higher productivity for employees. Browser-based, centrally managed solutions reduce downtime, cut license costs, and make IT operations more agile. With AI layered on top, cloud platforms are enabling smarter workflows, intelligent data access, and faster decision-making. Concerns about data security are being addressed with enterprise-grade safeguards, ensuring compliance even as businesses scale.

Emerging Technology Trends

Looking ahead, cost optimization will drive the adoption of low-code and no-code platforms, which allow businesses to innovate without heavy coding dependencies. AI-as-a-service is also emerging as a practical choice, enabling organizations to leverage advanced capabilities without the risk of being locked into one fast-changing technology. Meanwhile, blockchain is gaining traction in industries where transparency and traceability are critical, such as supply chain and agriculture, strengthening customer trust and operational reliability.

Cloud Sovereignty and Geopolitical Risks

While global cloud providers currently dominate the market, recent geopolitical events have raised questions about over-dependence on foreign players. Enterprises are becoming more aware of the risks of service disruptions and are increasingly considering sovereign cloud solutions. The push for India-owned cloud platforms reflects a broader shift toward ensuring data sovereignty and long-term resilience in the face of global uncertainties.

Striking the Right Balance

Today, enterprises recognize that while innovation is the path to progress, disciplined cost management is the key to sustaining it. From rethinking ROI frameworks and reskilling workforces to modernizing legacy systems and harnessing cloud and AI, corporate conversations increasingly center around the understanding that sustainable transformation rests on achieving the right balance—between cost and innovation, agility and stability. Innovation without feasibility leads to wasted investment, while excessive cost-cutting stifles growth and agility.

CIOs and business leaders must act as both visionaries and pragmatists. Lean approaches, phased pilots, and employee adoption are critical levers to ensure innovation translates into measurable business value. At the same time, technology and business must operate as a shared venture, with IT driving not just efficiency but also competitive advantage.

Ultimately, balancing cost and innovation is less about trade-offs and more about alignment—of technology with strategy, people with purpose, and risk with resilience. Organizations that achieve this equilibrium will not only weather disruption but also thrive in it, turning innovation into a disciplined, value-creating engine for long-term growth. As enterprises continue their digital journeys, leaders who can harmonize innovation, cost, and security will be best positioned to build resilient, future-ready organizations. ENT

CIO500 KOCHI EDITION: CELEBRATING LEADERSHIP AND RECONNECTING KOCHI'S RELEVANCE IN INDIA'S IT MAP

The CIO500 Kochi edition, powered by Secure Network Solutions (SNS), took place on 17th September at Le Meridien. It was not just another chapter in the nationwide CIO500 journey, but a meaningful effort to re-establish Kochi's position as a vital IT hub in India's growth story.

BY SANJAY@ACCENTINFOMEDIA.COM

The evening began with a warm welcome address by Sanjay Mohapatra, Editor, Accent Infomedia Publications, who set the context by highlighting why cities like Kochi must not be overlooked when discussing India's economic growth. "Kochi has always been a city of potential — with its talent, infrastructure, and global connectivity," Mohapatra said. "As India drives its digital economy, tier-2 cities like Kochi will play a crucial role in balancing opportunities and investments across regions."

A Milestone Celebration with SNS

This year's Kochi edition carried a deeper sense of pride, as SNS celebrated its 25th anniversary with the region's IT leadership community. For a cybersecurity brand that has spent a quarter of a century safeguarding enterprises, marking this milestone in Kochi reflected its commitment to strengthening the IT ecosystem beyond metros.

Mr. N.K. Mehta, CEO & MD of SNS, delivered an inspiring keynote, sharing insights on the evolving cybersecurity landscape and the growing role of AI in defending enterprise infrastructure. "The cyber threat landscape is changing faster than ever," Mehta remarked. "As enterprises adopt AI and digital platforms, our defenses must also evolve. At SNS, completing 25 years is not just about longevity; it's about adapting, innovating, and continuing to protect our clients in an unpredictable digital world."

To make the session interactive, Mr. Mehta also led an engaging Cybersecurity Quiz, alongside Tobola, which combined knowledge with fun and showcased the collaborative spirit of the Kochi IT community.

Knowledge Sessions and Panels

The event's learning sessions brought together respected thought leaders who addressed pressing themes at the intersection of technology, business, and strategy.

- Presentation by CyberArk: Akash Guruprasanna, Regional Sales Manager – South India and SAARC, outlined how identity and privileged access security are becoming cornerstones of enterprise defense. His presentation emphasized that as attackers target identities, resilience begins with securing users and access points.

Panel Discussion: Ensuring Scalable and Resilient IT Infrastructure with AI

Moderated by Kunnel Jose, Chief Delivery Officer, Magnum Networks Support Pvt. Ltd., the panel featured:

- Adarsh Nair, Global Head of Information Security Compliance, UST
- V.V. Jacob, Senior General Manager – IT, Malayala Manorama
- Vinodhkumar C, CTO, Muthoottu Mini Financiers Limited

The discussion revolved around practical strategies for harnessing AI to build infrastructure that is not only scalable but also adaptive and resilient in the face of rising cyber threats.

Panel Discussion: Navigating Boardroom Expectations and Digital KPIs

Moderated by Arun Kallaril, Associate Director, EY, the panel included:

- Sangeeth K Mohan, Associate VP IT (India & Sri Lanka), MANE
- Prince Joseph, Group CIO, NeST Group, SFO Technologies
- Nitha Sasi, Deputy CISO, Geojit Financial

PANEL DISCUSSION
NAVIGATING BOARDROOM EXPECTATIONS AND DIGITAL KPIS
MODERATOR
PANELLISTS
ARUN KALLARIL
Associate Director EY
NITHA SASI
Deputy CISO Geojit Financial Services Ltd.

SNSin 25 Enterprise IT WORLD
PRESENT
CIO 500 AWARDS
India's Largest Gathering of CIOs
Recognizing the Best IT Minds in the Industry
17 SEPTEMBER 2025 LE MÉRIDIEN, KOCHI
ORGANIZED BY
CHENNAI
HYDERABAD
BANGALORE
KOLKATA

Services Ltd.

This session explored how CIOs must bridge the gap between technology execution and board-level expectations. It focused on aligning IT outcomes with measurable KPIs, demonstrating value creation, and ensuring digital strategies resonate with business priorities.

Honoring Excellence: CIO500 & Accelerator X Awards

The event culminated in the CIO500 and Accelerator X Awards 2025, honoring senior IT leaders for their innovation, resilience, and contribution to the digital transformation journey. These awards recognized individuals who have shaped enterprise technology strategies and strengthened their organizations' competitiveness.

A Grateful Closing

The evening concluded with the vote of thanks delivered by Sanib Mohapatra, Publisher, Accent Infomedia Publications, who extended gratitude to all speakers, partners, delegates, and the host venue. "Events like this are possible only with

collaboration and shared vision," Sanib said. "We thank SNS, our speakers, our delegates, and especially Kochi's IT leaders for coming together to make this edition memorable." He also acknowledged the efforts of the Accent Info Media organizing team, the SNS family — with special mention to Anita Sengupta — and the Le Meridien staff for their seamless support.

Kochi's Reconnection with the Future

The Kochi edition of CIO500 was not just a celebration but a reaffirmation that Kochi remains an important IT employment and investment destination. With its strong talent pool, entrepreneurial spirit, and renewed attention from industry leaders, the city has a unique opportunity to contribute to India's next phase of digital growth.

As SNS celebrated 25 years of cybersecurity excellence, and as CIO500 continued its mission to honor India's IT leadership, Kochi stood out as a city ready to reclaim its place on the IT map — not just as a regional hub, but as a partner in India's economic journey. ENT

GUARDING THE GATEWAYS: WHY SUPPLY CHAIN SECURITY DEMANDS A NEW APPROACH

As global supply chains grow increasingly complex, organizations must prioritize data resilience and security to protect against evolving risks and disruptions

RICK VANOVER
VICE PRESIDENT OF PRODUCT STRATEGY
VEEAM SOFTWARE

> "Ensuring systems are operational is no longer enough. True resilience requires **a deeper understanding of how systems behave under** stress and how their failure impacts the broader supply chain."

In conversations around supply chain resilience, attention often centers on logistics, infrastructure, or supplier diversification. But because supply chains now rely heavily on digital systems, resilience also means having clear visibility into those systems. This includes the ability to understand what's happening across systems and the data flows that power supply chains, as well as the capacity to respond effectively when disruptions occur.

Unfortunately, many systems powering today's supply chains lack transparency. They are built on outdated software, complex integrations, or third-party components that few within an organization fully understand. These opaque environments make it difficult to detect weaknesses or recover efficiently following disruptions. Without clarity on what systems are doing and how they interact, recovery becomes uncertain and risk increases. These challenges aren't hypothetical. Recent findings show that only half of enterprises meet their recovery time objectives (RTOs) during real-world disruptions, despite widespread investment in backup and continuity strategies. Many organizations believe they're prepared, only to discover otherwise in the middle of a crisis.

Visibility gaps are especially pronounced in organizations where information technology (IT) and operational technology (OT) remain siloed. A lack of communication and shared accountability between these teams can delay responses, complicate recovery efforts, and introduce blind spots. In this context, visibility is no longer a nice-to-have capability; it's a fundamental element of business continuity.

Visibility as the cornerstone of resilience

Ensuring systems are operational is no longer enough. True resilience requires a deeper understanding of how systems behave under stress and how their failure impacts the broader supply chain. Visibility plays a critical role here. It's not just about detecting when something breaks, but also knowing what platforms and processes are in use, where third-party dependencies lie, and how different components interact in real time. Without that situational awareness, it's nearly impossible to anticipate points of failure or plan for effective recovery.

Yet too often, organizations struggle with unexamined complexity. Layers of software, inherited infrastructure, and siloed vendor tools obscure what's truly at risk. When an issue arises, teams may be forced to troubleshoot in the dark, wasting critical time.

A major contributor to these blind spots is the prevalence of "black box" systems — technology environments where inputs and outputs are visible, but the internal workings are not. Whether because of limited documentation, third-party control, or legacy design, these systems create uncertainty. In crisis situations, even identifying the root cause of an outage can be a challenge. If teams don't understand how a system functions or how it connects to others, recovery efforts can quickly stall.

This becomes especially problematic in environments where IT and OT functions are disconnected. Manufacturing, logistics, and other supply chain-intensive industries often rely on operational systems that don't easily communicate with newer digital platforms. Visibility gaps widen further when ownership of these systems is unclear or accountability is fragmented across departments. Without clear lines of responsibility and integrated system awareness, resilience remains out of reach.

Shifting the focus to recovery readiness

Modern resilience strategies must prioritize recovery as much as prevention. It's essential to know not only how systems can fail, but also how long disruption can be tolerated and how quickly functionality can be restored. Recovery readiness means proactively mapping dependencies, regularly testing systems under real-world conditions, and preparing for a wide range of scenarios, including those where third-party providers may not respond promptly.

Backup solutions may restore data; however, without a full picture of system interdependence,

To access the complete article log on to: **www.enterpriseitworld.com**

GROUP PHOTO
eventus Enterprise IT WORLD
CIO 500 AWARDS
India's Largest Gathering of CIOs
Recognizing the Best IT Minds in the Industry

CIO500 & ACCELERATOR X AWARDS 2025 POWERED BY EVENTUS AND CO-POWERED BY REDINGTON CONCLUDES ON A HIGH NOTE AT THE WESTIN GOREGAON, MUMBAI

A grand finale celebrating technology leadership, innovation, and business transformation

BY SANJAY@ACCENTINFOMEDIA.COM

The CIO500 & Accelerator X Awards 2025 powered by Eventus and co-powered by Redington, in association with Enterprise IT World, concluded successfully with a spectacular gathering at The Westin Goregaon, Mumbai on September 12, 2025. The event marked the culmination of a 10-city journey, recognizing over 500 CIOs and IT leaders across India for their exemplary contributions to business transformation, innovation, and digital modernization.

The Mumbai chapter drew an elite audience of industry leaders, decision-makers, and innovators. The day-long agenda combined keynotes, panel discussions, technology showcases, and networking, culminating in the prestigious Accelerator X Awards ceremony.

Key Highlights of the Mumbai Event

Musical Welcome: The day began with a soulful performance by Kirti Mishra and Band (KM).

Keynote Sessions:

- Apoorba Kumar Patranabish, Partner – Cyber Advisory, Grant Thornton Bharat, addressed the gathering on the growing importance of cyber resilience.
- Akash Sureka, Founder of TheNoah.ai, spoke on the transformative power of AI, stating that "AI is no longer a buzzword but a core driver of business strategy."

Panel Discussion 1: Balancing Innovation with Cost Control

Moderated by Abhik Basak, Global Security Director, LKQ Corporation.

Panellists:

- Satish Mahajan, Senior General Manager – IT, VFS Global Services
- Kumar Vinodanand, Sales Head – Enterprise BU, Motadata
- Kush Wadhwa, Partner – Crisis & Resilience, Grant Thornton Bharat
- Sunil Sonare, Vice President, Avinyasai Techsystems Pvt Ltd

Panel Discussion 2: Ensuring Scalable and Resilient IT Infrastructure & AI

Moderated by Rahul Patil, Partner – Cyber Advisory, Grant Thornton Bharat.

Panellists:

- Keyur Desai, Head IT, Prince Pipes and Fittings Ltd
- Ashok Kannan, President – IT, Luthra Group
- Satyavrat Mishra, Head – Corporate IT & Group CISO, Godrej Industries Group
- Vikas Somani, Vice President – Sales India, Eventus
- Sarjerao Tupsamudre, Global Lead – Cyber Security & Architecture, UPL

Panel Discussion 3: Navigating Boardroom Expectations & Digital KPIs

Moderated by Hetal Presswala, Cyber Security Advisor.

Panellists:

- Meheriar G Patel, Group CTO & Director IT, Master Group
- Abhay Karhade, CIO & VP IT, Indo Count Industries Ltd
- Krushna Sahoo, Director IT, JM Financial Services Ltd
- Ketan Patel, Vice President (CIO), Indoco Remedies Ltd

Technology Presentations:

- Jaimin Doshi, Global Head – Channel Partnerships, Techdefencelabs
- Vipul Kumar, SVP, CtrlS Datacenter
- Roscoe Lobo, Sales Leader – Data, AI & Security, IBM
- Nischay Kandpal, Redington
- Saurabh Barjatiya, Co-Founder & CTO, Cybervigilens
- Bhinang Tejani, TechOwl / Fortinet
- Chetana Chaudhari, CTO, Shivaami
- Jiten Motwani, Director – BD SOC, Eventus

Recognition, Networking, and Celebration

The evening concluded with the CIO500 & Accelerator X Awards powered by Eventus and co-powered by Redington, recognizing more than 80 CIOs and IT leaders from Mumbai and Western India. Sanjib Mohapatra, Publisher of Enterprise IT World, delivered the vote of thanks, acknowledging the contributions of CIOs in driving India's growth story.

A group photograph captured the spirit of achievement, followed by cocktails and dinner that enabled deeper peer-to-peer networking.

The 10-City Journey of CIO500 2025

The Mumbai edition was the final milestone of an ambitious journey that spanned Chennai, Hyderabad, Bangalore, Kolkata, Ahmedabad, Delhi, Pune, Kochi, Coimbatore, and Mumbai,

making it one of the largest CIO recognition platforms in India.

Speaking on the successful conclusion, Sanjay Mohapatra, Editor, Enterprise IT World, said: "CIO500 & Accelerator X Awards 2025, powered by Eventus and co-powered by Redington, has been more than just an awards program — it has been a platform for collaboration, knowledge-sharing, and celebration of leadership that drives India's digital future."

The success of the event was amplified by the unwavering support of partners: Eventus, Redington | Windows 11, CtrlS, Shivaami, Essen Vision | IBM, Techowl | Fortinet | SaveX Technologies, Cyber Vigilens, TechDefenceLabs, GrantThornton, eScan, Cache, ESET | Amity Infosoft, and Motadata.

"CIO500 Accelerator X Awards is more than just an award ceremony. It is a powerful platform for technology leaders to exchange ideas, collaborate with partners, and drive innovation across industries," said Sanjay Khera, Head of Marketing, Eventus. ENT

IDEAFORGE Q6V2 UAVS ASSIST JHARKHAND FOREST OFFICIALS IN PREVENTING HUMAN-ELEPHANT CONFLICT

Real-time aerial intelligence enables safe evacuation of villagers and guides herd back to forest without confrontation

Enterprise IT WORLD
ideaForge Q6V2 UAVs Assist Forest Officials in Preventing Human-Elephant Conflict in Jharkhand
www.enterpriseitworld.com

> "Our UAV provided forest officials with the speed, accuracy, and intelligence **needed to protect both villagers and wildlife, while** ensuring zero disturbance to the animals."

In a compelling demonstration of how technology can aid conservation, ideaForge Technology Limited, India's leading UAV manufacturer, successfully deployed its Q6V2 drone to help forest officials in Jharkhand prevent a potentially dangerous human-elephant conflict. The operation took place in the Silli region, where a herd of elephants had wandered into nearby villages, triggering panic among residents. The mission was executed in collaboration with Sathi Planners Pvt. Ltd. (SPPL), a channel partner of ideaForge, under the leadership of the Divisional Forest Officer, Ranchi. The Q6V2 UAV, equipped with both daylight and night vision payloads, provided uninterrupted surveillance across dense forest terrain and village boundaries.

Eyes in the Sky, Safety on the Ground

The Q6V2's high-definition optical and thermal imaging capabilities enabled real-time, geo-tagged situational awareness, even in low-light and rainy conditions. This allowed forest officials to track the elephants' movements with precision, anticipate their direction, and take proactive measures.

Armed with this intelligence, authorities were able to alert villagers in advance, facilitate safe evacuations, and guide the elephants back to their natural habitat — all without direct confrontation. The drone's silent operation and long endurance ensured continuous monitoring, which was critical in coordinating a safe and humane response.

A New Era in Wildlife Management

This successful deployment underscores the growing role of drone-enabled intelligence in wildlife and forest management. Traditional methods of monitoring wildlife often face limitations due to challenging terrain, poor visibility, and delayed response times. UAVs like the Q6V2 bridge these gaps, offering a faster, safer, and more efficient alternative.

The incident also highlights how technology can serve both conservation and community safety. By preventing a potentially deadly encounter, the operation not only protected human lives but also ensured the elephants were not harmed or stressed — a win-win for both sides.

A Model for Future Deployments

As human-wildlife interactions become more frequent due to habitat encroachment and climate change, real-time aerial intelligence is emerging as a vital tool for forest departments across India. The success in Jharkhand could serve as a blueprint for similar interventions in other conflict-prone regions.

With its rugged design, advanced sensors, and autonomous capabilities, the Q6V2 is proving to be more than just a surveillance tool — it's becoming an essential asset in modern conservation strategy. ENT

CIO500 PUNE CELEBRATES ICT LEADERSHIP WITH AWARDS, INSIGHTS, AND A UNIQUE QUIZ EXPERIENCE

After Chennai, Hyderabad, Bangalore, Kolkata, Ahmedabad, and Delhi, the CIO500 journey reached Pune with a full house at Hotel Hyatt Regency Viman Nagar, recognizing more than 80 ICT leaders for their industry contributions.

BY **SANJAY**@ACCENTINFOMEDIA.COM

Pune Hosts a Power-Packed Gathering of Technology Leaders

The Pune chapter of the prestigious CIO500 & Accelerator X Awards 2025 unfolded at Hotel Hyatt Regency, Viman Nagar, with an overwhelming response from the region's technology community. Following its successful editions in Chennai, Hyderabad, Bangalore, Kolkata, Ahmedabad, and Delhi, the Pune event drew a houseful audience of CIOs, CISOs, and senior ICT decision-makers, marking yet another milestone in the nationwide celebration of India's digital leadership.

The evening was dedicated to acknowledging and honoring over 80 CIOs and senior ICT leaders who have made remarkable contributions in driving transformation, resilience, and growth within their organizations. The recognition reinforced CIO500's mission of creating a platform where IT leaders are celebrated not only for their technology acumen but also for their role in shaping business outcomes.

Spotlight on Awards and Recognition

The awards ceremony was the central attraction of the event, where ICT leaders from diverse industries were recognized for their achievements in areas such as digital transformation, cybersecurity, innovation, automation, and cloud strategy. Each award was a testimony to the relentless efforts of CIOs who are enabling enterprises to thrive in today's rapidly evolving digital economy.

By spotlighting such leaders, CIO500 continues to create a community of excellence, empowering CIOs to share experiences, learn from peers, and inspire the next generation of technology leadership.

An Evening with a Twist: Quiz by NK Mehta

One of the most engaging highlights of the Pune edition was the interactive quiz competition conducted by NK Mehta, CEO & MD of Secure Network Solutions (SNS). Known for his innovative and people-centric approach, Mehta brought a lively twist to the awards night, energizing the audience and adding an element of fun learning to the program.

The quiz not only tested participants' knowledge of ICT and digital trends but also sparked healthy competition and collaboration, reflecting the spirit of curiosity and innovation that defines the CIO500 community.

A Celebration of Collaboration and Innovation

The Pune event was not just about recognition, but also about networking, collaboration, and dialogue. Senior technology leaders exchanged perspectives on emerging priorities such as cyber resilience, AI adoption, digital KPIs, and future-

SANJ
Editor, En

NGH PUNJABI
ader

THARO
CONC
FIE WITH 6 WOMEN MPs
ER ISSUES APOLOGY
INDIA TODAY
© 2025 Secure Network Sol

PANEL DISCUSSION
ENSURING SCALABLE AND RESILIENT IT INFRASTRUCTURE AND AI
MODERATOR
PANELLISTS
HATAWADEKAR
RAJEEV KH
AVINASH
DR. ATUL ANAND
Director IT
Cencora
SNSin
India's Largest Gathering of CIOs

RAJEEV M
Chief Information
Endurance Techno

PANEL DISCUSSION
NAVIGATING BOARDROOM EXPECTATIONS AND DIGIT KPIS
MODERATOR
NELLISTS
PANKAJ
Founder
Digizen C

SNSin
Enterprise IT WORLD
PRESENT
CIO 500 AWARDS
India's Largest Gathering of CIOs
Recognizing the Best IT Minds in the Industry
CHENNAI
HYDERABAD
BANGALORE
KOLKATA

AKA
Head Pro

ready infrastructure. This dialogue reinforced the role of CIO500 as a knowledge-sharing ecosystem where leaders from different industries can connect and collectively address the opportunities and challenges of the digital era.

"Every city edition of CIO500 brings its own flavor, and Pune stood out with its energy, innovation, and the sheer enthusiasm of its ICT community," Mohapatra added.

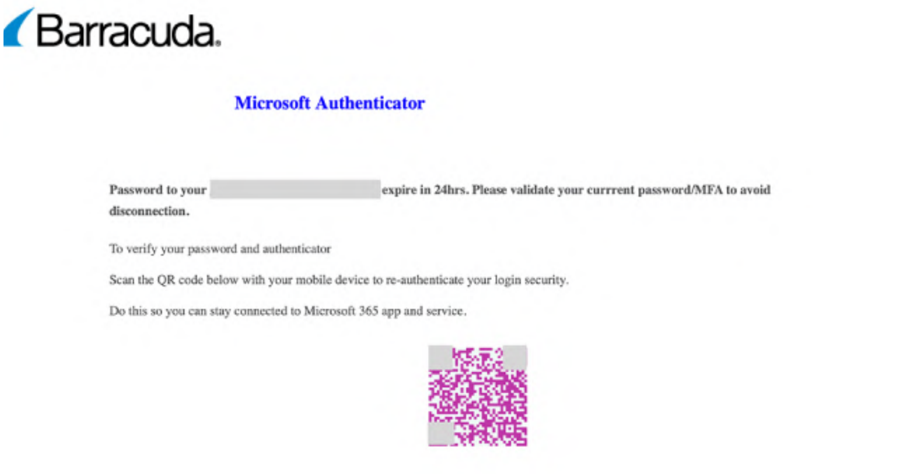
The Road Ahead for CIO500

With Pune adding another successful chapter, the CIO500 journey continues to expand its footprint across India, celebrating the people behind the digital revolution. By recognizing CIOs and ICT leaders city by city, CIO500 has established itself as one of the most credible and prestigious platforms for technology leadership recognition in the country.

As the event series heads to its final stages, it leaves behind a trail of inspiration, recognition, and collaboration, amplifying the message that India's digital future is in safe hands, guided by visionary CIOs and ICT leaders.

QR CODE PHISHING EVOLVES: BARRACUDA UNCOVERS ‘QUISHING’ ATTACKS USING SPLIT AND NESTED CODES

New techniques in QR-based phishing campaigns evade traditional scanners, highlighting the need for integrated AI defenses



Barracuda.

Microsoft Authenticator

Password to your [redacted] expire in 24hrs. Please validate your currrent password/MFA to avoid disconnection.

To verify your password and authenticator

Scan the QR code below with your mobile device to re-authenticate your login security.

Do this so you can stay connected to Microsoft 365 app and service.

SARAVAN MOHANKUMAR
MANAGER, THREAT ANALYSIS, BARRACUDA

> “Attackers are innovating with split and nested QR codes to **bypass traditional security, taking users outside the corporate perimeter.** AI-powered, multi-layered protection is essential to stay ahead.”

In a stark reminder of how rapidly cyber threats are evolving, Barracuda Networks has uncovered a new wave of QR code phishing attacks, or ‘Quishing,’ that use split and nested QR codes to evade detection. These sophisticated techniques are designed to bypass traditional email security filters and exploit the growing reliance on mobile devices for scanning QR codes.

Quishing attacks typically embed malicious links within QR codes, redirecting unsuspecting users to fake websites that harvest credentials or sensitive data. But the latest campaigns, analyzed by Barracuda’s threat intelligence team, reveal a disturbing level of innovation.

Split and Nested QR Codes: A New Threat Vector

Barracuda’s report highlights two advanced tactics:

- Split QR Codes: In this method, a single malicious QR code is divided into two separate images placed side by side. While they appear harmless to the human eye, they confuse traditional email scanners, allowing the malicious payload to slip through undetected. This technique was notably used in phishing campaigns powered by the Gabagool phishing-as-a-service (PhaaS) kit, which impersonated Microsoft password reset alerts.
- Nested QR Codes: Here, attackers embed a malicious QR code within or around a legitimate one. The outer code leads to a phishing site, while the inner code may redirect to a trusted domain like Google. This layered approach, seen in attacks using the Tycoon PhaaS kit, creates ambiguity for scanners and users alike.

Mobile Devices: The Weak Link

“Malicious QR codes are attractive to attackers because they look legitimate and bypass standard filters,” said Saravan Mohankumar, Manager of Threat Analysis at Barracuda. “Since users often scan them on mobile devices, they are outside company protections, making these attacks harder to detect and prevent.”

This shift toward mobile-targeted phishing is particularly concerning for enterprises, as mobile devices often operate outside the traditional corporate security perimeter. Once a user scans a malicious QR code, they are taken to a phishing site that may look identical to a legitimate login page, increasing the likelihood of credential theft.

AI-Powered Defense is Key

To counter these evolving threats, Barracuda recommends a multi-layered security strategy that includes:

- Security awareness training to help users recognize suspicious QR codes.
- Multi-factor authentication (MFA) to reduce the impact of stolen credentials.
- Advanced spam filters that can detect image-based threats.
- Multimodal AI-powered email protection capable of decoding and inspecting QR codes in real time, even when obfuscated.

These measures are essential to stay ahead of attackers who are constantly refining their tactics to exploit human behavior and technological blind spots.

The Road Ahead

As QR codes become more embedded in everyday workflows — from restaurant menus to corporate logins — the attack surface continues to expand. The emergence of split and nested QR code attacks signals a new chapter in phishing, where visual deception and mobile-first targeting are the weapons of choice.

Organizations must evolve their defenses accordingly, embracing AI-driven, context-aware security solutions that can adapt as quickly as the threats themselves. ENT

DIGITATE'S OPENTELEMETRY INTEGRATION BRINGS CIOS CLOSER TO SELF-HEALING IT

Vendor-neutral observability and AI-driven automation promise cost savings, resilience, and faster business outcomes for enterprises

AMIT SHASTRI
FIELD CTO, DIGITATE

> "CIOs need freedom from tool sprawl and vendor lock-in. By combining **OpenTelemetry with ignio's AI and automation, we are enabling** enterprises to achieve predictive and autonomous IT operations."

In the age of digital acceleration, CIOs are under constant pressure to deliver resilient, cost-efficient, and agile IT operations. Yet, despite spending millions on monitoring and observability tools, many enterprises still grapple with fragmented visibility, vendor lock-in, and mounting operational costs. Digitate, a global leader in AI-driven enterprise solutions, has stepped into this gap with the integration of OpenTelemetry™ (OTel) into its flagship ignio™ platform—a move that brings enterprises closer to achieving truly self-healing IT.

The Promise of Vendor-Neutral Observability

OpenTelemetry has rapidly emerged as the global standard for telemetry data collection, offering enterprises the flexibility to consolidate metrics, events, logs, and traces (MELT data) without being tied to proprietary tools. By embedding OTel into ignio, Digitate provides CIOs with a vendor-neutral, future-ready observability layer that cuts across hybrid and multi-cloud environments.

The integration goes beyond visibility. When combined with ignio's AI-powered intelligence and closed-loop automation, it empowers IT teams not only to detect anomalies and trace their root causes faster but also to resolve them autonomously.

Three-Pronged Strategy for CIOs

With OTel embedded, Digitate strengthens ignio's three-pillar approach to modern IT operations:

- Visibility: Providing a real-time, end-to-end view of both IT health and its impact on business outcomes.
- Intelligence: Leveraging AI-driven insights for predictive detection and faster root cause analysis.
- Automation: Enabling self-healing through closed-loop remediation that reduces MTTR (mean time to resolution) and minimizes manual intervention.

For CIOs navigating boardroom scrutiny, this triad is a blueprint for resilience. It translates to fewer outages, lower costs, improved compliance, and a scalable IT backbone that supports innovation.

Tackling the CIO Paradox

Industry analysts highlight that the move comes at a pivotal moment. Enterprises are investing heavily in monitoring and operations tools, but without interoperability and automation, the returns are diminishing. Fragmented visibility, tool sprawl, and escalating costs have left many CIOs stuck in reactive firefighting.

"Organizations are investing heavily in monitoring, yet they remain constrained by vendor lock-in and limited interoperability," said Shastri. "Our OTel-powered ignio platform gives them the freedom to operate in a truly open, scalable, and future-ready manner."

The significance of this move lies in shifting the narrative from tool-centric monitoring to business-centric resilience. By unifying observability data and automating incident response, Digitate positions ignio as more than just another IT operations tool—it becomes a strategic enabler of autonomous enterprises.

ROI in Business Outcomes

For business leaders, the integration promises measurable ROI. Enterprises can expect:

- Reduced downtime: Faster detection and resolution of incidents.
- Cost efficiency: Elimination of redundant monitoring tools and reduced manual intervention.
- Compliance and resilience: Improved auditability and risk management.
- Future scalability: The ability to evolve IT operations seamlessly with digital transformation demands.

To access the complete article log on to:
www.enterpriseitworld.com

MARUT DRONES' SKYSWIFT 56 SECURES DGCA TYPE CERTIFICATION

Indigenously developed surveillance drone strengthens India's law enforcement, training ecosystem, and UAV ambitions

PREM KUMAR VISLAWATH
CEO & CO-FOUNDER, MARUT DRONES

> "Skyswift 56 is built to empower frontline personnel with silent, **compact, and high-precision surveillance tools — crucial for** national security and public safety."

Marut Drones, India's pioneering drone manufacturer and the country's first with dual certification for both training and manufacturing, has achieved another milestone. Its latest innovation, the Skyswift 56, has secured DGCA type certification, marking a significant step forward in India's journey toward building a self-reliant and robust UAV ecosystem.

The Skyswift 56 is a small-category quadcopter-class rotorcraft designed for tactical surveillance, high-precision mapping, and field training. At a time when national security and public safety have become critical priorities, the platform represents a leap in capability for law enforcement and defense agencies, offering speed, precision, and resilience in diverse operational scenarios.

Tactical Power in a Compact Form

Marut has built Skyswift 56 with frontline operatives in mind. The drone can be deployed in under two minutes, fits conveniently into a rugged backpack, and functions effectively even in low-visibility missions. With speeds of up to 15 m/s and a shock-absorbent, weather-resistant design, it provides an optimal mix of discretion, rapid deployment, and resilience—qualities essential for tactical reconnaissance, covert operations, and disaster response.

Supporting multiple payloads, including an FPV camera, a 24MP mapping camera with PPK support, a 4K surveillance lens, and thermal imaging capabilities, Skyswift 56 adapts to varied mission requirements. This flexibility makes it a multi-role asset for both civilian and defense needs, ranging from monitoring and security patrols to search-and-rescue operations.

Strengthening Law Enforcement and Security

For agencies tasked with maintaining security in complex environments, Skyswift 56 offers much-needed agility. Its ability to operate silently and withstand adverse conditions provides an edge in surveillance and tactical missions, enhancing situational awareness and enabling quicker, data-driven decision-making.

"At a time when national security concerns are prompting deeper investments in tactical drone surveillance, Marut's Skyswift 56 emerges as a timely solution," noted Prem Kumar Vislawath, CEO & Co-Founder, Marut Drones.

Boost to India's Drone Economy

Beyond its tactical advantages, Skyswift 56 also supports India's broader drone ecosystem goals. With the government targeting more than 1 lakh skilled drone pilots and aiming to grow the drone economy from USD 150 million today to over USD 630 million by 2030, certified platforms like Skyswift 56 are poised to play a central role.

Currently, India has over 1 lakh drones in operation, a figure projected to reach 1 million by 2027. Marut estimates that this expansion could create employment worth INR 6000 crore, with certified drone pilots earning between INR 50,000 to INR 80,000 per month.

By aligning technological innovation with skill development, Marut Drones is not only contributing to national security but also addressing the demand for jobs in the fast-growing UAV sector. Reinforcing Indigenous Leadership

With this certification, Marut Drones reaffirms its leadership in indigenous drone manufacturing. The company has been at the forefront of developing UAVs that support agriculture, logistics, healthcare, and law enforcement, making it one of the most versatile players in the sector.

By designing Skyswift 56 locally and tailoring it to India's operational and climatic conditions,

To access the complete article log on to: www.enterpriseitworld.com

ESCAN STRENGTHENS CIO CONNECT WITH ENTERPRISE SECURITY SUITE AT CIO 500 INTERCITY EVENTS

Enterprise DLP and unified management console draw strong interest from CIOs across six major cities as the company gears up for Mumbai chapter

SHWETA THAKARE
GLOBAL VICE PRESIDENT, SALES AND MARKETING, ESCAN

> "CIOs today are not just protecting IT **assets, they are enabling business growth, and our unified** platform empowers them to achieve both."

EScan, a global leader in IT security solutions, has been making strong strides across India's CIO community through its active participation in the CIO 500 Intercity events. Showcasing its flagship Enterprise Security Suite, eScan has engaged directly with CIOs across Delhi, Hyderabad, Bangalore, Kolkata, Chennai, and Ahmedabad. With these successful chapters completed, the company now sets its sights on the upcoming Mumbai edition, continuing its mission to bridge enterprise needs with cutting-edge security innovation.

Enterprise DLP Takes Center Stage

At the heart of CIO discussions has been data protection in hybrid and remote work environments. eScan's Enterprise Data Loss Prevention (DLP) module has generated significant interest, reflecting CIO concerns over insider threats, unintentional data leaks, and regulatory compliance. With enterprises increasingly handling sensitive information across distributed workforces, DLP is no longer viewed as a "nice to have" but as a business-critical safeguard.

The Enterprise Security Suite extends well beyond DLP, encompassing Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Enterprise Mobile Management (EMM). This comprehensive portfolio has been positioned as a unified response to escalating cyber risks, offering both depth of defense and operational simplicity.

"Our interactions at CIO 500 reaffirmed what we've always believed – cybersecurity should be powerful yet easy to manage. CIOs today are not just protecting IT assets, they are enabling business growth, and our unified platform empowers them to achieve both," said Shweta Thakare, Global Vice President, Sales and Marketing, eScan.

Solving the Multi-Console Challenge

One of the standout features resonating with CIOs has been eScan's unified management console. Enterprises have long struggled with fragmented tools, siloed dashboards, and overwhelming alert volumes. eScan's platform consolidates operations across Windows, Mac, Linux, and mobile ecosystems, giving security leaders a single pane of glass to manage threats.

This consolidation not only improves visibility but also streamlines workflows, enabling teams to respond faster to incidents with reduced dependency on scarce cybersecurity talent. In an industry marked by skill shortages and rising complexity, this ease of management is proving to be a critical differentiator.

Grounded in Real-World CIO Challenges

The CIO 500 forums have provided eScan with direct insights from the frontlines of enterprise IT security. From insider threat detection and zero-day attack response to phishing simulations and behavioral analysis, the questions posed by CIOs reflect the growing sophistication of both threats and boardroom expectations.

"From a strategic point of view, these events help us stay grounded in real-world challenges rather than getting caught up in theoretical security scenarios. The questions we received — about insider threat detection, zero-day response, phishing simulation, and long-term behavioral analysis — directly influence our development priorities," said Govind Rammurthy, CEO and Managing Director, eScan.

This customer-centric approach ensures that eScan's product roadmap evolves hand-in-hand with enterprise realities, aligning innovation with practical value.

To access the complete article log on to: www.enterpriseitworld.com

zeroday ops

TATTVA
UNLOCKING CYBER CONFIDENCE

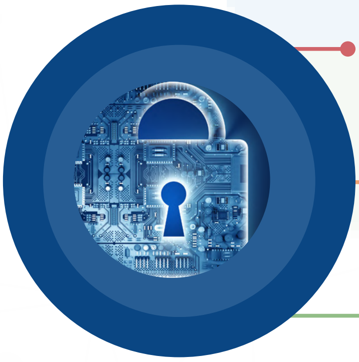
OUR SERVICES

- DORA
- PCI DSS
- ISO/IEC 27001 / 27701
- GDPR
- AI MANAGEMENT SYSTEM ISO 42001
- TISAX
- HIPAA
- ISO 9001, 45001, 14001
- SOC2/SSAE ATTESTATIONS TYPE I & II

VAPT

- Firewall PT
- Web Application
- Mobile Application
- Cloud
- Network
- API

TRAININGS & SIMULATIONS



- Compliance and Data Privacy Training
- Phishing Simulations
- Multi Lingual Support for Content (Security Awareness Training Content)
- RED Teaming
- Cyber Challenge
- Role-Based Courses
- Infosec Trainings
- Ransomware Simulations

PCI DSS | ISO 27001 | ISO 27701 | GDPR | SOC 2 | HIPAA

info@5tattva.com

www.5tattva.com | www.zerodayops.com

+91-9810005685 +1-(347)298-0694

+506-6152-3953 +971 50 328 9600

LinkedIn X Facebook

“Empowering secure, compliant, and resilient digital ecosystems.”

RNI NO: DEL ENG/ 2017/ 69906
Postal Reg. No.: DL-SW-01 / 4200 / 17-19

Date of Publication: 15 of Every Month
Date of Posting: 1 & 2 of Every Month