INDIA'S FRONTLINE IT MAGAZINE

# VARINDIA

THE ULTIMATE *Voice* OF INDIAN VALUE ADDED RESELLERS

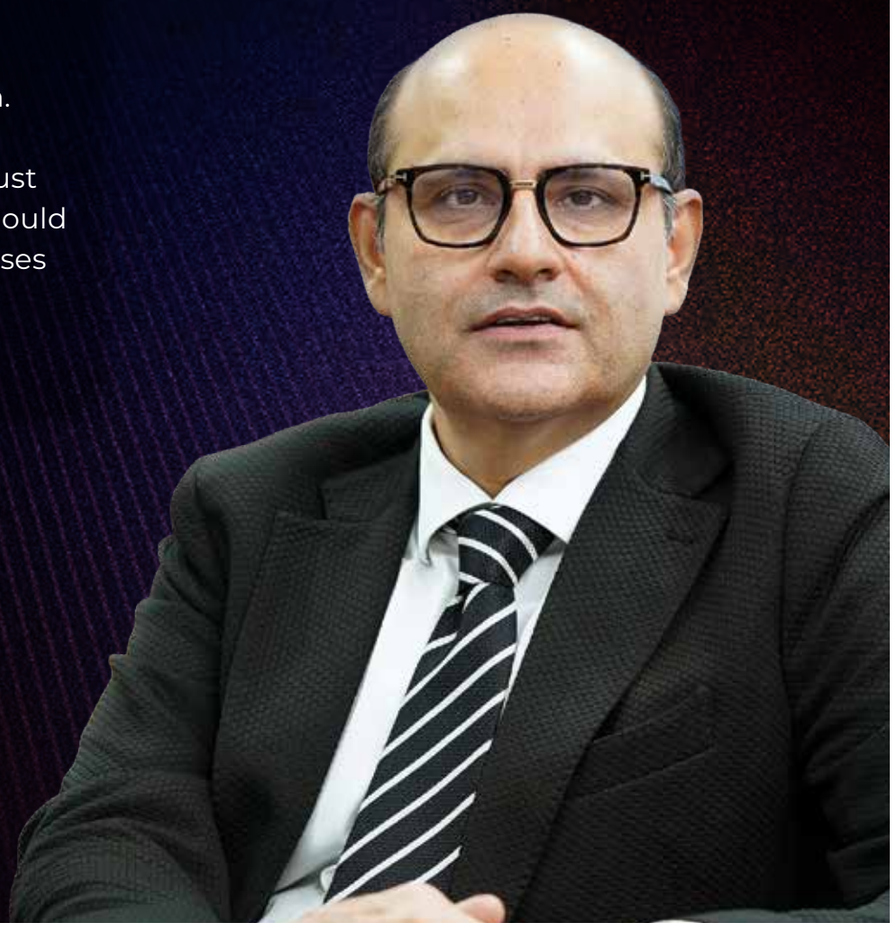


VOLUME XXVII ISSUE 09 MAY 2026 PRICE RS. 50

IRIS GLOBAL

# IRIS 2.0
## THE LEADERSHIP CONVERSATION
### FROM DISTRIBUTION TO INTELLIGENCE

"Iris.ai is the intelligence layer of the **IRIS 2.0 vision**. It represents our commitment to building connected entperprise ecosystems powered by intelligence, automation & innovation. The idea is simple - Technology should not just support businesses. It should rather empower businesses to think smarter & move faster."



**ANIL SETHI**
CEO
**Iris Global Ltd**

एनटीपीसी
NTPC

# 50 YEARS OF POWERING INFINITE POSSIBILITIES FOR INDIA

एनटीपीसी NTPC

50 YEARS

OF POWERING GROWTH

For 50 years, NTPC has been a key force behind India's rise. From a modest beginning, it has emerged as a powerhouse of innovation, helping India realise its dreams. NTPC powers industries, uplifts communities and touches people's lives in myriad ways. As a trusted energy leader, NTPC is now championing India's journey towards clean, sustainable power for all and a Viksit Bharat by 2047.

### Powering Progress for a Resilient Future

A target of 130 GW by 2032 on the back of a strong portfolio across conventional, RE sources and nuclear plans

### A Trusted Source of Energy

Lighting every fourth bulb in the country, and ensuring reliable, affordable supply of power

### Empowering Lives Beyond Energy

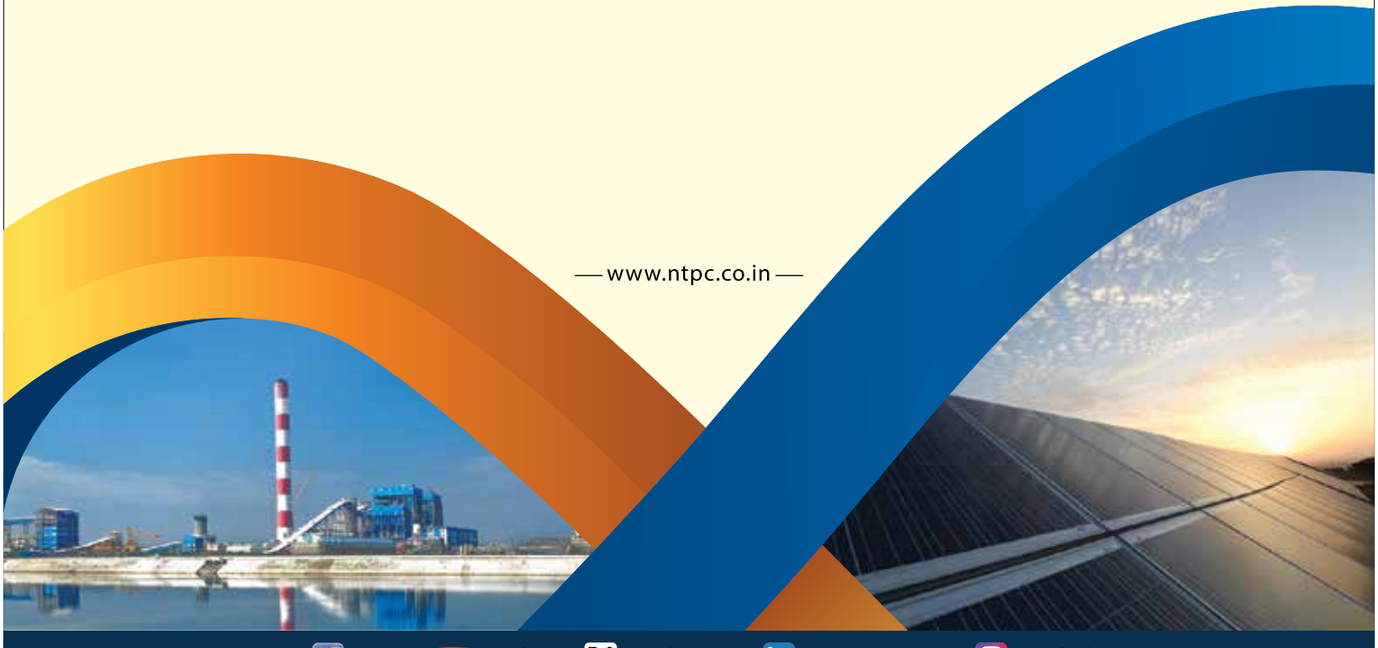
Serving communities, protecting environment, and securing biodiversity for inclusive growth

### Innovating for a Greener Tomorrow

A leader in floating solar, green hydrogen, e-mobility, carbon capture, biofuels and energy storage solutions

### Sustainability at its Core

Driven by a 'People, Planet, Prosperity' approach, NTPC is steadily marching towards a Net Zero future



— www.ntpc.co.in —

Visit: /ntpc1 /ntpcltd1 /ntpclimited /company/ntpc /ntpclimited

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS



VOLUME XXVII ISSUE 09 MAY 2026 PRICE RS. 50 SUBSCRIPTION COPY NOT FOR SALE

**MULTI-CLOUD, EDGE, SERVERLESS: WHAT IT MEANS FOR INDIA BUSINESSES**

PAGE 38

## SK Hynix and Micron join global trillion-dollar club amid AI boom

Riding the wave of growing demand for AI infrastructure and advanced semiconductors, memory-chip makers SK Hynix and Micron Technology have crossed the $1 trillion market valuation milestone. SK Hynix, the world's second-largest memory chip manufacturer, has seen its share price more than triple this year, lifting its market value to around $1.06 trillion. Micron also entered the trillion-dollar club following a strong rally in its stock. The achievement reflects rising investor confidence in AI-driven semiconductor companies and the critical role memory chips play in the expanding AI ecosystem.

## Samsung marks 30 years of customer service operations in India

Samsung has completed 30 years of customer service operations in India, marking its evolution from a single service centre in Delhi in 1996 to a nationwide support network. The company now operates more than 3,000 service touchpoints supported by over 12,500 engineers across the country. Samsung said its customer care ecosystem has transformed from manual complaint handling to AI-enabled support, including remote diagnostics, WhatsApp assistance and SmartThings-powered monitoring. The company has also expanded accessibility through multilingual support while promoting skill development and sustainability initiatives across its service operations.

# BEYOND MODELS: THE NEXT AI BATTLEGROUND

Artificial Intelligence has entered a new phase of evolution. The competition is no longer limited to building larger language models or achieving benchmark superiority. Instead, AI is transforming the foundations of the global technology ecosystem, influencing infrastructure, software engineering, cybersecurity, energy, financial services, and public policy. As organizations accelerate AI adoption, the focus is shifting from experimentation to enterprise-scale deployment, making AI a core pillar of economic and industrial strategy.

Technology companies are investing in AI, automation, cybersecurity, semiconductor innovation, cloud infrastructure, and immersive digital experiences to stay competitive and adapt to the upcoming technology revolution. Technology leaders are quietly preparing for the next wave of disruption. OpenAI is rethinking its infrastructure strategy to gain greater control over computing resources and reduce dependency on external providers. Meta is reorganizing its operations around AI computing, investing heavily in custom chips, data centers, and AI research. Microsoft is strengthening its cloud and AI ecosystem while preparing for increased regulatory scrutiny. AWS, meanwhile, is making substantial investments in autonomous AI agents that could redefine enterprise software and cloud consumption models.

At the center of this transformation is compute infrastructure. The explosive demand for AI training and inference has created an unprecedented need for advanced processors, GPUs, networking equipment, and high-performance computing environments. Technology giants are building AI factories powered by thousands of specialized chips, while cloud providers are expanding hyperscale facilities to support growing enterprise workloads. Control over compute capacity is increasingly becoming a strategic advantage in the AI economy.

The rapid growth of AI is also reshaping the energy sector. Large-scale AI deployments require enormous amounts of electricity, cooling systems, and resilient infrastructure. Governments and enterprises are investing in renewable energy, advanced power grids, small modular nuclear reactors, and energy-efficient computing architectures. The intersection of AI and energy has become a matter of national competitiveness, with countries seeking to secure sufficient power resources to support future digital growth.

Software development is undergoing its most significant transformation in decades. AI-powered coding assistants, low-code platforms, and autonomous development tools are enabling developers to create applications faster than ever before. Tasks that once required weeks of effort can now be completed in hours. However, this acceleration introduces new risks, including software vulnerabilities, governance challenges, and the need for continuous validation of AI-generated code.

The emergence of AI agents represents another major shift. Unlike traditional assistants that respond to prompts, AI agents can plan, reason, execute tasks, and interact with multiple systems autonomously. Organizations are exploring the deployment of thousands of digital workers across customer service, finance, cybersecurity, software development, and operational functions. This evolution is creating a new software economy where intelligent systems become active participants in business processes rather than passive tools.

The high cost of GPUs, power, and massive token consumption is making fully autonomous AI systems unexpectedly expensive. To manage these costs and minimize errors, organizations are shifting toward Human-in-the-Loop (HITL) models.

Microsoft's Agent Framework exemplifies this approach by requiring human approval for critical actions. The future of enterprise AI lies in combining human judgment with AI productivity, delivering more reliable, scalable, and cost-effective outcomes rather than complete automation.

Cybersecurity is simultaneously becoming more complex. While AI strengthens threat detection and automated response capabilities, it also empowers adversaries with sophisticated attack techniques. Deepfakes, synthetic identities, automated phishing campaigns, and AI-generated malware are raising the stakes for enterprises. Security strategies are therefore evolving toward real-time monitoring, behavioral analytics, identity-centric controls, and AI-driven defense mechanisms capable of responding at machine speed.

Financial services and wealth management are experiencing profound disruption as AI transforms decision-making and customer engagement. Intelligent systems now analyze market movements, customer preferences, risk factors, and economic trends in real time. Financial institutions are leveraging AI for fraud prevention, compliance automation, portfolio optimization, and personalized advisory services. This is improving efficiency while creating new opportunities for financial inclusion and digital innovation.

Regulation has emerged as a critical factor shaping the future of AI. Governments worldwide are introducing frameworks covering AI transparency, privacy, digital identity, cybersecurity, and responsible innovation. Technology companies are investing heavily in governance structures, compliance mechanisms, and trust architectures to navigate an increasingly complex regulatory environment. Success will depend not only on technological leadership but also on the ability to align innovation with accountability and societal expectations.

The next decade of disruption will be defined by the convergence of AI, cloud infrastructure, energy systems, cybersecurity, autonomous agents, and regulatory frameworks. The companies that succeed will not necessarily be those with the most powerful models, but those capable of integrating intelligence, scale, resilience, and trust into sustainable ecosystems. AI is no longer just a technology trend—it is rapidly becoming the foundational infrastructure upon which future industries, economies, and societies will be built.

**S. Mohini Ratna**
**Editor, VARINDIA**
**mohini@varindia.com**

CADYCE

Life Aasaan Banaao
www.cadyce.com

CA-VDCC10

# USB-C® Male to Male Fiber Active Optical Cable

PICKUP FREE DELIVERY


Full-speed data, stable power, and clear display performance across 10 meters.

| 4K | | DP 1.4 | | 10M |
|---|---|---|---|---|
| 4K Display Output Support | 60W Power Delivery Support | DisplayPort™ Support | 10Gbps Data Transfer | Long Range Cable |

**Warranty :** rma@cadyce.com | **Online Chat :** www.cadyce.com | **Email Support :** support@cadyce.com | **Sales :** sales@cadyce.com

Toll Free : **1800 266 9910**
Tech Support : **+91 91722 12959**

**Pune:** +91 9226783571, 9322153959 | **Mumbai:** +91 9769726552, 9307742595 | **Maharashtra:** +91 9890227701 | **Gujarat:** +91 9974800847 | **Delhi:** +91 9999071626 | **Bangalore:** +91 9972534115, 9880660912 | **AP & TS:** +91 8882212998 | **Tamil Nadu:** +91 9840894013 | **Other Territories:** +91 9699375712.

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS
Website: www.varindia.com

**Publisher:** Dr. Deepak Kumar Sahu
**Editor:** S Mohini Ratna
**Executive Editor:** Dr. Vijay Anand
**Consulting Editor:** Gyana Swain
**Associate Editor:** Samrita Baruah
**Assistant Editor:** Ramesh Kumar Raja
**Sub. Editor:** Aparna Mullick
**Art Director:** Rakesh Kumar
**Network Administrator:** Ashok Kumar Singh
**Visualizer:** Ravinder Barthwal
**Manager-IT:** Subhash Mohanta
**Manager-SEO:** Santosh Kumar
**Web Developer:** Shivangi Mishra
**SEO-Executive:** Karan Arora

**BUSINESS:**
Commercial Manager: Amit Kumar Jha
Circulation Executive: Manish Kumar

**CORPORATE OFFICE:**
**VAR House**, A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030
Tel: 011-41656383, 46061809
Email: edit@varindia.com

**Bangalore: Bureau office**
Marketing Manager: S. Kamala kar
D-103 G.F., Ashish JK Apartments
Thubarahalli Extended Road
Bangaluru- 560066
Tel: 080-49530399 I Mobile:09886280836
E-mail: kamlakar@varindia.com

**Mumbai: Bureau office**
Regional Manager (West): Anil Kumar Sahu
Radha Krishna Complex, B/202, Plot no 24, Sector-25, Kamothe, Navi Mumbai - 410206, Maharashtra
Tel: 022-65561292, Mobile: 08108017479
E-mail: anil@varindia.com, mamta@varindia.com

**Chennai: Bureau office**
Branch Manager: K. Parthiban
F1, Meadows Green Apartments, 64, Chetty Street
1st Cross, Mel Ayanambakkam, Chennai - 600 095

**Hyderabad: Bureau office**
Branch Manager: Sunil Kumar Sahu
32-161/3, 202 Neha Paradise, Nr. Maissamma Temple, Venketeswara colony
Ramakrishna Puram, Hyderabad - 500056
Telangana, Tel: 040-32989844/ Cell No. 08100298033
E-mail: sunil@varindia.com

**Kolkata: Bureau office**
Marketing Officer: Sunil Kumar
Correspondent: B Kiran Dutta
Haritasa Electronics Solutions Pvt Ltd
204 Tower- 2, PS Srijan Corporate Park,
Block EP-GP, Salt Lake, Sector - V, Kolkata - 700091
Mobile: 08100298033, E-mail: sunil@varindia.com
Mobile: 09903088480, E-mail: kiran@varindia.com

**Bhubaneswar: Bureau office**
Jagannath Warrior Residency, Suit No.A5/501, Kaimatia Bhubaneswar-752054 I Cell No. 8100298033

Printed and Published by **Deepak Kumar Sahu** on behalf of M/s. Kalinga Digital Media Pvt. Ltd. and Printed at Pushpak Press Pvt. Ltd. Shed No. 203 - 204, DSIDC Complex, Okhla Industrial Area, Phase-I, New Delhi-110020 and Published at A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030, Editor - S Mohini Ratna.

For Subscription queries contact: info@varindia.com
Subscription: Rs. 500(12 issues)Rs. 1000 (24 issues)

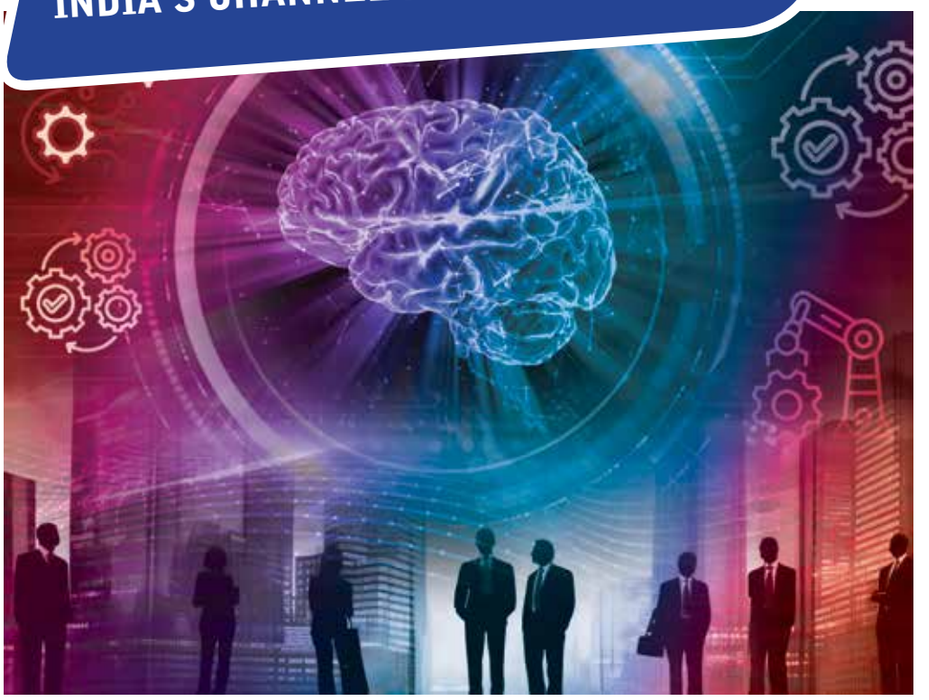
All payments favouring:
KALINGA DIGITAL MEDIA PVT LTD



# CONTENTS

**COVER STORY / 30pg**

## FROM TECH DEBT TO AI READINESS: INDIA'S CHANNEL PARTNERS STEP UP



Omada
by tp-link

# Seamless Connectivity. Unified Control.

## Powerful Wireless + Switching with Omada SDN

EAP683 UR | EAP723 | EAP723 | SG3428XPP-M2

### Wireless (EAP Series)

**Wi-Fi 6 Performance**
Faster speeds, higher capacity

**Seamless Roaming**
Uninterrupted user experience

**High-Density Coverage**
Ideal for enterprise environments

### Switching (SG M2 Series)

**Multi-Gig Ports**
Unlock next-gen network speeds

**High PoE Budget**
Power access points and devices efficiently

**Advanced L2+ Features**
Reliable and secure switching

**Omada SDN Integration** › **Single platform** › **Complete control** › **Cloud to edge**

## Call for Product Demo!

From access to aggregation - **build a fully unified network with TP-Link Omada ecosystem.**

**One Network. One Platform. Omada.**

### TP-Link India Contacts:

**North**
**Rajendra Mohanty**
M: +91 98711 51116
E: rajendra.mohanty@tp-link.com

**South**
**Sunil Nair**
M: +91 96111 13909
E: sunil.nair@tp-link.com

**AP & Telangana**
**Raminder Singh**
M: +91 97045 75432
E: raminder.singh@tp-link.com

**East**
**Satish Panda**
M: +91 91639 33951
E: satish.panda@tp-link.com

**Mumbai**
**Mahesh Mani**
M: +919820291229
E: mahesh.mani@tp-link.com

**Nagpur**
**Abhay Lanjewar**
M: +91 95796 46634
E: abhay.lanjewar@tp-link.com

**North**
**Bhushan KR Saxena**
M: +91 97174 74061
E: bhushan.kumar@tp-link.com

**Bengaluru**
**Srikanth S**
M: +91 99852 15156
E: srikanth.s@tp-link.com

**Hyderabad**
**Srikant R**
M: +91 94825 57627
E: srikanth.r@tp-link.com

**East**
**Abinash Roy**
M: +91 95236 53074
E: abinash.roy@tp-link.com

**West**
**Sanjay Shinde**
M: +91 97697 79085
E: sanjay.shinde@tp-link.com

**Pune**
**Sumeet Lambe**
M: +91 89995 64587
E: sumeet.lambe@tp-link.com

**www.tp-link.com/in** | **sales.in@tp-link.com | support.in@tp-link.com** | **+91 7738044366**

# IRIS 2.0
## THE LEADERSHIP CONVERSATION
### From Distribution to Intelligence

**IRIS 2.0 IS THE NEXT PHASE IN THE TECHNOLOGY JOURNEY THAT TRANSITIONS IRIS FROM A TRADITIONAL TECH COMPANY TO A SCALABLE, INTELLIGENT ECOSYSTEM DESIGNED FOR THE AI ERA. AT THE CENTER OF THIS VISION IS IRIS.AI, A FUTURE-FORWARD PLATFORM DESIGNED TO SIMPLIFY AND ACCELERATE ENTERPRISE TRANSFORMATION.**

**ANIL SETHI SHARES HIS VISION FOR IRIS 2.0, WHILE EXPLAINING HOW IT IS RESHAPING THE COMPANY'S IDENTITY AS WELL AS ITS OVERALL BUSINESS STRATEGY AND APPROACH.**

**ANIL SETHI**
**CEO**
**IRIS GLOBAL SERVICES**

**Everyone knows IRIS as a technology distribution company. Why IRIS 2.0 now?**

The world of technology has fundamentally changed. Businesses today are no longer looking for just products. They are looking for intelligence, speed, automation, security, and business outcomes.

Earlier, technology conversations revolved around devices and infrastructure. Today, the conversation is about how organizations can become AI-ready and future-ready.

IRIS 2.0 is our answer to that transformation. It is the evolution of IRIS from a traditional technology company into an intelligent enterprise ecosystem designed for the AI era.

**What exactly is IRIS 2.0?**

IRIS 2.0 is the next phase of our journey. It is a strategic transformation focused on enabling intelligent enterprises through infrastructure, AI, automation, and integrated technology experiences.

At the center of this vision is Iris.ai, a future-forward platform designed to simplify and accelerate enterprise transformation.

**IRIS 2.0 REPRESENTS:**

- Smarter technology ecosystems
- AI-enabled business operations
- Intelligent workplace solutions
- Secure and scalable infrastructure
- Data-driven decision-making
- Human-centered innovation

The idea is simple -Technology should not just support businesses. It should rather empower businesses to think smarter and move faster.

**Why is AI such an important part of this transformation?**

AI is no longer the future. It is the present.

Every organization today is under pressure to - improve efficiency, reduce complexity, increase productivity, make faster decisions, and deliver better customer experiences.

AI enables all of this.

But real transformation happens only when AI becomes practical, accessible, and integrated into everyday business operations.

That is the vision behind IRIS 2.0. We want to make intelligent transformation real for enterprises.

**What does Iris.ai stand for?**

IRIS.AI is the intelligence layer of the IRIS 2.0 vision. It represents our commitment to building connected enterprise ecosystems powered by intelligence, automation, and innovation.

**IRIS.AI FOCUSES ON:**

- Intelligent workflows
- AI-powered productivity
- Smart enterprise experiences
- Automation-led efficiency
- Data intelligence
- Future-ready business solutions

More importantly, it represents a mindset shift.

From reactive technology... to predictive, intelligent technology.

**Is IRIS changing its identity as a company?**

IRIS is evolving its identity.

The technology industry is moving from product-led conversations to solution-led ecosystems. Organizations today do not want fragmented technology experiences. They want simplicity, integration, intelligence, and long-term value.

**IRIS 2.0 REFLECTS THAT EVOLUTION.**

We are moving from being known only as a distribution-driven organization to becoming a transformation-led technology partner focused on enterprise growth.

**What makes IRIS 2.0 different?**

What makes IRIS 2.0 different is its approach.

This is not about showcasing isolated technologies. This is about creating connected experiences.

Every element of IRIS 2.0 is designed around one central question - "How can technology create real business impact?"

The focus is not just innovation.

The focus is meaningful innovation.

**THAT MEANS:**

- Technology with purpose
- AI with usability
- Infrastructure with intelligence
- Automation with measurable outcomes

IRIS 2.0 is where technology becomes business transformation.

**Who is IRIS 2.0 designed for?**

IRIS 2.0 is designed for modern enterprises that are preparing for the next decade of business.

From startups to large enterprises, every organization today is navigating - Digital acceleration

AI adoption, Data growth, Workforce

transformation, Security challenges and Operational complexity.

IRIS 2.0 is built to support organizations through that journey. Whether the goal is scalability, agility, productivity, or innovation — the objective remains the same - Helping businesses become more intelligent and future-ready.

### Which industries can benefit from this vision?

Every industry today is becoming technology-driven. However, sectors experiencing rapid transformation include -

- Banking and financial services
- Healthcare
- Retail
- Manufacturing
- Education
- Government
- Enterprise services
-

Each of these industries is looking for smarter operations, intelligent automation, predictive capabilities, and seamless digital experiences.

IRIS 2.0 is designed to help enterprises adapt to this new reality.

### What does "Powered by IRIS.AI" truly mean?

It means intelligence becomes the foundation of every experience.

"Powered by IRIS.AI" is not just a tagline. It is a philosophy.

**IT REPRESENTS A FUTURE WHERE -**

- Systems become smarter
- Workflows become faster
- Decisions become data-driven
- Businesses become more adaptive
- Technology becomes more human-centric

The goal is not simply to digitize businesses. The goal is to intelligently transform them.

### How will customers and partners benefit from IRIS 2.0?

The biggest benefit is simplification. Technology ecosystems today are often fragmented and difficult to manage.

IRIS 2.0 brings together intelligence, infrastructure, innovation, and enterprise enablement into one connected ecosystem.

**FOR CUSTOMERS, THIS MEANS -**

- Faster transformation
- Better efficiency
- Smarter operations
- Improved scalability
- Reduced complexity

For partners, it creates opportunities to move beyond transactional business models and become strategic transformation enablers.

### Is IRIS 2.0 just an event or a long-term vision?

IRIS 2.0 is a long-term strategic vision.

This is not a campaign. This is not a trend. This is the future direction of IRIS.

Technology is entering a new era where intelligence will define competitiveness. The companies that succeed tomorrow will be the ones that can combine – Technology, Intelligence, Automation, Innovation and Human experience.

IRIS 2.0 is our commitment to building that future.

### What is the one message people should take away from tonight?

The future of business will not be driven by technology alone. It will be driven by intelligent ecosystems.

The next era belongs to organizations that can think faster, adapt quicker, automate smarter, and innovate continuously.

IRIS 2.0 represents the beginning of that journey.

A journey from distribution to intelligence.

From systems to ecosystems.

From technology to transformation.

**WELCOME TO IRIS 2.0.**

# Veeam Enabling Enterprises Build Trust, Security and Compliance for AI

**SANDEEP BHAMBURE**
Vice President and Managing Director,
India & SAARC, Veeam Software

**Veeam Software launched its VeeamON Tour India 2026 in Mumbai, bringing together enterprise leaders, government stakeholders, partners and customers to address data governance, protection and trust as AI adoption accelerates. The event focused on DPDP compliance, data localization, ransomware resilience, sovereign-ready infrastructure and AI governance, while showcasing innovations including the DataAI Command Platform and Veeam Data Platform. Speaking on the sidelines, Sandeep Bhambure, Vice President and Managing Director, India & SAARC, Veeam Software highlighted how these solutions help organizations strengthen security, ensure compliance and enable workload portability across evolving hybrid, virtualized and containerized IT environments.**

**With the launch of the Data AI Command Platform following Veeam's acquisition of Securiti AI, how does Veeam plan to help enterprises balance rapid AI adoption with strong data compliance, privacy, and security governance?**

One of the biggest inhibitors to AI adoption at enterprise scale has been the absence of a dedicated AI and data trust layer. Existing security frameworks from the pre-AI era were primarily designed around preventing unauthorised human access to sensitive data through perimeter-based security models such as network and application security. However, these approaches are no longer sufficient in the AI era because organisations now also need controls for AI agents, not just humans.

At the same time, the unstructured data landscape is expanding rapidly. Globally, nearly 230 zettabytes of information are expected to be created, with almost 90% of it being unstructured data. In the BI era, enterprises largely operated on structured and transactional data. However, the AI era is fundamentally driven by unstructured data. This means that large volumes of enterprise data that previously remained dormant are now becoming accessible and usable through LLMs and AI agents.

Alongside this, the threat landscape is becoming increasingly sophisticated. AI agents themselves are now emerging as one of the biggest threats to enterprise data security, with one in eight cyberattacks being carried out by AI agents and a significant number of attacks originating from shadow data or shadow AI environments.

For enterprises, the challenge of scaling AI securely has therefore become extremely complex. The missing layer between enterprise data sources, AI models, AI control planes and industry-specific agents is the AI and data trust layer. This is precisely what Veeam is addressing through the Data AI Command Platform.

Through this single platform, Veeam enables customers to manage security, compliance, governance, privacy and data resilience within one integrated framework. Traditionally, organisations would have needed multiple disconnected products to achieve these capabilities, resulting in fragmented environments and operational complexity. The Data AI Command Platform instead delivers these foundational capabilities through a unified architecture designed specifically for AI-scale environments.

At the core of the platform is the Data Command Graph, which provides enterprises with complete visibility into their data estate at a granular level. This allows organisations to understand whether data is mission-critical, whether it contains PII, how frequently it is being accessed, who or what is accessing it and whether it is relevant to regulatory frameworks such as GDPR, DPDP or RBI-related compliance requirements.

**With the upcoming Veeam Data Platform V13.1, is Veeam seeing a clear shift from legacy hypervisors to open-source and container-based environments, and how is it capitalising on this transition?**

Yes, we are seeing a growing number of organisations moving even mission-critical applications away from traditional Broadcom VMware environments toward alternative hypervisors and increasingly toward containerised environments as well. Application modernisation is happening at a significant scale, particularly within the financial services industry.

As enterprises modernise workloads from traditional virtualised environments into Kubernetes and other container platforms, the earlier approaches to data protection and resilience no longer remain sufficient. Organisations now require native Kubernetes backup and recovery capabilities specifically designed for these modern environments.

This is an area where Veeam is helping customers through its Kasten solution, which is designed to support Kubernetes-native backup and recovery requirements.

Veeam already supports a broad range of hypervisors and has been helping enterprises migrate workloads from one hypervisor platform to another. Because of the way Veeam's backup architecture works, customers can back up workloads from virtually any virtualised platform and recover them onto another platform. This flexibility is becoming increasingly valuable as enterprises explore hypervisor portability strategies.

DELL Technologies

# Stay Ahead with
# Dell Pro Essential Micro

AMD

## Dell Pro Essential Micro PVM1265: Big power. Ultracompact. Exception Security.

### Performance for day-to-day demands

Boost productivity with AMD Ryzen™ processors performance and up to DDR5 memory[1] for seamless multitasking.

### Easy to access

Tool-less entry and an easily removable panel allow for quick access to upgrade or service your desktop's internal components.

### Hardware TPM

Protect your data with Trusted Platform Module (TPM), a security technology designed to secure hardware with integrated cryptographic keys.

### Ultracompact

This ultra-compact desktop saves valuable space and is compatible with a wide range of mounts and stands, giving you flexible setup options to suit your business needs.

**Meet the demands of your busy workdays with AMD Ryzen (TM) 5 150, MS Windows Pro OS, 1X16GB DDR5, 512 GB SSD. Wired KB and Mouse, Internal Wifi, Bluetooth, and 3 Yrs Onsite Warranty.**

## Contact Us to Know More:

Name: Pooja Chavan | Email ID: dell.amd@rptechindia.com
Mobile Number: +91 86579 78028

[1]Up to 64GB, regional availability may vary.
[2]WiFi 6 module is optional.

Dell Technologies Global Headquarters is located at One Dell Way, Round Rock, TX, 78682

# Excellence in Technology Amidst Paradoxes

I sometimes wonder how things happen! Most of the time, they occur suddenly without any premonitions. Take for instance, the Covid -19! No one had any inkling that such disasters would descend on mankind.

Millions lost lives, fear gripped across the world, and importantly, there were winners and losers in the midst of the pandemic. One important winner is the pharma companies who have developed the vaccine for preventing the pandemic and the entire ecosystem that was connected with the supply chain of vaccines. Yet, no one wants to know the exact reason why that had happened. I believe that there is a public amnesia that forces people to forget things and carry on with the life as holocausts never happened. May be that is a boon since that helps people to seek new pathways and forget about sinister things that haunted us in the past.

I am aware that these things are happening in an era where science rules supreme and rational thinking is the most desirable pathway. It is also an era where Artificial Intelligence is omnipresent, quantum theories applied in every walk of life and data mining is resorted to get in to the bottom of things. Yet, the real reasons for the pandemic termed as the most horrible global development of recent centuries evades a proper answer for its occurrence. Same way, I feel many such developments that had happened in the past evade a proper cause and effect analysis. For instance, why the World Wars were fought, what was the rationale of forming axis to fight war, what was the real damage caused by the world wars etc are still to be explained in clearer paradigms. Reasons attributed by historians, we feel, are Gospel truth. Should we go beyond that postulates and try to see things from a new perspective? That way, every development that had happened in the past can be analysed and interpretations and narratives formed whether such narratives are close to the reality.

Let us now focus on the present. We are all presently going through the negative impact of the middle east war, which disrupted the world economy. We are given to understand that there are two groups in the war. On one side is Iran and the other side, Israel and the US. I am not involving the peripheral players involved, be they China or Russia or European Union. We all know the destruction caused by the war is immense and it is still counting. No one knows when the war will end; yet we are aware of its impact and a stakeholder of that either directly or indirectly. Every household across the world is suffering in one way or the other.

The counting of losses due to war will continue till the war is over and will spill over to post war period also when the losses are more accurately assessed. There is a set of people amidst the war who is gaining. They do not get mentioned in the way. Who are these beneficiaries?

A recent report surfaced suggest that oil industry is a major beneficiary, besides defence establishments, green energy outfits and banks. In future, when the reconstruction work starts, construction sector will get a boost since trillions of dollars have to be spent in the Middle East to revamp the damaged infrastructure, military installations etc.

The biggest economic impact of the war so far has been a surge in energy prices. Around a fifth of the world's oil and gas is transported through the Strait of Hormuz, but those shipments effectively ground to a halt at the end of February. The result has been a rollercoaster of price movements on energy markets, with some of the world's biggest oil and gas companies benefiting. Interestingly, main beneficiaries are not oil producing countries. Profit is flowing into the pockets of European oil giants, who have trading arms to gain from sharp price movements boosting profits.

Some of the biggest banks have also seen their profits boosted during the war in Iran. JP Morgan's trading arm made a record $11.6billion of revenue in the first three months of 2026, helping the bank overall to its second biggest ever quarterly profit.

Across the rest of the "Big Six" banks – which includes Bank of America, Morgan Stanley, Citigroup, Goldman Sachs and Wells Fargo, as well as JP Morgan – profits all rose substantially in the first quarter of the year. Overall, the banks reported $47.7bn in profits for the first three months of 2026.

One of the most immediate beneficiaries in any conflict is the defence sector. BAE Systems, which makes products including F35 fighter jet components, said in a trading update it expects strong growth in sales and profits this year. Gulf countries including Iran will have to spend trillions to replenish their armaments. Also, growing "security threats" around the world will push up government defence spending, which has in turn created a "supportive backdrop" for the global companies involved in defence production. Lockheed Martin, Boeing and Northrop Grumman, three of the world's biggest defence contractors, have each reported having record order backlogs at the end of the first quarter of 2026.

The conflict has also highlighted the need to diversify away from reliance on fossil fuels. The Trump administration has popularised the "drill, baby, drill" slogan encouraging greater fossil fuel usage. The war has led to renewable investment being seen as increasingly important to stability and resilience to shocks. The Florida-based NextEra Energy, has seen shares surge by 17% so far this year as investors pile in on its mission. Danish wind power giants Vestas and Orsted have also reported surging profits, highlighting how the fallout from the Iran war is also boosting renewable energy firms. A good number of Chinese companies in the renewal energy sector have also benefited immensely from the surging global demand for replacing the fossil fuel, not necessarily in the present but in the future.

My esteemed readers may ask me what I am trying to drive home by mentioning these things. It may seem to be disjointed ideas that have occurred to me. It may be partially true. However, I am trying to weave a big picture. Amidst the faster development of technology, overriding importance of rational mind, and human quest for excellence and desire to leap the technology frontiers, we are lagging behind in predicting the human behaviour, which unnecessarily escalate tensions. Is it true that humans have failed in conquering their own minds?

**DR. ASOKE K. LAHA**
**CHAIRMAN-EMERITUS AND FOUNDER, INTERRAIT**

# Haritasa Electronics Solutions Pvt. Ltd.

(AN ISO 9001-2015 CERTIFIED COMPANY)

## IT System Integration & Leaders for Communication, Security and Building Management Systems

**Mission-Critical Solutions Trusted by India's Strategic Infrastructure**

Haritasa Electronics Solutions Pvt. Ltd, has consistently delivered high-performance system integration and manufacturing solutions for misson-critical environments.

**Trusted Partner for National Security and Core Infrastructure**

Systems in ensure as:

- Nuclear Power Plants
- Multi-layer redundancy
- Safety and Security Solutions
- High compliance
- 24X7 uptime
- Defense
- Data & Voice Solutions

**Haritasa Electronics Solutions is a leading provider of Extra Low Voltage (EL V) turnkey solutions in the field of:**

- Security Systems
- Building Management Systems (BMS)
- Maintenance Services
- Safety and Security Solutions
- Nurse Call System (NCS)
- Voice & Data communication
- Parking Management System

## Our Partners

BOSCH Security Certified Partner

Bosch is our preferred OEM partner for PAS, IPA, CCTV, ACS, FAS.

COMMEND

Commend International is our OEM partner for IP Based Two Way Communication System.

Alcatel·Lucent

Alcatel- Lucent is our OEM partner for EPABX and Data Products.

HELION CONCEPTS

Helion Concepts Inc. is OEM Partner for Smart Energy

TREND

Honeywell Trend is our OEM partner for Building Management System


## Haritasa Electronics Solutions Pvt. Ltd.

#4194, 2nd 'A' Main, Girinagar, 4th Phase, (Behind Seetha Circle Petrol Bunk) Bangalore-85

Tel:- +**91-80-26253610/3611** | Fax:- **+91-8026253612** | E-mail:- **info@haritasa.net** | **designs@haritasa.net.** | Web:-**www.haritasa.net**

## Fortinet integrating FortiAIGate solution with NVIDIA's AI platforms and software technologies

Fortinet has announced that it is accelerating the FortiAIGate solution with NVIDIA's AI platforms and software technologies. The joint solution protects AI workloads, data, and autonomous agents in real time in data centers and the cloud, enabling organizations monitor AI usage, and securely build, deploy, and scale agentic AI without compromising performance or governance. The solution's inline deployment provides visibility while supporting data sovereignty requirements, delivering high-performance protection with minimal latency.

"Enterprises everywhere are racing to adopt AI, and security has become a critical enabler of that innovation. Together with NVIDIA, we're delivering a solution that helps organizations secure and optimize AI deployments while maintaining performance, controlling costs, and meeting data sovereignty requirements. FortiAIGate combines Fortinet's AI-driven Security Fabric with NVIDIA's high-performance computing and AI factories to stop threats, from malicious prompts to data exfiltration, without disrupting AI workflows," says John Whittle, Chief Operating Officer, Fortinet.

## Lenovo launches "Maximum David" AI campaign with David Beckham ahead of FIFA 2026

Lenovo has launched "Maximum David," a new global campaign centred on former football star David Beckham. The initiative highlights how AI-driven technology enhances creativity, performance, and impact across sport, business, and everyday life.

The campaign showcases Lenovo's broad AI portfolio, spanning devices, solutions, and services. It demonstrates how the company's technology helps individuals, teams, and enterprises unlock new possibilities to work, create, play, and connect more effectively in an increasingly digital world.

David Beckham's involvement reflects his continued evolution beyond football. As co-owner of Inter Miami CF, entrepreneur, investor, and global cultural icon, he represents a blend of athletic excellence, creativity, and global influence, aligning with Lenovo's vision for AI-powered transformation.

## Google Cloud to help build Meesho a High-Performance Foundation for Next Phase of Growth

Google Cloud and Meesho announced a strategic partnership to build a high-performance digital foundation designed to power Meesho's next phase of growth. As part of this collaboration, Meesho will leverage capabilities from Google Cloud's unified stack to enhance its data and AI-led operations. This collaboration ensures the performance and scale necessary to support Meesho's rapidly growing ecosystem of 961,000 sellers and 264 million users nationwide.

A cornerstone of this technology evolution is the launch of Vaani, Meesho's generative AI shopping assistant. Built with support from Google's Gemini family of models, Vaani is targeted especially at users in Tier-2 and Tier-3 cities who prefer voice over typing, Vaani allows shoppers to discover products, ask questions, and navigate the platform through natural conversation in both Hindi and English.

## AMD Expands AI Infrastructure Push

AMD has announced two major milestones that strengthen its position in the rapidly growing AI infrastructure market. The company unveiled a more than $10 billion investment initiative to expand advanced packaging capabilities while also confirming that its next-generation EPYC processor, codenamed "Venice," has become the industry's first HPC product to achieve production ramp on Taiwan Semiconductor Manufacturing Company(TSMC)'s advanced 2nm process technology.

The announcements highlight AMD's broader strategy to compete aggressively in the AI and high-performance computing race dominated by increasing demand for cloud infrastructure, generative AI, and data center workloads. As AI systems become more complex, chipmakers are now focusing not only on raw processing power but also on advanced packaging technologies that improve speed, energy efficiency, and integration between processors, memory, and accelerators.

## Gartner Warns Poor AI Agent Governance Could Lead Enterprises to Shut Down Autonomous Systems

Gartner said 40% of enterprises could demote or shut down autonomous AI agents by 2027 because of governance failures discovered after the systems are deployed in production environments.

The research firm said many organizations are incorrectly applying the same governance controls to all AI agents, regardless of how much autonomy or system access those agents have.

According to Gartner, that approach creates two major risks: over-restricting simpler AI agents, which slows innovation and encourages shadow IT, or under-restricting highly autonomous agents, which can expose organizations to operational, security, and compliance failures.

## Ingram Micro India strengthens its cybersecurity offerings with Yubico partnership

Ingram Micro India announced a strategic distribution partnership with Yubico. Through this collaboration, Ingram Micro India aims to strengthen its cybersecurity offerings and help enterprises address the growing risks associated with identity-based cyberattacks.

Through Ingram Micro's extensive partner ecosystem, businesses will now gain access to Yubico's complete portfolio, including the YubiKey 5 Series, Bio Series, and Security Keys. The solutions will enable secure password-less authentication across devices, applications, and hybrid work environments, while supporting compliance requirements such as FIDO2, PIV, and OTP amid an evolving cyber threat landscape.

## Snowflake deepens AWS Collaboration with $6B Commitment to Advance Enterprise Agentic AI

Snowflake announced that it has signed a multi-year strategic collaboration agreement (SCA) with Amazon Web Services (AWS) to accelerate enterprise agentic AI adoption to help joint customers worldwide build and deploy AI faster and more securely. As part of the expanded collaboration, Snowflake is making a $6 billion multi-year infrastructure commitment to AWS, its largest to date, reflecting the accelerating enterprise demand for AI and data workloads running on AWS.

The majority of Snowflake's customers run on AWS today, with AWS recognizing Snowflake as a leading partner driving global customer adoption. The latest agreement builds on this momentum with deeper product integrations across generative AI and agentic AI, expanded go-to-market through AWS Marketplace, and joint investments in customer success programs, workload migrations, and strategic industry solutions designed to help enterprises move from AI experimentation to production-scale outcomes.

## LTM to acquire Randstad Tech Services for $500 Mn, Targets European AI Expansion

LTIMindtree is proposing to acquire parts of Randstad's Technology and Consulting Services business across France, Germany, Belgium, Luxembourg, and Australia in a deal aimed at strengthening its AI and industry-focused services footprint in Europe and other key markets.

The business being acquired represents more than $500 million in annual revenue and would expand LTM's presence in sectors including aerospace and defence, automotive, utilities, and banking and financial services.

Under the deal, LTM would gain additional regional engineering, cybersecurity, IoT, and digital transformation capabilities supported by onshore and nearshore delivery centers in Romania and Portugal. The company said the acquisition would help create a more diversified portfolio while expanding its scale in Europe and Australia.

CEO Venu Lambu said the transaction aligns with LTM's broader strategy to combine global AI-centric capabilities with local industry expertise and regulatory compliance requirements in strategically important markets.

## CERT-In mandates 12-hour fix for critical cyber flaws as AI threats surge

The Indian Computer Emergency Response Team (CERT-In) has released updated cybersecurity guidelines mandating faster remediation of critical vulnerabilities, especially in internet-exposed systems, as artificial intelligence increasingly accelerates cyberattacks and reduces response time for defenders.

In its latest 38-page framework, the agency has recommended that organisations patch high-risk security flaws within 12 hours, wherever feasible. The directive comes amid growing concerns that threat actors are using AI tools and large language models to automate vulnerability discovery, exploit development, and large-scale attack execution. CERT-In noted that AI-assisted cyber operations significantly shorten the time required for attackers to identify weak systems, compromised identities, insecure APIs, and misconfigured infrastructure. This has led to faster and more complex attack cycles across digital environments.

## NTT, NTT DATA and INDYCAR extend entitlement partnership with multi-year agreement

NTT, Inc., together with NTT DATA Group Corporation has announced the renewal of its sponsorship of the NTT INDYCAR SERIES. Under the renewed agreement, NTT has expanded its role beyond race analytics and fan engagement to provide advanced AI and data capabilities for Penske Entertainment and INDYCAR. This includes AI-driven operations, real-time decision intelligence and emissions visibility across INDYCAR, the historic Indianapolis Motor Speedway (IMS) and marquee events within the Penske Entertainment portfolio.

NTT, along with its subsidiary NTT DATA, a global leader in AI, digital business and technology services, will continue as the Official Technology Partner for INDYCAR, the NTT INDYCAR SERIES, IMS, the Indianapolis 500 and the NASCAR Brickyard weekend.

During a typical race weekend, including the Indianapolis 500, the NTT INDYCAR SERIES generates billions of real-time data points from cars, teams and track operations. NTT DATA provides actionable insights to inform race control, operations teams, broadcast partners and event planners to support faster, more precise decisions.

Penske Entertainment and NTT DATA are deploying AI to transform how fans experience INDYCAR—starting with "Up To Speed," a new AI-powered feature delivering smarter, more dynamic race insights to fans, alongside expanded real-time data, content and digital experiences coming online throughout this season. The new "Up To Speed" feature is available now on the INDYCAR App powered by NTT DATA.

## Omega Healthcare modernises global IT infrastructure with Dell Private Cloud

Omega Healthcare Management Services has modernised its core IT infrastructure with Dell Technologies' private cloud platform to strengthen operational reliability, simplify infrastructure management and support uninterrupted healthcare services across its global delivery network.

Omega Healthcare adopted Dell Private Cloud powered by the latest Intel Xeon 6 processors. The platform provides a unified architecture that standardises management across compute, storage and networking infrastructure while supporting existing systems and preferred hypervisors. The company said the deployment has simplified lifecycle management and improved operational control as it continues to scale healthcare operations globally.

## Zscaler Buys Symmetry Systems

Zscaler has announced its proposed acquisition of San Francisco-based startup Symmetry Systems to tackle the complex security risks associated with artificial intelligence, identities, and cloud data. Founded in 2019 by University of Texas professor Mohit Tiwari, the startup has raised $35.7 million in funding. The acquisition aims to solve a critical visibility gap in enterprise environments, where tracking multi-channel AI risk across disconnected security tools remains highly complex.

According to Dhawal Sharma, Zscaler's Executive Vice President of AI Security, traditional enterprise security operations rely on disparate datasets like endpoint agents, inline traffic monitors, and public cloud scans. Organizations frequently struggle to connect these separate channels to understand total AI exposure. Symmetry Systems bridges this crucial gap using specialized access graph technology to map data relationships across various IT silos.

# INDIAN RENEWABLE ENERGY DEVELOPMENT AGENCY LIMITED

A Government of India Enterprise

ENERGY FOR EVER

इरेडा IREDA

ONCE IREDA ALWAYS IREDA

(A Navratna CPSE)

# PROVIDING INVESTMENTS THAT HELP ACHIEVE INDIA'S SUSTAINABILITY GOALS

## ATMANIRBHARTA. GREEN ENERGY. NET ZERO EMISSION.

## नई ऊर्जा नई सोच

**Established and trusted brand with 38 years of experience**

**Highest Credit Rating of 'AAA/Stable'**

**Comprehensive suite of financial products and services across:**

Traditional Technologies ➤ Solar ➤ Energy Efficiency & Conservation ➤ Hydro ➤ Biomass & Cogeneration ➤ Wind ➤ Waste To Energy ➤ Transmission ➤ Ethanol

Emerging Technologies ➤ Battery Storage System ➤ Fuel Cells ➤ Pumped Storage Hydro ➤ Green Hydrogen ➤ RE Component Manufacturing ➤ Electric Vehicle & Charging Infra

Registered Office: India Habitat Centre, East Court, Core-4A, 1st Floor, Lodhi Road, New Delhi – 110003, India | 011- 24682206- 19 | www.ireda.in | Follow us on:

## Cloudera announces Workflow Data Fabric Zero Copy Connector for ServiceNow

Cloudera has announced the availability of a Workflow Data Fabric Zero Copy Connector for ServiceNow, a new integration that seamlessly connects hybrid data lakehouses with intelligent workflows to enable secure, real-time autonomous AI execution, without the need for costly data duplication.

As organizations race to operationalize AI, many are running into a fundamental barrier: their data. Despite strong investment and clear strategies, most enterprises still struggle to access, integrate, and govern data across fragmented environments. In fact, nearly 8 in 10 organizations say their AI initiatives are hindered by incomplete data access. This disconnect is driving demand for new architectures that eliminate data movement and bring AI directly to where data resides. The connector allows enterprises to query data directly where it already lives, eliminating traditional data movement requirements while maintaining strict security and governance standards.

## CyberEvolve Unveils AI-Native Cyber Defense Platform

Recently unveiled in Gurugram, CyberEvolve is positioning itself as a next-generation cybersecurity platform designed to help organizations overcome the limitations of legacy SIEM systems. Founded in 2023 by cybersecurity veteran Rahul Yadav and headquartered in New Delhi, CyberEvolve aims to transform Security Operations Centers (SOCs) from reactive monitoring hubs into proactive, intelligence-driven defense centers. The platform combines Socleus, a high-performance SIEM engine, with Iryne, an Agentic AI layer that investigates, prioritizes, and responds to threats at machine speed.

CyberEvolve's AI-native architecture leverages high-speed search, real-time context, behavioral analytics, and automated decision-making to eliminate alert fatigue and surface only actionable threats. By correlating events across the digital environment, it reduces false positives and provides security teams with clear, risk-based insights. The company believes the future of cyber resilience lies in combining intelligent automation with human expertise, enabling CISOs to detect threats faster, respond more effectively, and stay ahead of increasingly sophisticated adversaries.

## Check Point launches its Agentic Network Security Orchestration platform

Check Point Software Technologies has launched its Agentic Network Security Orchestration Platform, a purpose-built autonomous agent architecture that executes network security operations across enterprise environments, without requiring constant human intervention. The launch continues the company's mission to fundamentally transform the way enterprise network security is managed, an approach that has remained largely unchanged since the early days of the firewall era.

Enterprise networks have grown beyond human capacity to manage. Hybrid cloud adoption, M&A-driven fragmentation, the explosion of connected devices, and the rapid proliferation of AI agents across infrastructure have created environments that no human team was designed to secure at this scale. A single change request can take two to four weeks to work through analysis, security review, and policy dependencies - only to break something else and restart the cycle. Segmentation projects sit on the board for years and never ship. Policies drift because workloads move faster than any team can follow.

## Equinix announces expansion of its network-level, multicloud sovereignty solution

Equinix announced the global expansion of Equinix Fabric Geo Zones, the first network-level, sovereignty enforcement layer that operates across interconnected clouds and providers. Enterprises face growing compliance risks from network rerouting events that can inadvertently move sovereign data across borders they are legally required to respect. Built natively into Equinix Fabric, Geo Zones eliminates that risk by keeping data within defined geographic boundaries.

Most networks prioritize availability and performance over geographic or regulatory boundaries, often leaving customers with limited visibility or control over where their data travels. Fabric Geo Zones ensures that rerouted data remains within defined jurisdictions. This capability is especially critical for organizations operating in regulated industries. Unlike solutions built within a single cloud or delivered as software overlays, Fabric Geo Zones enforces sovereignty at the network layer.

## STL Digital expands its Ainnov portfolio with new AI-powered enterprise solutions

STL Digital Limited has announced the expansion of its AInnov platform with three new enterprise-grade solutions — AInnov Space, AInnov Shield, and AInnov Talent — designed to address critical workforce engagement, vendor risk management, and talent acquisition challenges facing enterprises today. These additions strengthen the AInnov portfolio and reinforce STL Digital's commitment to delivering intelligent, experience-first products that solve real-world enterprise challenges through the power of AI.

Building on AInnov's vision of helping enterprises transition their operations to intelligent, data-driven ecosystems, the three new solutions target some of the most pressing business priorities organizations face today.

"The expansion of the AInnov suite of products reflects our commitment to building AI solutions that deliver real, measurable outcomes," said Naveen Bolalingappa, CEO, STL Digital. "These platforms are purpose-built to help enterprises operate smarter, manage risk proactively, and hire with greater precision — across every market they serve."

## HPE brings AI and mission-critical workloads to severe, ruggedized environments

HPE has expanded its HPE ProLiant edge portfolio for customers seeking to extend AI and mission-critical workloads to highly distributed and harsh environments. The new HPE ProLiant Compute EL2000 chassis, the foundation for two new Gen12 servers, and the enhanced HPE ProLiant DL145 Gen11 are part of a portfolio of resilient and secure solutions engineered for edge deployments, complex environments, and disconnected operations. Additionally, each platform is now available with an Environmental Ruggedization Option Kit ideal for harsh locations, including high- or low-altitudes, extreme temperatures, and hazardous transit.

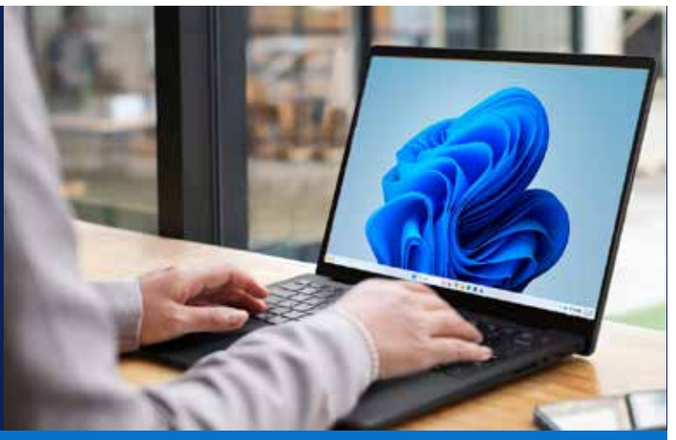

"Organizations are pushing towards the edge for AI inferencing, and remote operations, where traditional IT structures are impractical for many industries," said Krista Satterthwaite, senior vice president and general manager, Compute, HPE. "HPE ProLiant is engineered with enterprise-grade security, right-sized performance, and a unified approach to managing and automating operations, enabling organizations to easily deploy, manage, and scale edge environments with confidence."

DELL Technologies

Windows 11

# Transform Your Productivity

## Work smarter with Dell Pro Essential



## Streamline IT and simplify your business

**Security**
Encrypt credentials with **TPM 2.0,** enable quick sign-in with an optional **fingerprint reader**, and secure devices with a lock slot.

**Manageability**
Autopilot and Intune streamline setup and configuration, while **Dell Management Portal** simplifies cloud-based PC management. Support

**Support**
**Support Assist** resolves issues proactively, and **ProSupport** offers 24/7 expert assistance with extended warranty options.

**Built for Business**
Enterprise-grade productivity unlocked with optimized thermals, enhanced display, and extended battery life.

**Intelligent Software**
**Dell BIOS, Dell Optimizer's AI,** and **Excalibur OS** improve performance, security, and system recovery.

**Recycled Materials**
**Dell Pro Essential** devices are built with durability and use responsibly sourced, **recycled materials** to reduce environmental impact.

**Always choose Genuine pre-installed Windows 11 Pro devices**
Ensure a secure, trusted foundation from day one.

**Secure and reliable**
Built to withstand everyday business use with features like FHD IR camera, fingerprint reader, and AI-powered noise reduction.

**Gain more than just a secure OS**
Genuine Windows 11 Pro reduces overall cyber-risk and helps lower security costs.

**Seamless views for smarter work**
Enjoy crisp visuals on a 14-inch screen with a 16:10 aspect ratio and 300 nits brightness.

92% of successful ransomware attacks originated from unmanaged devices, underscoring the need for built-in OS-level security and device control.

## Professional Designs in Various Shades

Dell Pro Essential laptops are available with optional chassis materials and colors; crafted to meet military-grade standards (MIL-STD) for proven reliability.

**Carbon Black**

**Platinum Silver**

**Midnight Blue**
(Aluminum)

Contact Us to Know More

Email ID: EnquiryDell@kestoneglobal.biz

## HP defines Future of Work with 20+ new products and solutions in India

HP India has unveiled a broad portfolio of 20+ new products and solutions spanning personal systems, print, and workforce solutions to address the full spectrum of India's evolving technology needs from students and creators to professionals and enterprises. The portfolio also marks HP's entry into new categories with the India-first HP OmniPad 12, bringing PC-like productivity with the flexibility of a tablet to first-time PC users, students and MSMEs, and the HP EliteBoard G1a Next Gen AI PC the first and only AI keyboard PC in the world built to deliver powerful, portable, and simplified computing for modern workplaces.


"In India's growth journey, technology is integral and central to how people learn, earn, and create. If you look at the technology adoption in the country, people are at very different stages. For some, it begins with access to technology itself," said Ipsita Dasgupta, Senior Vice-President & Managing Director, HP India, Sri Lanka, and Bangladesh.

## Dell Technologies announces a new class of modern storage platform

Dell Technologies has introduced Dell PowerStore Elite, a new class of modern storage platform that delivers breakthrough performance and efficiency through software-driven innovation and a fully refreshed hardware platform. PowerStore Elite supports block, file, virtual machines and container workloads with mixed-generation clustering that lets existing customers adopt the latest PowerStore without disruption. Enterprise storage decisions have never been more important. Data is exploding. AI workloads are expanding. Cyber threats are intensifying. Flash supply dynamics are putting new pressure on infrastructure planning. IT teams are expected to modernize through all of it without adding complexity, risk or operational overhead.

PowerStore Elite is built for this moment. It's an intelligent, open storage platform combining AI-driven software, next-generation hardware and non-disruptive modernization so customers can keep storage infrastructure modern as future requirements change.

## Kyndryl unveils agentic AI capability that proactively prevents IT outages

Kyndryl has unveiled a new patented capability in Kyndryl Bridge – the company's AI-powered, open integration platform – that enables customers to automatically detect and resolve IT risks before they escalate into business-impacting outages. Kyndryl's prediction and prevention capability has been deployed on Kyndryl Bridge and is providing AI agent-assisted support to the more than 1,400 customers using Kyndryl Bridge. Kyndryl Bridge generates more than 16 million AI insights each month, has demonstrated a reduction in IT incidents by up to 50% and drives an aggregate $3 billion in annual customer savings from avoided impact events and planned maintenance costs.

"By embedding AI agents in Kyndryl Bridge for proactive risk detection, we are transforming IT operations from reactive outage recovery to proactive, evidence based prevention," said Xerxes Cooper, Global Leader, Kyndryl Delivery. "Correlating millions of observability signals across applications and deep infrastructure helps our customers see and resolve issues before they ever feel them."

## Palo Alto Networks rolls out Next-Generation Identity Security Platform Idira

Palo Alto Networks unveiled the next-generation identity security platform Idira to discover, control and govern all identities, eliminating the silos that have left the modern enterprise exposed. This launch marks a significant upgrade with expanded capabilities for existing CyberArk customers and the industry as a whole by delivering modern privilege access management (PAM) with agentic functionality. Organizations can now extend dynamic privilege controls across every human, machine and agentic identity.

The rapid adoption of AI has fundamentally changed who and what has privilege inside the enterprise. Every identity – human, machine and agentic – can now operate with autonomous access to sensitive data and systems at scale. However, traditional identity point solutions were built for yesterday's problems, where elevated access was reserved for a select few. As privilege becomes increasingly pervasive and agentic access remains uncontrolled, identity has become the primary attack vector, with 9 out of 10 organizations experiencing an identity-related breach in the past year.

## Acer India announces new Aspire 5 AI laptop powered by Intel Core ultra-processors

Acer has announced the launch of its latest Aspire 5 AI laptop in India. Designed to meet modern users' needs, the new Aspire 5 strikes a balance between performance, portability, and everyday usability. Powered by the latest Intel Core Ultra processors, the device supports a wide range of use cases from productivity and multitasking to entertainment and light gaming.


At the heart of the Aspire 5 are Intel Core Ultra 5 and Ultra 7 H-series processors, engineered to deliver fast, efficient, and responsive performance. Combined with up to 32GB of LPDDR5 memory and up to 1TB NVMe SSD storage, the laptop ensures smooth multitasking, faster data access, and reduced load times. This configuration allows users to seamlessly handle demanding applications, large files, and everyday computing tasks without compromising on speed or efficiency. The Aspire 5 features a 14-inch WUXGA IPS display with a 16:10 aspect ratio, offering improved screen space for productivity and content consumption.

## Zoom expands My Notes & agentic search across several workplace apps

Zoom has launched My Notes on mobile and expanded its agentic search tools, extending its AI note-taking and search features across Zoom and several workplace applications. The mobile version of My Notes is designed to capture and organize conversations from Zoom meetings and in-person discussions. My Notes was introduced earlier as an AI-based personal note-taking tool. With the mobile release, users can record, transcribe and summarise in-person conversations on a phone, with notes synchronised between mobile and desktop.

Most note-taking tools capture conversations, but few help finish the work that results from them. My Notes is an AI-first personal notetaker that works across video conferencing platforms—Zoom, Microsoft Teams, Google Meet— and in-person conversations. It doesn't just transcribe; it captures, organizes, and converts every discussion into actionable next steps, right where the conversation happens.

## Airtel India launches Priority Postpaid leveraging 5G slicing technology

Bharti Airtel has announced the launch of Priority Postpaid, a new service that leverages 5G slicing technology to deliver superior and more consistent experience to customers on postpaid. This service is specially built for busy customers who depend on uninterrupted connectivity for work, entertainment, or online collaboration. For this service, Airtel has upgraded its 5G network with advanced capabilities of slicing technology. By intelligently and dynamically segmenting network capacity, Airtel is offering stable and dependable experience for postpaid customers, even when traffic demand is high.

Over the past year, slicing based 5G services have been launched in many countries like USA, Singapore, United Kingdom and Malaysia. Airtel's launch is the first such launch in India, reflecting Airtel's continued investment in building a smarter, more resilient, and future-ready digital network and reinforces its commitment to combining advanced technology with customer-centric innovation.

## PhonePe introduces AI-Powered Integration Layer for Merchants

PhonePe announced the launch of its AI-powered integration layer for merchants, marking a major step toward simplifying the payment gateway go-live process. Built for AI Coding Assistants and enhanced by PhonePe's proprietary 'Integration Intelligence' layer, this innovation aims to reduce integration timelines for merchants from weeks to minutes.

Traditionally, developers spend days navigating technical documentation and resolving complexities. With this new AI Agent, merchants can now integrate PhonePe's payment gateway in just minutes through a conversational interface. This significantly reduces the integration time for merchants, removing dependency on deep technical expertise. By automating integration workflows, businesses can go live faster, accelerating their ability to accept payments and generate revenue.

## New Aadhaar app replaces mAadhaar with advanced verification features

The Unique Identification Authority of India has announced plans to discontinue its mAadhaar application and has started encouraging users to move to a newly launched Aadhaar app equipped with upgraded security and digital verification features.

The new platform has been designed to provide a more secure and streamlined identity verification experience while improving privacy protections for Aadhaar holders. According to UIDAI, the updated app includes features such as QR code-based Aadhaar sharing, face authentication support, offline verification tools, and biometric lock and unlock controls.

Officials said the migration process will not happen automatically. Users will have to manually set up their Aadhaar profiles after downloading the new application from official Android and iOS app stores.

UIDAI has also shared official download links through its website and social media platforms to guide users during the transition process.

## Vi strengthening its 5G footprint in West Bengal; to introduces services across 10 cities

Following its 5G launch in Kolkata and Siliguri last year, Vi is now strengthening its 5G footprint across multiple cities in West Bengal. As part of its planned rollout, Vi 5G is now available in Malda, Haldia, Berhampur and will soon be live in Durgapur, Asansol, Habra-Ashoknagar, Burdwan, Kharagpur, Gangtok, and Darjeeling by June.

To expand its 5G services, Vi has been prioritising key markets, including industrial hubs, high data consumption centres and emerging urban clusters. The planned rollout across these 10 cities reflects Vi's strategic approach to cover key industrial centres such as Durgapur and Asansol, port and commercial hubs like Haldia, as well as important regional and tourism-driven markets including Darjeeling and Gangtok, all witnessing growing data demand.

With this expansion, Vi aims to enhance connectivity across West Bengal, catering to the increasing demand for high-speed data services.

## New Paytm Pocket Money lets teens use Paytm UPI without a bank account

Paytm has launched Pocket Money, a feature that lets teenagers make Paytm UPI payments without needing their own bank account. Built on NPCI's UPI Circle, the service is designed to let parents or trusted family members provide safe and controlled spending access to teenagers while retaining real-time visibility over their transactions from the Paytm app.

As part of the feature, parents can invite a teenager through UPI Circle, set a monthly spending limit, and track their payments as they happen. To ensure a safe experience, individual transactions are capped at ₹5,000 and the monthly limit is set at ₹15,000 across the UPI network. The service works on savings and current accounts, with international payments and cash withdrawals restricted. Several safety controls are built in including payments being capped at ₹500 for the first 30 minutes after setup and ₹5,000 within the first 24 hours. Further, a device lock is mandatory, and parents can modify limits or revoke access instantly using their Paytm UPI PIN.

## WhatsApp to introduce private 'Incognito Chat' for AI conversations

WhatsApp has started introducing a new premium subscription service called "WhatsApp Plus," aimed at users seeking additional personalisation and enhanced interface controls within the messaging platform.

The optional paid plan adds a range of cosmetic upgrades and convenience-focused features without altering WhatsApp's core communication services. Messaging, voice calls, video calls, status updates, and end-to-end encryption will continue to remain free for all users.

According to reports, the feature is currently being rolled out to a limited group of Android and iPhone users following earlier beta testing phases. Initial availability appears to be restricted to select regions, including parts of Europe and Mexico.

The subscription marks one of WhatsApp's latest efforts to diversify revenue streams while preserving its traditional ad-free messaging experience.

## CP PLUS reinforces leadership in intelligent surveillance at InnoMetro 2026 and CCTV TECH INDIA 2026

CP PLUS reinforced its focus on intelligent surveillance and digital infrastructure through its participation at InnoMetro 2026 and CCTV TECH INDIA 2026, two key industry events that brought together policymakers, technology leaders, security experts, and infrastructure stakeholders.


At InnoMetro 2026, the company showcased its AI-enabled surveillance solutions designed for rail and metro environments. As India continues to modernize its transportation infrastructure, CP PLUS highlighted how intelligent monitoring technologies can enhance passenger safety, operational efficiency, and infrastructure resilience. The company also presented its Made-in-Bharat innovations tailored to the evolving needs of the mobility sector.

M.A. Johar, President – Project Business at CP PLUS, participated in a conference session on digital technologies in railways, where he discussed the role of AI-powered analytics, centralized monitoring, intelligent video management, and integrated command centres in strengthening railway security and operational readiness.

At CCTV TECH INDIA 2026, CP PLUS showcased its vision for integrated and cyber-secure surveillance ecosystems. Company representatives discussed the growing importance of intelligent surveillance, Video Management Systems (VMS), Security Operations Centers (SOC), and cybersecurity in enabling proactive threat detection and informed decision-making. Through its presence at both events, CP PLUS underscored its commitment to supporting India's digital transformation and smart infrastructure development.

## Vikas Narang elected new President of Amritsar Computer Traders Association

The Amritsar Computer Traders Association (ACTA) has elected its new executive committee following a successful election process that witnessed strong participation from members of the local computer trading community. Out of 128 registered voters, 109 cast their votes, reflecting active engagement in the association's affairs.

Vikas Narang was elected President unopposed after no other nominations were filed for the position. The newly elected office bearers also include Jaggu as Vice President, Sunil Thakur as General Secretary, Rajeev Anand as Treasurer, Rajnish Sharma as Joint Secretary, Bhavneet Singh as Media Incharge, Amritpal Singh as Public Relations Officer (PRO), and Rohit Rana as Sports Secretary.

All elected members secured the confidence and support of the association's members through the voting process. The election was completed smoothly with the cooperation of members and office bearers, ensuring a transparent and orderly transition to the new leadership team.

Following the declaration of results, the newly elected committee thanked members for their trust and support. The team said it would work collectively to promote the welfare, unity, and development of the computer trading community in Amritsar while strengthening collaboration and addressing the interests of traders across the region.

## ASIRT TechDay #136 highlights cybersecurity, MSP opportunities and business leadership

The Association of System Integrators and Retailers in Technology (ASIRT) hosted TechDay #136 at Sai Palace Hotel, Andheri East, Mumbai, recently, bringing together members and industry professionals for discussions on technology, business growth and leadership.

The event began with ASIRT founder Chetan Shah sharing updates on the association's initiatives, member engagement activities and the progress of its consortium ecosystem. He highlighted the continued growth of the ASIRT community and its focus on creating value for members through collaboration and knowledge sharing.

Among the technology sessions, 3F Security discussed the growing importance of cybersecurity and the need for stronger protection against evolving threats. ITCG Technologies, recently rebranded as Goyama Securetech, showcased opportunities for partners to build managed service provider (MSP) capabilities using Atera, enabling recurring revenue streams and greater service independence. The company also introduced channel opportunities around OpenText solutions. Jaypeetex Engineering Pvt. Ltd. presented its expertise in infrastructure deployment and enterprise technology projects.

The Evolve Speaker session featured Dr. Radhakrishnan Pillai, who spoke on applying Chanakya Neeti principles to professional and personal success. The event concluded with a networking dinner, enabling members to exchange ideas and strengthen industry relationships.

## Consistent Infosystems conducts West Bengal Surveillance Installer Meet

Consistent Infosystems successfully hosted its grand West Bengal Surveillance Installer Meet, bringing together more than 571 channel partners, system integrators, distributors, and CCTV installers from Kolkata, Bankura, Durgapur, Siliguri, and Malda.


Designed to celebrate collaboration, technology, and long-term growth, the large-scale partner engagement initiative witnessed enthusiastic participation from the surveillance community across the state. The event featured live product demonstrations, technical knowledge sessions, networking opportunities, and discussions around emerging security technologies and evolving business opportunities in the surveillance industry.

Partners also got hands-on exposure to Consistent Infosystems' latest surveillance, networking, interactive display, and gaming technologies. The showcased portfolio included STQC-certified CCTV Cameras, DVR/NVR/HVR systems, POE Switches & Extenders, Media Converters, HDMI Extenders, CCTV UPS solutions, Routers, and advanced P2P connectivity solutions designed for modern security and networking requirements.

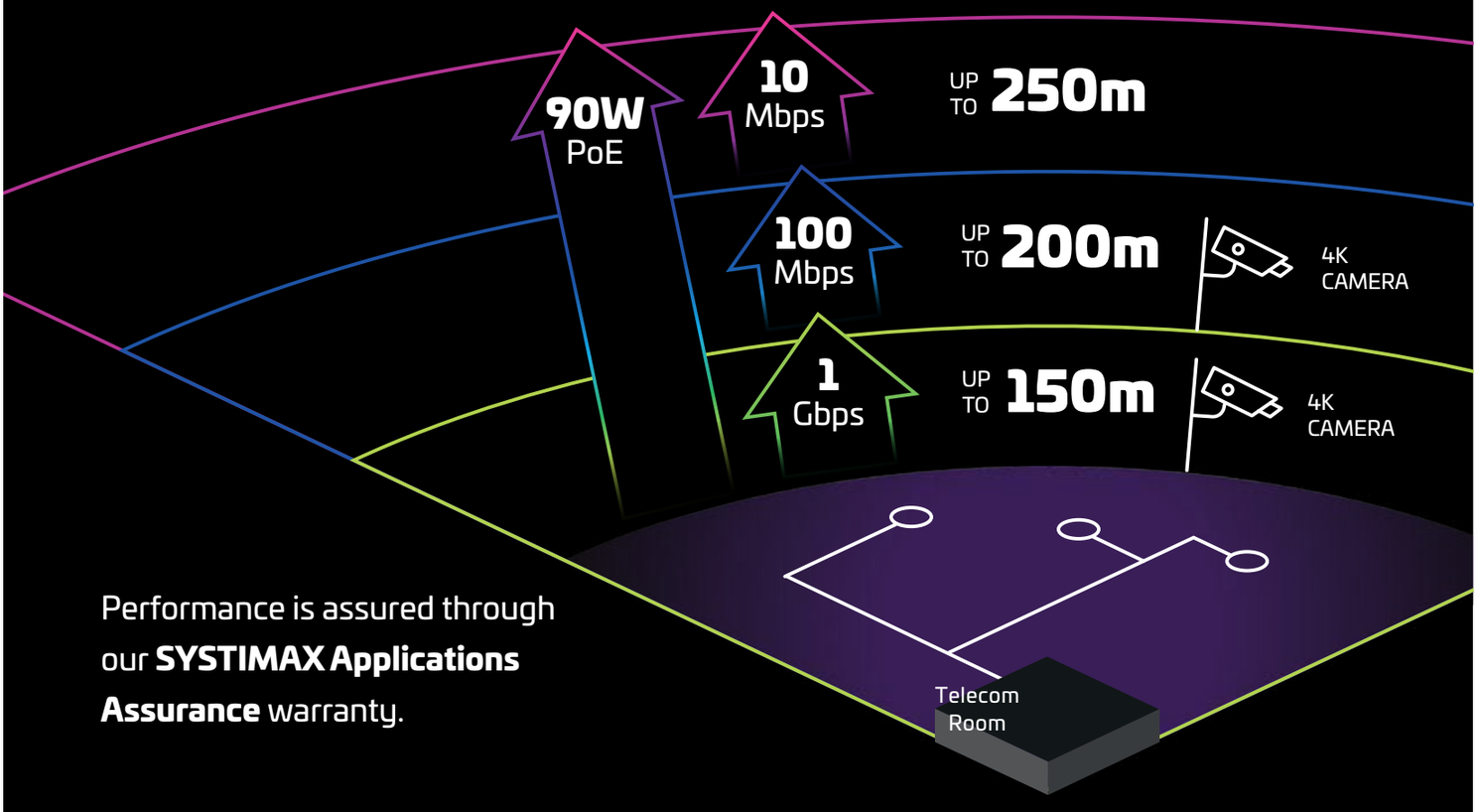
In addition, the company showcased its expanding product ecosystem featuring AAGO Interactive Panels, Gaming Cabinets, and newly launched CPU ARGB Fans, which received strong interest from partners and system builders. Consistent also shared updates on upcoming installer engagement initiatives, technical training programs, service enhancements, and partner-focused business growth plans.

SYSTIMAX®
COMMSCOPE

# GigaREACH™ XL

## Extend your reach, not your risk.

**GigaREACH XL**, the first Cat 6, UTP solution to ensure support for 100 Mbps/90 W up to 200 m, 1 Gbps/90 W up to 150 meters and 10 Mbps/90 W up to 250 m.




Performance is assured through our **SYSTIMAX Applications Assurance** warranty.

PRODUCTS & APPLICATIONS
25 YEAR
SYSTIMAX ASSURANCE™
EXTENDED WARRANTY

### Warrantied performance

- **100 Mbps—200 m—90 W PoE**
- **1 Gbps—150 m—90 W PoE**
- **10 Mbps—250 m—90 W PoE**

Performance is warrantied, supported by CommScope's **SYSTIMAX Assurance** and backed by our **25-Year Extended Product Warranty**

**Learn more**

# Privacy-First Architecture Builds Digital Trust

**An enterprise technology leader with an expertise in privacy-first architecture, AI-powered automation, and digital platform modernization, Ajit Sahu, Director of Engineering - Data Safeguard Inc. in an interaction with Dr. Deepak Kumar Sahu, Editor-in-Chief - VARINDIA, discusses his focus on Privacy-first digital engineering, enterprise platform modernization, Consent management and much more.**

**AJIT SAHU**
**Director of Engineering**
**- Data Safeguard Inc.**

## What would you describe as your core area of expertise?

My core area of expertise is privacy-first digital engineering and AI-driven enterprise architecture.

This means I work at the intersection of software engineering, data privacy, compliance infrastructure, AI automation, and enterprise platform modernization. I focus on designing systems that help organizations collect, manage, enforce, and audit consent across complex digital ecosystems.

My work includes areas such as consent management, cookie governance, AI-powered cookie classification, just-in-time consent, preference management, microservices architecture, cloud platforms, and compliance automation for regulations such as GDPR, CPRA/CCPA, and India's DPDP Act.

## Why is privacy-first architecture important today?

Privacy-first architecture is extremely important because organizations today are collecting and processing customer data at a much larger scale than ever before.

At the same time, regulations are becoming more strict, customers are becoming more aware of their rights, and AI systems are increasing the complexity of data usage.

A privacy-first architecture allows organizations to build trust by ensuring that customer data is used only for permitted purposes. It helps enforce user consent, manage preferences, support audit trails, and reduce compliance risk.

In my view, privacy is no longer just a legal function. It is now a core engineering and architecture responsibility.

## What is your role in AI-powered cookie classification?

One of my key contributions has been in designing and contributing to an AI-powered cookie classification capability.

In many enterprises, cookie classification is still a manual and time-consuming process. Teams need to scan websites, identify cookies, understand their purpose, map them to the correct consent category, and verify whether they comply with regional privacy requirements.

My contribution focused on using AI to accelerate this process. The system analyzes cookie names, domains, script sources, behavior, expiration duration, vendor attributes, and usage patterns to classify cookies into appropriate categories.

This helped reduce work that could take around 90 days into a much shorter cycle, in some cases close to a few hours depending on the scan size and review process. It also improved accuracy, reduced manual effort, lowered operational cost, and created a repeatable governance model.

The broader significance is that it transforms cookie governance from a manual compliance task into an intelligent, scalable, and auditable privacy engineering capability.

## What is just-in-time consent?

Just-in-time consent means asking for consent at the exact moment when a specific data use is required, rather than asking users for broad consent upfront.

For example, if a user is interacting with a chatbot or digital assistant and asks to access billing, payment, health, or personalized information, the system should check whether the required consent already exists. If it does not, the system should trigger a consent request at that moment.

Once the user provides consent, the action can continue, and the consent is stored with proper audit evidence. In some use cases, the consent may be valid only for that session or for a specific purpose.

This is important because it makes consent more contextual, transparent, and meaningful. It avoids unnecessary upfront consent collection and aligns data access with actual user intent.

I consider just-in-time consent a major advancement because it moves consent from a static banner model to a dynamic, purpose-driven, real-time privacy control.

## What makes your work significant?

The originality of my work comes from combining enterprise engineering, privacy compliance, AI automation, and real-time consent enforcement into a single operating model.

Traditional privacy systems often focus on documentation, consent banners, or manual compliance workflows. My work focuses on building privacy as an active engineering layer.

That means consent is collected, validated, enforced, propagated, monitored, and audited across systems. AI is used to reduce manual effort and improve classification, while just-in-time consent makes privacy decisions contextual and user-driven.

The significance is that this approach helps organizations move from passive compliance to active privacy automation. It supports regulatory compliance, improves customer trust, reduces operational burden, and creates a scalable framework for responsible data usage.

### How Do You Design Scalable Enterprise Platforms?

My approach begins with understanding the business domain, regulatory requirements, system boundaries, and long-term scalability needs.

From there, I focus on a few key principles: modular and domain-driven architecture, API-first design, security and privacy by design, observability, auditability, DevSecOps, and operational controls.

Finally, architecture should support business outcomes. A technically strong system is only valuable if it improves delivery, reduces risk, increases efficiency, or creates measurable business impact.

## CBSE faces cybersecurity scrutiny following ethical hacker's claims

The Central Board of Secondary Education (CBSE) has come under scrutiny after 19-year-old ethical hacker Nisarga Adhikary claimed to have gained significant access to the board's On-Screen Marking (OSM) portal. The issue gained attention after Adhikary shared a video allegedly showing the "Bad Apple" animation running on what he described as a CBSE server, raising concerns about potential vulnerabilities in the board's digital infrastructure.

Adhikary claimed he discovered the flaw within 30 minutes and reported it to CBSE on February 25 through responsible disclosure. According to him, the vulnerability provided extensive permissions, including the ability to create, read, update and delete records, along with shell-level access to servers. He said the issue was reported to help improve security rather than to exploit the system.

CBSE maintained that the access was limited to a testing environment containing sample data and that no real student records or examination systems were affected. However, Adhikary disputed the explanation, asserting that the vulnerability remained active after the board's clarification. The incident has drawn attention from cybersecurity researchers, triggering discussions around vulnerability management, responsible disclosure and the need for stronger cybersecurity practices as educational institutions increasingly rely on digital platforms.

## Google launches AI cybersecurity platform to counter rising AI threats

Google Cloud has unveiled AI Threat Defense, an artificial intelligence-powered cybersecurity platform designed to help organisations detect, prioritise and respond to cyber threats. The company said the solution continuously monitors enterprise environments, identifies vulnerabilities and helps security teams focus on risks that are most likely to be exploited.

The launch comes as organisations face growing challenges from

AI-driven attacks and an increasing volume of security alerts. AI Threat Defense combines capabilities from Google's security portfolio with technologies from Wiz, Mandiant and CodeMender. The platform evaluates vulnerabilities based on factors such as internet exposure, network accessibility and exploitability. It also uses AI models to conduct large-scale scanning and deeper analysis of high-risk assets.

In addition to threat detection, the platform offers automated remediation features to help organisations address vulnerabilities faster. AI agents can assist with code modernisation, dependency analysis, testing and validation of fixes before deployment. The system also supports continuous monitoring and automated response workflows.

Google said automated, intelligence-led security is becoming increasingly important as cyber threats grow more sophisticated, making faster detection and response essential for modern cybersecurity operations.

## WiFi routers could soon identify people without connected devices

Researchers in Germany have developed a tracking technique that can identify individuals using ordinary WiFi signals, even when they are not carrying smartphones, smartwatches or other connected devices. The study has raised concerns about privacy and surveillance, as the technology relies on wireless infrastructure already present in homes, offices, airports, cafés and public buildings.

The method, called BFId, exploits Beamforming Feedback Information (BFI), a feature introduced with WiFi 5 technology to improve wireless performance. According to the researchers, these feedback signals can be captured and analyzed using machine learning models. The system then creates what the researchers describe as "radio images" by studying how human bodies interact with and alter surrounding radio waves.

Unlike CCTV cameras or facial-recognition systems, the technology does not rely on visual data. Instead, it identifies individuals based on unique patterns generated as radio waves move around their bodies. Researchers claim the approach is accurate enough to distinguish between specific people without requiring them to carry electronic devices. The findings have sparked debate among privacy advocates and cybersecurity experts, highlighting the need for stronger safeguards, improved security controls and greater transparency around the collection and use of wireless data.

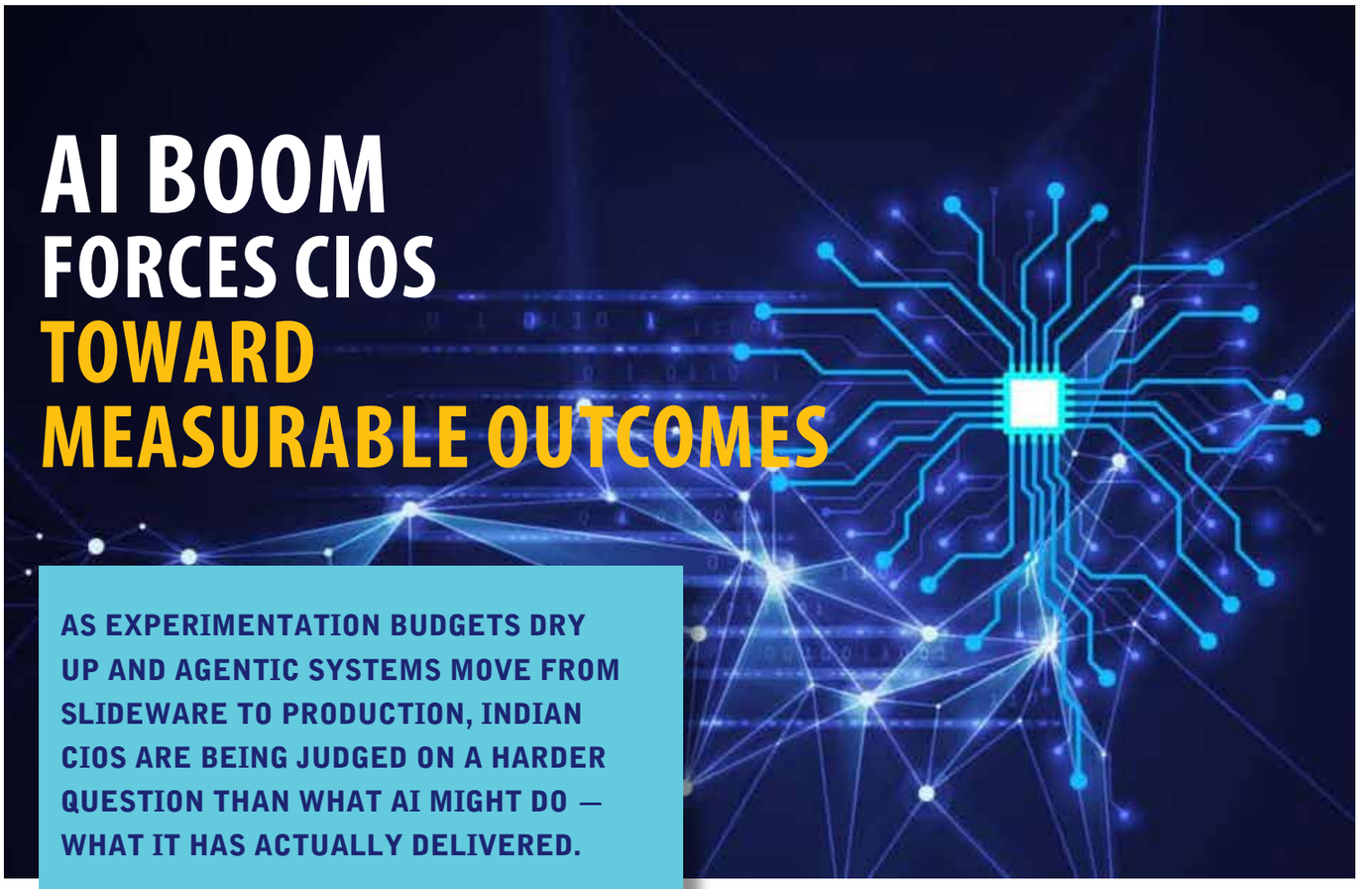
## Leaked Meta audio reveals employee activity used for AI training

Meta is facing fresh scrutiny after leaked audio from an internal meeting revealed that CEO Mark Zuckerberg defended the company's use of employee work activity to train its artificial intelligence systems. The discussion reportedly took place shortly before large-scale layoffs, adding to concerns among employees over monitoring and transparency.

According to reports, Meta's internal Model Capability Initiative collects activity data from company-issued devices, including keyboard inputs, mouse movements and interactions across approved workplace applications. Zuckerberg reportedly argued that employee-generated data offers higher-quality insights than information sourced from external contractors, helping AI models learn advanced coding and problem-solving patterns. He also maintained that the data is anonymised and used only for AI training.

The revelations prompted internal concerns, particularly as employees reportedly had no option to opt out of the programme. The monitoring initiative coincided with broader restructuring and workforce reductions, further heightening unease among staff.

The incident underscores the growing debate around AI development and employee privacy. As technology companies increasingly use workplace data to improve AI systems, questions around transparency, consent and responsible data use are likely to remain under close scrutiny.



# AI BOOM FORCES CIOS TOWARD MEASURABLE OUTCOMES

**AS EXPERIMENTATION BUDGETS DRY UP AND AGENTIC SYSTEMS MOVE FROM SLIDEWARE TO PRODUCTION, INDIAN CIOS ARE BEING JUDGED ON A HARDER QUESTION THAN WHAT AI MIGHT DO — WHAT IT HAS ACTUALLY DELIVERED.**

The mood in the Indian boardroom has changed. For two years, the conversation about artificial intelligence was permissive. Pilots were funded on the strength of a demo, proofs of concept multiplied across functions, and a CIO could earn credibility simply by showing that the organisation was "doing something with AI." That window has closed. In 2026, the directive coming down from CEOs and boards is unequivocal, and it is no longer about ambition. It is about return.

The numbers explain the urgency. Gartner projects global AI spending will reach $2.52 trillion in 2026, a 44 percent year-over-year increase. Yet the same body that tracks the spending also tracks the disappointment. By Gartner's own reckoning, 94% of CIOs expect major changes to their plans within the next 24 months, while only 48% of digital initiatives meet or exceed business targets. The gap between what is being spent and what is being realised has become the defining management problem of the year, and it is forcing a discipline that the experimentation era never demanded.

Kris van Riper, Practice Vice President at Gartner, framed the shift in a single line that has since been repeated across CIO forums. "2025 was about AI pilots, discovery and experimentation. 2026 will be about delivering agentic AI ROI" she said. Agentic AI, in Gartner's view, offers a more direct path to business value than previous generative AI initiatives — but only for organisations that have built the capabilities to capture it.

## THE INDIA CONTEXT IS SHARPER, NOT SOFTER

For Indian enterprises, the pressure arrives with local characteristics that make it more acute. According to Bain & Company, capital expenditure now accounts for 50 to 60 percent of enterprise technology budgets in India, against 20 to 30 percent globally, putting Indian technology capex at roughly 2.5 to 3 times that of international counterparts. A large share of that money is flowing into AI platforms and data modernisation. When a country spends at that intensity, the demand for evidence of return is correspondingly louder.

The maturity question runs underneath all of it. NASSCOM's AI Adoption Index found that enterprise spending on AI in India remains low, with 67 percent of organisations allocating less than 10 percent of their IT budget to AI, and fewer than 15 percent having aligned their AI goals with broader corporate strategy. The same study identified the obstacle that every CIO now names first: end-users see value in moving up the AI adoption curve but are hamstrung by legacy systems and siloed data.

That obstacle has a price tag attached. Bain's India research found that approximately 72 percent of CIOs cite legacy tech debt as the top barrier to transformation, alongside shortages in next-generation skills and unproven ROI from new-age initiatives. The conclusion the firm draws is blunt. Companies must move beyond implementation-based success metrics and adopt outcome-based measures linked to growth, efficiency and profitability.

## FROM PILOT TO P&L

The metrics that graduate an AI project from experiment to value have themselves changed, and productivity gains — the currency of the generative AI era — are no longer sufficient on their own.

A May 2026 reading of the State of the CIO data noted that revenue generation has climbed into the top three CIO performance metrics, with the C-suite demanding that AI function as a primary lever for revenue growth rather than a productivity abstraction.

This is the inversion that defines 2026. Where a CIO could once report adoption rates and hours saved, the board now wants the figure mapped to the profit and loss statement. Gartner's guidance for CIOs is explicit that the discipline must connect technical performance to financial outcomes, replacing speculative AI pilots with an architecture that ensures every model and agent delivers a measurable and sustainable impact on the P&L.

The financial leadership is already operating this way. Salesforce research

found that 61 percent of CFOs say AI agents are changing how they evaluate ROI, measuring technology investment success across a broader range of business outcomes than traditional metrics capture. The KPI conversation is now a joint one with the CFO, conducted in the language of cost reduction, margin improvement and revenue, with productivity treated as a supporting indicator rather than the headline.

The Indian opportunity, where the discipline is applied, is substantial. Bain estimates that enterprises adopting a "future-back" strategy — redesigning operations and architecture around long-term AI-driven business models — could unlock 15 to 20 percent absolute EBITDA improvement through a mix of efficiency gains and revenue growth. That is the prize that disciplined measurement is meant to secure.

## THE INFRASTRUCTURE BOTTLENECK

AI agents are only as good as the data and systems beneath them, which has lifted infrastructure modernisation from a back-office concern to a board-level precondition for any return.

The structural point is direct. A May 2026 assessment of the CIO mandate held that moving from static, siloed databases to real-time, event-driven architectures is now a prerequisite for any AI initiative intended to generate actual ROI.

NASSCOM's Strategic Review for 2026 frames the industry-level shift as a structural realignment in which AI moved from optional to core infrastructure, with agentic systems shifting AI from support to execution and embedding efficiency and governance as new competitive strengths. The Indian IT services and channel ecosystem has read this correctly. Providers are re-engineering revenue models away from FTE-based delivery toward outcome-based, risk-sharing constructs as AI-driven productivity materialises — a change that places the burden of measurable results on the vendor as much as the buyer, and one that channel partners will feel acutely as procurement language shifts from licences to deltas.

For the CIO, the practical implication is that infrastructure modernisation can no longer be sequenced after AI adoption. It is the entry ticket. The warning attached to inaction is sharp: organisations that fail to move from experimentation to architectural integration risk seeing their budgets diverted to more agile, data-native competitors.

## DEFENCE AT MACHINE SPEED

Readiness against automated attack now reaches well beyond uptime into a category that did not exist in its current form two years ago, because the threat environment has been rewritten by the same technology driving the boom.

The scale of the shift is documented in primary threat research. CrowdStrike's 2026 Global Threat Report recorded a 340 percent increase in AI-assisted intrusion attempts compared with 2024, with adversarial AI tools now responsible for roughly 38 percent of all credential-harvesting campaigns globally. The barrier to entry has collapsed: what once required a skilled operator and weeks of reconnaissance can now be executed cheaply against thousands of targets at once.

The velocity is the core of the problem. Mandiant's analysis of agentic attack clusters in 2026 found that such systems can achieve lateral movement in under four minutes, while the average enterprise security team still takes 197 minutes to detect a breach, according to IBM's Cost of a Data Breach research. That gap is the new attack surface, and it is one that fixed-script defences and human-paced response cannot close.

Measuring defensive readiness, therefore, means measuring response velocity, not just availability. The vendor response signals where the metric is heading. IBM has introduced Autonomous Security, a machine-speed service of AI agents that automates vulnerability remediation at a pace humans alone cannot sustain, on the explicit basis that enterprises must now match the speed of AI-generated attacks. Microsoft has taken a parallel route, disclosing that its multi-model agentic scanning system uncovered sixteen new vulnerabilities across the Windows networking and authentication stack, including four critical remote-code-execution flaws, by orchestrating more than a hundred specialised AI agents to discover and prove exploitable bugs end to end.

The lesson for the CIO is that defensive readiness, measured honestly, is no longer a single uptime figure. It is a composite of detection-to-containment time, the proportion of the estate covered by autonomous response, and the auditability of every action an agent takes — because automation without governance simply moves the risk rather than removing it.

## THE DISCIPLINE YEAR

The thread connecting the three priorities is the same. The AI boom has not slowed in India — IDC projects domestic AI spending will reach $6 billion by 2027 at a compound annual growth rate of 33.7 percent, and agentic adoption is already running ahead of the global curve. What has changed is the standard of proof.

The CIO who thrives in 2026 will be the one who can point to a number, defend the architecture beneath it, and demonstrate that the same intelligence reshaping the business has been turned into a measurable defence of it.

**94% vs 48%**

**SHARE OF CIOS EXPECTING MAJOR PLAN CHANGES WITHIN 24 MONTHS, AGAINST THE SHARE OF DIGITAL INITIATIVES THAT ACTUALLY MEET BUSINESS TARGETS.**

**(GARTNER)**

**72%**

**INDIAN CIOS WHO NAME LEGACY TECH DEBT AS THE SINGLE BIGGEST BARRIER TO AI TRANSFORMATION.**

**(BAIN & COMPANY)**

**340% / 197 minutes**

**RISE IN AI-ASSISTED INTRUSION ATTEMPTS SINCE 2024, AGAINST THE AVERAGE TIME AN ENTERPRISE TEAM STILL TAKES TO DETECT A BREACH, WHILE AGENTIC ATTACKERS MOVE LATERALLY IN UNDER FOUR MINUTES.**

**(CROWDSTRIKE)**

## IBM invests $5 billion for a cybersecurity initiative called Project Lightwell

IBM has announced a $5 billion cybersecurity initiative called Project Lightwell, aimed at protecting open-source software from highly advanced AI threats. The company has enlisted its subsidiary Red Hat, and the project is backed by a global force of more than 20,000 engineers. According to IBM CEO Arvind Krishna, the catalyst for this enormous investment was the capability of Anthropic's powerful AI model, Mythos, which found software vulnerabilities and worried banks and governments worldwide.

Project Lightwell will establish a trusted enterprise clearinghouse combined with a global force of engineers to identify and fix vulnerabilities at scale. The clearinghouse will serve as a security coordination layer, using advanced AI capabilities to validate and test fixes across an unprecedented volume of open source code. These capabilities will be offered through commercial subscriptions, allowing enterprises to integrate secure patches directly into their existing software supply chains with enterprise-grade validation and lifecycle management.

## Intel, Odisha government to set up $3.3 billion semiconductor materials facility in India

Intel signed a pact with 3D Glass Solutions (3DGS) and the Odisha government to set up a $3.3 billion advanced packaging glass-core substrate manufacturing facility in the Bhubaneswar-Khurda region. The government said in a press note that Intel will support the project with technology know-how and process expertise.

The proposed project is among the largest high-technology manufacturing investments in the country, particularly in the semiconductor space. The facility will focus on substrate manufacturing, a critical material and process technology used for mounting semiconductor chips on motherboards.

The project, to be implemented in phases over the next five to six years, is expected to generate around 1,800 highly skilled jobs. The facility will focus on substrate manufacturing, a critical material and process technology used for mounting semiconductor chips on motherboards.

## Govt pushes big-tech investments to strengthen West Bengal's digital economy

The Indian government is stepping up efforts to position West Bengal as a major technology and innovation destination by engaging with global technology companies and domestic business groups for large-scale investments in data centres, semiconductor projects, and research and development facilities.

According to reports citing sources familiar with the developments, discussions are currently underway with semiconductor firms and global capability centres, with some investment proposals expected to move forward as early as June. The initiative is part of a broader push to accelerate industrial growth and expand the state's digital infrastructure ecosystem.

The move also aligns with the state government's ambitious Silicon Valley project, a large technology hub being developed over nearly 250 acres. The project is expected to attract investments worth around Rs. 30,000 crore and generate close to 7,500 employment opportunities. Officials indicate that development work is progressing steadily, with land already allotted to several companies.

## Chhattisgarh's e-Governance nodal agency partners with Salesforce to empower Digital Dwaar

Chhattisgarh Infotech Promotion Society (CHiPS), the state's nodal agency for e-Governance, announced a strategic collaboration with Salesforce to deploy MuleSoft as the technology backbone of Digital Dwaar — the state's unified Application Programming Interface (API)-based data exchange platform.

The collaboration marks a significant step in Chhattisgarh's journey toward building a connected, citizen-centric digital governance ecosystem aligned with the Government of India's Digital India vision.

As Chhattisgarh scales its digital transformation, the state recognized that fragmented systems and manual data coordination were barriers to effective, responsive governance. CHiPS adopted an API-led integration strategy with MuleSoft at its core, establishing Digital Dwaar as a centralized API exchange where all state departments can publish and consume data services through a single, governed platform. This replaces coordination that previously took days or weeks with instant, API-driven data access.

## Dell bags Pentagon software deal worth $9.7 billion after donating to Trump accounts

The U.S. Department of Defense has awarded Dell Technologies a five-year contract worth approximately $9.7 billion to deliver a suite of software to the country's military.

As per the agreement, officially titled the Microsoft Department of War Enterprise Software Agreement II Core Enterprise Technology Agreement, Dell will provide Microsoft 365, advanced cloud subscriptions and on-premises licensing capability.

According to Defense Department Chief Information Officer Kirsten Davies and acting Navy CIO Barry Tanner during a Pentagon briefing, the contract was secured by Dell Federal Systems, the company's government-focused division. The company won the contract following a competitive evaluation process. Officials said vendors were assessed on competitive pricing, alignment with General Services Administration benchmarks and overall value delivered to the department, with Dell emerging as the top choice.

The contract comes amid growing ties between Michael Dell, founder and CEO of Dell Technologies and Trump administration. Michael Dell pledged $6.25 billion last year to fund investment accounts for children known as "Trump accounts."

## Anthropic surpasses OpenAI in valuation after massive funding round

Artificial intelligence company Anthropic has emerged as the world's most valuable AI startup following a major Series H funding round that significantly boosted the company's market valuation. The latest financing round reportedly valued Anthropic at $965 billion, placing it ahead of rival OpenAI, which was previously valued at $852 billion earlier this year.

According to reports, the funding round was backed by major investors including Altimeter Capital, Dragoneer, Greenoaks, and Sequoia Capital. The financing package also included previously committed investments, among them a substantial contribution from Amazon. The latest capital infusion marks a sharp rise in Anthropic's valuation compared to earlier this year, highlighting growing investor confidence in enterprise-focused AI companies.

Anthropic's rapid growth has also been reflected in its financial performance. The company reportedly reached a $47 billion revenue run rate, a major jump from earlier projections. Much of this momentum has been driven by the increasing adoption of Claude Code, Anthropic's AI-powered coding assistant, which has gained popularity among enterprises and software developers.

## Palo Alto Networks to Acquire Portkey to Strengthen AI Agent Security

Palo Alto Networks has announced plans to acquire Portkey, a specialist in AI gateway technology, as it looks to address rising security risks tied to autonomous AI agents in enterprises.

The deal is aimed at integrating Portkey's capabilities into Palo Alto Networks' Prisma AIRS platform, creating a centralized control layer to monitor, manage, and secure AI-driven interactions across organizations.

Portkey's technology acts as an "AI gateway," enabling enterprises to oversee how AI agents operate, communicate, and access data. The platform already processes trillions of tokens each month and is designed to support low-latency, agent-to-agent communication at scale.

The acquisition comes as enterprises move beyond AI copilots to deploying autonomous agents capable of making decisions and executing workflows across systems. This shift, Palo Alto Networks said, is creating a new and largely unmanaged attack surface.

## Delhi government seeks AI solutions to improve public services

The Delhi government has announced plans to collaborate with technology companies, startups, and academic and research institutions working in artificial intelligence to develop innovative solutions aimed at improving governance and public service delivery. Officials said that the initiative will focus on key urban and civic sectors including healthcare, education, air quality monitoring, mobility, urban planning, and citizen services, with the goal of making administrative systems more efficient and responsive.

The Information Technology Department has formally invited participation from eligible stakeholders to showcase AI-based tools that can strengthen governance frameworks across multiple departments. The emphasis will be on applications such as digital health governance, predictive disease detection, hospital resource optimisation, smart mobility systems, and citizen-centric digital platforms. According to senior officials, the initiative is designed to identify practical, scalable technologies that can be adopted through pilot deployments at the departmental level.

## Karnataka Govt. inaugurates state-led Centre of Excellence for Space Technology in Bengaluru

To strengthen India's rapidly growing space economy, Government of Karnataka has come up with the country's first state-led Centre of Excellence for Space Technology, established by Karnataka Innovation and Technology Society in collaboration with SIA (Satcom Industry Association India) -India.

The facility was inaugurated by Minister for Electronics, IT/BT, and Rural Development and Panchayat Raj, Priyank Kharge, in the presence of senior officials and industry leaders.

The initiative will enhance India's ability to convert space innovation into scalable commercial opportunities.

At the launch, Kharge said that Karnataka has consistently led India's technology and innovation journey, and that the new Centre extends this leadership into one of the country's most strategic future-facing sectors.

"Our focus is not just on advancing research, but on creating an ecosystem where innovation can translate into real-world applications, economic growth, and high-quality jobs. This Centre will play a critical role in positioning Karnataka as a key driver of India's space economy," he said.

## Tata Electronics becomes Apple's largest manufacturing partner in India

Tata Electronics has overtaken Foxconn to become Apple's largest contract manufacturing partner in India by employee strength, marking a significant shift in the country's electronics manufacturing landscape. According to a recent report, the company's workforce has surged to nearly 75,000, reflecting an aggressive scale-up strategy within a short span.

This growth is particularly striking given that Tata Electronics had a workforce of just around 15,000 employees two years ago, when it entered into a partnership with Apple. The rapid expansion has been fuelled by its large manufacturing facility in Hosur, Tamil Nadu, as well as the acquisition of Indian operations from global suppliers Wistron and Pegatron.

The company's hiring push has been part of a broader effort to build the scale and expertise required to meet Apple's stringent global manufacturing standards. By expanding across multiple locations, Tata Electronics has strengthened its operational footprint and positioned itself as a key player in iPhone assembly in India.

## Cabinet clears ₹3,900-crore semiconductor projects to boost domestic chip ecosystem

The Union Cabinet has approved two new semiconductor projects in Gujarat under the India Semiconductor Mission, aiming to expand chip manufacturing capacity, generate skilled jobs, and strengthen India's position in global electronics supply chains.

In a significant move to strengthen India's semiconductor ambitions, the Union Cabinet led by Narendra Modi has approved two new chip manufacturing projects with a combined investment exceeding ₹3,900 crore. The projects, sanctioned under the India Semiconductor Mission, will be established in Gujarat and are expected to generate employment for over 2,200 skilled professionals.

With these additions, the total number of approved semiconductor projects in the country has risen to 12, taking cumulative investments in the sector to approximately ₹1.64 lakh crore. The move reflects the government's continued focus on building a resilient and self-reliant semiconductor ecosystem amid rising global demand for advanced electronics.

## Reliance explores major push into satellite internet business

Reliance Industries is reportedly preparing a large-scale entry into the satellite communications sector, with plans to invest heavily in low earth orbit (LEO) satellite technology as competition intensifies in the global broadband connectivity market.

According to reports, the initiative will be led through Jio Platforms, the company's digital and telecom arm, which is expected to spearhead Reliance's ambitions in space-based internet services. The move could place the conglomerate in direct competition with global players such as Starlink, Project Kuiper and Eutelsat OneWeb.

Reliance Industries Limited

Industry reports suggest Reliance is evaluating multiple strategies to accelerate its satellite ambitions, including both in-house development and potential acquisitions. The company is believed to be exploring ways to create a domestic satellite network capable of supporting broadband access across India, particularly in underserved and remote regions.

# From Tech Debt to AI Readiness: India's Channel Partners Step Up

**Channel leaders discuss how legacy modernisation, measurable AI outcomes, and Zero Trust security are helping enterprises navigate the challenges of an increasingly AI-driven world.**

Artificial intelligence is no longer a futuristic concept or a technology confined to pilot projects. Across industries, organisations are increasingly looking to AI as a strategic enabler of growth, efficiency, innovation, and competitive advantage. However, as enterprises move from experimentation to large-scale deployment, the path to successful AI adoption is proving far more complex than simply implementing new tools or platforms. Legacy infrastructure, fragmented data environments, mounting technical debt, and rapidly evolving cybersecurity threats continue to present significant challenges, forcing organisations to rethink their technology strategies from the ground up.

For India's channel partners, this shift marks a pivotal moment. The traditional role of delivering hardware and software solutions is rapidly evolving into one that demands deeper business understanding, consulting expertise, and the ability to guide customers through complex digital transformation journeys. Enterprises today are looking for trusted partners who can help modernise legacy environments, create AI-ready infrastructure, ensure security and compliance, and deliver measurable business outcomes from technology investments.

One of the most pressing challenges facing organisations is the burden of technical debt accumulated over years of operating legacy systems, siloed applications, and disconnected data environments. Many enterprises recognise the potential of AI but struggle to realise its benefits because their existing infrastructure lacks the scalability, interoperability, and data accessibility required to support modern AI workloads. As a result, infrastructure modernisation and cloud readiness have become critical priorities for organisations seeking to unlock the full value of AI.

At the same time, business leaders and CIOs are under increasing pressure to justify AI investments through tangible and measurable outcomes. The conversation has moved beyond experimentation and proof-of-concept projects to questions around productivity improvements, operational efficiency, cost optimisation, faster decision-making, enhanced customer experiences, and overall business impact. Demonstrating clear return on investment has become essential for securing stakeholder confidence and scaling AI initiatives across the enterprise.

Adding another layer of complexity is the rise of AI-powered cyber threats. As attackers leverage artificial intelligence to automate and enhance their tactics, traditional security models are becoming increasingly inadequate. This has accelerated the adoption of Zero Trust architectures, identity verification frameworks, continuous authentication mechanisms, and AI-driven threat detection capabilities, with security now being embedded into the foundation of digital transformation strategies rather than treated as an afterthought.

Against this backdrop, VARINDIA engaged with leading channel partners, particularly system integrators and technology solution providers, to understand how they are helping customers navigate this rapidly evolving landscape. Their insights centre on three critical priorities: reducing technical debt and modernising legacy systems to enable advanced AI adoption; demonstrating measurable business outcomes and return on investment from AI initiatives; and integrating Zero Trust and identity-centric security frameworks to counter increasingly sophisticated AI-driven cyber threats. Together, their perspectives provide a comprehensive view of how India's channel ecosystem is evolving to meet the demands of an AI-driven future.

## Prioritising secure AI modernisation with measurable business outcomes

**AMARDEEP SHARMA**
**CTO & DIRECTOR, PRARUH TECHNOLOGIES LTD.**

"Overcoming challenges in today's AI-driven landscape requires channel partners to evolve from transactional vendors into long-term digital transformation advisors. At Praruh Technologies, our approach is focused on helping enterprises modernise securely while delivering measurable business outcomes and sustainable growth. One of the biggest barriers to AI adoption is the accumulation of "tech debt" within legacy infrastructure, where fragmented systems often lack interoperability, scalability, and real-time data visibility, slowing innovation and limiting the effectiveness of AI initiatives.

To address this, we help clients through phased modernisation strategies that include cloud readiness assessments, infrastructure consolidation, API-led integration, automation frameworks, and workload optimisation. Rather than encouraging complete rip-and-replace transitions, we focus on hybrid and scalable architectures that allow enterprises to modernise gradually while maintaining operational continuity. This approach improves AI readiness while reducing long-term operational complexities and infrastructure costs. For today's cost-conscious CIOs, AI investments must deliver measurable business value beyond experimentation.

Every deployment we undertake is aligned with business KPIs such as reduction in manual workloads, faster incident response times, improved predictive analytics accuracy, lower infrastructure downtime, enhanced employee productivity, and optimisation of operational expenses. At the same time, AI-driven cyber threats are becoming increasingly sophisticated, making security a critical foundation of every transformation initiative. Our solutions are designed around Zero Trust principles, integrating continuous verification, least-privilege access, identity-centric security, multi-factor authentication, endpoint visibility, and AI-driven threat monitoring to strengthen cyber resilience."

## Modernising legacy infrastructure for secure and scalable AI adoption

**GURPREET SINGH**
**FOUNDER & MD, ARROW PC NETWORK PVT. LTD.**

"At Arrow PC Network, we see tech debt as one of the biggest barriers to meaningful AI adoption. Many organisations want to move fast, but their existing systems are not always ready. Our approach is to modernise in phases, starting with infrastructure assessment, workload rationalisation, and integration planning. We are also helping enterprises upgrade into modern IT through the IT Recycling Program by Arrow PC Network, enabling customers to unlock value from existing IT assets while moving toward scalable, secure, and AI-ready architectures without disrupting business continuity.

CIOs today are looking for clear business impact, not just technology promises. We demonstrate AI ROI through measurable outcomes such as improved productivity, faster decision-making, reduced manual effort, better resource utilisation, and stronger operational efficiency. We also track improvements in response time, automation levels, and infrastructure performance. For us, AI must show value in practical terms, whether that is lowering operating effort, improving service delivery, or helping teams work smarter and faster. That is how trust is built with cost-conscious decision-makers.

AI-led threats require a security model that assumes risk at every layer. That is why Zero Trust and identity verification are central to our approach. We focus on strong access control, continuous authentication, least-privilege access, and identity-aware security policies to help organisations protect users, devices, data, and applications more effectively. At Arrow PC Network, we believe security must be embedded by design, not added later."

## Reducing tech debt for AI-ready telecom and IT transformation

**JIGAR SANGHVI**
**DIRECTOR, SANGHVI INFOTECH PVT. LTD.**

"At Sanghvi Infotech, we help clients reduce tech debt by modernising legacy telecom and IT environments into secure, scalable, and AI-ready platforms. Our system integration approach connects networks, Wi-Fi, cloud, cybersecurity, and digital infrastructure to eliminate silos, improve efficiency, and create the technological foundation needed for advanced AI-driven innovation. In telecom, ISP, and managed Wi-Fi environments, tech debt often appears as siloed networks, ageing infrastructure, poor visibility, manual operations, and systems that do not share data well.

We address this by consolidating networks, modernising core infrastructure, improving interoperability, and building resilient architectures using managed Wi-Fi, SD-WAN, VPNs, cloud-based networking, edge services, and enterprise system integration. We demonstrate AI ROI through measurable outcomes such as lower operating costs, faster process turnaround, reduced manual effort, improved network and system uptime, better service response times, and stronger decision-making through real-time data visibility. For cost-conscious CIOs, we focus on business metrics that matter most, including productivity gains, error reduction, automation-led savings, and the speed at which AI use cases move from pilot to scalable business value.

We embed Zero Trust and identity verification frameworks into our core solutions so that every user, device, application, and network request is continuously verified before access is granted. By combining strict identity controls, least-privilege access, segmentation, and real-time monitoring, we help clients build resilient digital environments to counter AI-led cyber threats."

## Building secure and scalable digital infrastructure for AI-driven transformation

**KUMAR BACHCHAN**
**MD & CEO, NIVESHAN TECHNOLOGIES INDIA PVT. LTD.**

"At Niveshan Technologies, we believe AI adoption must begin with secure and scalable digital infrastructure. Many enterprises and PSUs still operate fragmented legacy environments that limit automation and operational efficiency. Our focus is therefore on infrastructure modernisation through cloud-ready platforms, cybersecurity strengthening, SD-WAN, and integrated data centre transformation. Projects delivered for organisations across railways, petroleum, telecom, and BFSI have helped create resilient digital ecosystems capable of supporting future AI-driven operations.

We see AI as the next layer of transformation, enabling predictive monitoring, intelligent automation, and operational analytics on top of strong infrastructure foundations. Our AI strategy is focused on measurable business outcomes rather than experimentation alone. Since we already manage mission-critical environments across smart cities, telecom, transport, BFSI, healthcare, and PSU sectors, we view AI as a capability that enhances efficiency and resilience across existing infrastructure investments. Key performance indicators include reduced downtime, faster incident response, lower operational overhead through automation, improved SLA compliance, enhanced cybersecurity visibility, and better infrastructure utilisation.

Cybersecurity is being strengthened through Zero Trust and identity-centric security frameworks designed for hybrid and mission-critical environments. Our approach includes MFA, IAM, PAM, SOC-led monitoring, endpoint verification, micro-segmentation, and secure SD-WAN architectures. Building on our experience across telecom, smart cities, healthcare, transport, and government infrastructure, we see AI-enhanced cybersecurity capabilities such as anomaly detection and intelligent threat analytics further improving cyber resilience and secure digital transformation."

## Supporting enterprise AI adoption through infrastructure modernisation

**L ASHOK**
**MD, FUTURENET TECHNOLOGIES (INDIA) PVT. LTD.**

"As of now, at Futurenet Technologies, we advise and consult on AI migration and the setup of AI infrastructure both on-premises and in the cloud. Our focus is on helping organisations modernise infrastructure environments to support advanced AI adoption. We believe enterprises must first establish the right AI infrastructure foundation before implementing AI initiatives. Through our consulting and advisory approach, we help customers identify suitable deployment models, infrastructure requirements, and implementation strategies.

AI investments largely justify themselves through enormous increases in productivity and significant reductions in cost. However, the key lies in identifying the right areas for implementation. This is addressed through our audit and advisory framework, which helps organisations evaluate where AI can deliver improved efficiency, better resource utilisation, and operational value. Our approach is focused on ensuring AI adoption remains practical and aligned with business requirements.

Our SIEM comes built in with AI-based pattern recognition and user behaviour analysis to strengthen threat detection and monitoring capabilities. Before SIEM implementation, we help customers thoroughly define processes and implement best practices in technology. The key is identifying the threat landscape and working proactively. We believe organisations must combine strong processes, security visibility, and proactive monitoring to counter evolving AI-led cyber threats more effectively."

## Building AI-driven security ecosystems for enterprise transformation

**MUSTAFA LOTIA**
**SVP - GLOBAL ADVISORY & CONSULTING, INSPIRA ENTERPRISE**

"Being a global cybersecurity, AI, and data analytics service provider, we help organisations modernise legacy systems by implementing intelligent automation and security data ecosystems across business operations. Our AI-powered digital transformation services enable organisations to adopt cloud-ready architectures that support AI, analytics, and computing workloads. We are helping organisations accelerate AI adoption by moving from fragmented security operations to an integrated, AI-driven security ecosystem that delivers visibility, governance, automation, and resilience. Our key capabilities include AI-driven SOC operations, AI-Augmented Triage, Adversarial AI Defense, AI-Enhanced Threat Hunting, Continuous Threat Exposure Management, and Autonomous Intelligence Fusion and Response.

With our AI Control Tower, organisations are able to connect strategy to execution while maintaining compliance, transparency, and control effectiveness across the enterprise. CIOs are under growing pressure to prove AI ROI, and we address this through measurable outcomes such as reduction in mean time to respond, time saved with AI, lower infrastructure maintenance costs, improved operational efficiency, fraud detection, risk mitigation, and improved transaction monitoring and compliance adherence. One of the biggest value drivers is moving from periodic audits toward AI-driven real-time detection.

At Inspira Enterprise, our Zero Trust and Identity Verification posture is anchored to NIST SP 800-207 and the CISA Zero Trust Maturity Model 2.0. Through AI-driven behavioural analytics, real-time telemetry, and our proprietary iSMART2 platform, we help organisations strengthen cyber resilience against evolving AI-led threats, lateral movement, and anomalous access patterns across enterprise environments."

## Enabling secure and sustainable AI adoption through infrastructure modernisation

**NEEL SHAH**
**CHAIRMAN, INSIGHT BUSINESS MACHINES PVT. LTD.**

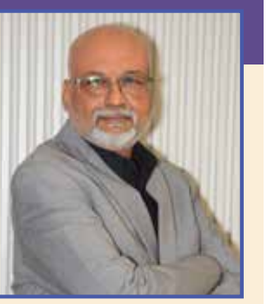
"At Insight Business Machines, I believe the biggest challenge in 2026 is not just adopting AI, but staying relevant while doing it securely, responsibly, and with clear business outcomes. Customers are moving beyond AI experimentation, while CIOs are under pressure to modernize legacy systems, improve resilience, control costs, and still drive innovation. Many organizations still run on fragmented infrastructure, disconnected security tools, and legacy applications not designed for AI-led environments, slowing decision-making and increasing operational complexity.

Through our ISMAC approach, which combines Infrastructure, Security, Mobility, AI/Automation, and Cloud, we help customers modernize in a phased manner. We focus on building strong foundations through hybrid cloud, observability, automation, identity governance, endpoint visibility, and data accessibility without disrupting business operations. Once stable and scalable, AI adoption becomes more effective and sustainable. CIOs today are highly outcome-focused, expecting measurable value such as lower downtime, faster incident response, better infrastructure utilization, reduced manual effort, and improved user experience. Customers also see faster detection and recovery cycles with stronger operational visibility, improving productivity, continuity, and decision-making.

Cybersecurity is central to every AI discussion as threats increasingly target identities, endpoints, and access layers. Security must be embedded from the start. Our approach combines Zero Trust principles, identity verification, privileged access management, endpoint visibility, continuous monitoring, observability, and integrated threat intelligence into a unified security framework. The goal is simple: help customers innovate with confidence while staying resilient against evolving cyber risks, ensuring relevance through trust, resilience, measurable outcomes, governance, and sustainability."

## Trust and identity verification are becoming the foundation of secure AI adoption

**PRASHANT JAIN**
**FOUNDER & DIRECTOR, JNR MANAGEMENT RESOURCES PVT. LTD.**



"Every AI initiative organisations want to pursue — agents, copilots, automated workflows, and predictive analytics — has a trust dependency. Data must be trusted, identities must be verified, models must be governed, and outputs must be auditable. Identity and trust of AI agents are most important. In many ways, tech debt is simply an accumulated trust deficit, and modernisation is what helps pay down that deficit while supporting advanced AI adoption.

The most credible AI ROI programs establish baseline metrics before rollout, control groups or phased adoption, quarterly measurement cadence, business-owner accountability, and a clear financial attribution methodology. Without baselines, AI ROI claims are often challenged by finance teams. For cost-conscious CIOs, measurable outcomes and operational accountability are critical in demonstrating the real business value of AI investments. AI adoption must therefore be backed by structured measurement frameworks rather than assumptions around productivity or efficiency gains alone.

AI-led threats are identity-first attacks, and Zero Trust is an identity-first defence. Every AI attack vector — phishing, credential stuffing, deepfakes, agent compromise, and session hijacking — targets identity. Zero Trust responds by making identity cryptographically verifiable, continuously validated, and dynamically enforced. Traditional security assumed users inside the network were trusted, whereas modern Zero Trust assumes every identity, device, workload, API call, and AI interaction could be compromised. That mindset shift is becoming the real foundation for defending against AI-driven cyber threats and building continuous trust across enterprise environments."

## Structured modernisation and Zero Trust are critical for enterprise AI

**PRASHANTH SUBRAMANIAN**
**CO-FOUNDER & DIRECTOR, QUADRASYSTEMS.NET (INDIA) PVT. LTD.**

"Legacy modernisation is less a technology problem and more a sequencing problem. Many enterprises attempt AI adoption without first resolving data readiness, integration architecture, and workflow dependencies, and that is where value gets stranded. Our starting point is a structured drivetrain audit that maps the gap between an organisation's current infrastructure and what is required to operationalise AI at scale. Remediation work spans Azure Fabric migrations, cloud-native re-architecture on AWS and Google Cloud, and decommissioning legacy data silos that block AI pipelines. The objective is not modernisation for its own sake, but building infrastructure that can convert AI capability into measurable business outcomes.

We have moved away from productivity framing entirely because CIOs today want business-case-level numbers, not efficiency percentages. Our AI engagement model establishes a measurement framework upfront across productivity, process efficiency, customer impact, innovation velocity, and business outcome contribution, each tracked against a pre-agreed baseline. Most AI investments stall not because technology underperforms, but because the measurement architecture was never built. We call the alternative "productivity theatre" — visible AI activity with no tracked business value.

Zero Trust is a design principle in our solution architecture, not a product category. Our approach combines identity-first security through Microsoft Entra, zero-trust network access through Zscaler, and endpoint threat intelligence through CrowdStrike, integrated and monitored through BluForge, our managed security operations service. AI-driven threats now extend across agentic workflows, AI model inputs, and API layers, making defensible architecture and structured threat assessment increasingly critical."

## Building AI-ready enterprises with outcome-driven modernisation

**RAJ KAMAL SINGHAL**
**CEO, HITACHI SYSTEMS INDIA**

"Enterprise modernisation is no longer a technology refresh exercise - it is a strategic imperative that defines how organisations compete, innovate, and lead in an AI-driven economy."

At Hitachi Systems India, legacy modernisation is the foundation on which AI-led enterprise transformation is built. Every engagement begins with a structured technology assessment to identify integration gaps, data silos, operational inefficiencies, and AI-readiness barriers. We then co-design phased migration roadmaps that help organisations retire redundant infrastructure while building cloud-native, AI-ready environments without disrupting business continuity.

Our transformation strategy spans Cloud, Cybersecurity, Data Centre, and Observability simultaneously because cloud adoption without security readiness creates new risks, while infrastructure modernisation without observability limits operational visibility and agility. Guided by ART - Agility, Responsibility, and Transparency - we focus on delivering measurable customer outcomes rather than isolated activities.

AI-powered Observability and ITSM platforms enable enterprises to shift from reactive operations to predictive, intelligence-led management through real-time visibility and actionable insights. Zero Trust and Identity Verification are embedded as foundational architecture principles across every solution. Our AI-driven Security Operations Centre leverages behavioural analytics and advanced threat intelligence to help enterprises detect, prevent, and respond to sophisticated cyber threats in an increasingly AI-led digital landscape."

## AI adoption must be built on secure and scalable infrastructure

**RANJAN CHOPRA**
**FOUNDER & MD, TEAM COMPUTERS**

"AI adoption cannot succeed on fragmented, legacy-heavy environments. Many enterprises today are dealing with accumulated tech debt, including disconnected data systems, siloed infrastructure, manual workflows, and outdated security architectures that limit scalability and slow down innovation. Our approach begins with infrastructure rationalisation and data modernisation to help organisations move toward integrated, cloud-ready architectures that support AI workloads securely and efficiently. Working closely with partners like Cisco and NVIDIA, we are helping enterprises build secure, scalable, and future-ready environments for AI adoption through AI-ready networking, modernised data centres, cybersecurity, scalable AI infrastructure, AI factories, and digital twin environments.

Today's CIOs are far more outcome-focused than they were during the early AI experimentation phase. At Team Computers, our approach is measured through operational efficiency, cost reduction, and measurable business value rather than theoretical AI narratives. We typically measure ROI through reduced incident resolution times, faster onboarding cycles, lower operational overhead, improved infrastructure uptime, better compliance readiness, enhanced service desk efficiency, and stronger utilisation of enterprise data assets. AI-driven automation also helps reduce manual intervention and improve decision-making speed.

As AI capabilities evolve, cyber threats are becoming faster, more adaptive, and harder to detect using traditional perimeter-based security models. At Team Computers, security is embedded into the design of our solutions through continuous identity verification, device posture validation, least-privilege access controls, policy-driven enforcement, conditional access, and AI-assisted threat detection across users, endpoints, applications, and cloud environments."

## Enterprise AI is shifting from experimentation to measurable outcomes

**SAI GOPAL**
**DIRECTOR, SOFTCELL TECHNOLOGIES GLOBAL PVT. LTD.**

"The challenge for Indian CIOs today is not that AI options are scarce. Every OEM is leading with its own AI capability, while large horizontal platforms are increasingly going direct. CIOs are left to sort through overlapping pitches and decide what is real, relevant, and safe to deploy. This is where a good IT partner makes the difference. Most AI conversations in India still begin with a legacy estate that was not built for AI. We help clients rationalise infrastructure, get data into a usable shape, tighten identity and access, and match workloads to the right environment. For the mid-market, where budgets are tighter and the gap is widest, we are also building offerings on top of our OEM stacks to make modernisation faster and more affordable.

CIOs are no longer willing to fund a pilot for its own sake. Conversations now begin with what is going to change — hours saved, tickets closed faster, audits made easier, and fewer incidents in the first place. We agree these outcomes with customers at the outset, put measurement in place, and track against them. AI spend has to show measurable operational impact.

Governance and security are now the same problem. We bring Zero Trust, identity verification, endpoint protection, data security, threat intelligence, and SOC monitoring together so controls are in place before the AI use case goes live. Where the use case allows, we also lean towards architectures that keep sensitive data closer to the endpoint or within the customer's own environment."

## Helping customers reduce technical debt and build AI-ready, secure digital environments

**SAIRAMAN MUDALIAR**
**DIRECTOR, PENTAGON SYSTEM AND SERVICES PVT. LTD.**

"At Pentagon, we are helping customers reduce technical debt by modernising legacy infrastructure through cloud adoption, scalable architectures and AI-ready environments. Many organisations today face challenges with fragmented systems and operational inefficiencies that slow down innovation. Our focus is on simplifying and integrating their IT ecosystem while ensuring flexibility, security and long-term scalability. This enables customers to build a stronger foundation for advanced AI adoption and future-ready digital transformation.

At the same time, CIOs are increasingly focused on measurable business outcomes rather than AI experimentation alone. We help customers evaluate AI investments through key metrics such as operational efficiency, automation impact, faster turnaround time, improved customer experience and cost optimisation. Our approach is centred around practical AI use cases that solve real business challenges and deliver visible, long-term ROI. By focusing on outcomes that matter to the business, we help organisations realise the value of their AI investments while supporting long-term growth and transformation.

As AI-led cyber threats continue to evolve, security has become a core business priority. We are integrating Zero Trust principles, identity verification frameworks, proactive monitoring and security-first infrastructure into our solutions to strengthen customer resilience. With our growing investments in cybersecurity capabilities, including managed security solutions, we are focused on delivering secure-by-design environments that support both innovation and business continuity."

## Addressing tech debt through layered modernisation, AI-driven ROI and Zero Trust security

**SANJAY PATODIA**
**CEO & DIRECTOR, GALAXY OFFICE AUTOMATION PVT. LTD.**

"We address infrastructure tech debt through a layered modernisation approach. Where necessary, we replace fragile legacy infrastructure with modern AI-ready, hyper-converged, software-defined data centres. Our AI Factory setup enables customers to try and benchmark solutions before purchasing infrastructure. Where justified, we execute structured cloud migrations with security built in from the outset and deploy proprietary AI-powered tools to continuously optimise infrastructure and cloud costs and performance. Our tools also help identify root causes of tech debt arising from software architectures not designed for today's state-of-the-art infrastructure. On this modernised foundation, our AI practice delivers vertical-specific use cases across banking, healthcare, manufacturing and retail, supported by managed services, 24/7 support and quarterly roadmap reviews to prevent future debt accumulation.

Our philosophy is simple: unless an AI-based project can deliver on a CEO's KPI, it is unlikely to succeed. We help organisations focus on measurable business outcomes such as reducing costs, increasing revenue, improving market share, mitigating risks and improving CSAT. We conduct data audits, assess governance and infrastructure costs, and validate outcomes through a proof-of-value exercise to directly map results to ROI. Our cybersecurity strategy is anchored in a Zero Trust architecture with Identity Verification at its core, enabling continuous authentication, least-privilege access and context-aware security. Supported by integrated OEM solutions across ZTNA, IAM, Endpoint Security, XDR, Data Protection and Cyber Resilience, and our AI-driven capabilities, we deliver predictive threat intelligence, behavioural analytics and automated response to ensure resilience against evolving cyber threats."

## Enabling AI adoption through structured execution, ROI focus and Zero Trust security

**SANJIV KRISHEN**
**FOUNDER & CMD, IRIS GLOBAL SERVICES PVT. LTD.**

"At Iris Global Services, we see AI adoption as an execution challenge, not just a technology upgrade. Enterprises are struggling with fragmented legacy environments, siloed data, and AI pilots that fail to scale. Through IRIS 2.0, we help customers move from experimentation to structured execution. Our approach focuses on enterprise modernization through AI-ready infrastructure, cloud-native transformation, tech debt remediation, and secure data environments. Our partner-led execution model creates scalable, repeatable architectures that integrate AI securely into core business operations while reducing complexity and improving agility.

Globally, CIOs are moving from 'AI for innovation' to 'AI for measurable business outcomes.' Our conversations focus on scalability, operational efficiency, and long-term value realization. We measure ROI through faster deployment cycles, reduced infrastructure overheads, improved automation efficiency, stronger cybersecurity response, and optimized workload performance. IRIS 2.0 enables customers to move from proof-of-concept to production at scale, reducing implementation risk, accelerating adoption timelines, and creating recurring operational value.

As AI becomes mainstream, cyber threats are evolving rapidly. Enterprises are adopting Zero Trust as a foundational security architecture, and security is embedded across our execution model. We integrate Zero Trust principles through continuous authentication, identity-led access controls, endpoint protection, governance frameworks, and secure cloud deployment models. We enable organizations to adopt secure AI frameworks where governance, risk assessment, and identity verification are built into the lifecycle, ensuring proactive, scalable security."

## Transforming enterprise IT to enable AI-ready, secure and scalable infrastructure

**SAURIN SHAH,**
**MD, ASHTECH INFOTECH (INDIA) PVT. LTD.**

"We help organisations reduce technical debt and modernise legacy environments by upgrading core IT infrastructure, including servers, storage, networking, GPU-enabled compute and cloud platforms. We also support the transition from traditional monolithic systems to modular, API-driven, cloud-native architectures. In addition, we build modern data platforms such as data lakes and streaming environments that support AI training, automation and advanced analytics workloads. This creates an AI-ready ecosystem that accelerates innovation while reducing long-term operational complexity and cost across enterprise environments.

We focus on measurable outcomes that directly align with business objectives. These include reducing infrastructure costs, lowering manual effort by 20–50% in repetitive processes, improving operational efficiency, and accelerating decision-making cycles. We also measure outcomes such as improved service levels, reduced errors, quicker issue resolution and stronger data-driven decisions. These metrics help CIOs clearly quantify business value and demonstrate both immediate cost optimisation and long-term growth benefits from AI investments across the organisation.

We integrate Zero Trust principles through a 'never trust, always verify' approach by implementing identity-based access controls, multi-factor authentication, least-privilege access and continuous monitoring. Security controls are embedded across infrastructure, applications and cloud environments to ensure users and systems are continuously validated in real time. This approach strengthens resilience against evolving AI-driven cyber threats while enabling secure, scalable and compliant digital transformation across the enterprise ecosystem."

## Driving AI-ready enterprises through modernisation, outcomes and Zero Trust security

**SUHAS DESAI**
**PRESIDENT & BUSINESS HEAD – CYBERSECURITY AND MANAGED SERVICES, EMBEE SOFTWARE**

"At Embee Software, we help customers address the barriers of legacy infrastructure and fragmented data environments by focusing on modernization before AI acceleration. This includes moving workloads to cloud-native environments, modernising data architecture, consolidating siloed systems and strengthening governance frameworks. We are seeing strong demand for platforms like Microsoft Fabric and Azure AI, which help organisations unify data and build AI-ready ecosystems. The focus is not just on replacing old systems, but on creating a foundation where AI can deliver measurable business impact without increasing operational complexity.

CIO conversations around AI have become more outcome-driven, moving from experimentation to measurable impact. Today, leaders expect productivity gains, faster decision-making, reduced operational costs and improved customer experience. In workplace AI deployments such as Microsoft Copilot, we track metrics like reduction in manual effort, faster document creation and shorter response times, while analytics initiatives focus on forecasting accuracy and turnaround times. Ultimately, AI adoption is no longer about deploying tools, but about proving business value quickly and at scale.

As AI-driven threats become more sophisticated, traditional perimeter-based security models are no longer effective. At Embee Software, we embed Zero Trust principles and identity-first security frameworks across cloud, workplace, data and endpoint environments. This includes continuous identity verification and real-time threat monitoring using Microsoft Defender and Sentinel. Through our 24x7 Cyber Defense Center, we help customers move from reactive security to proactive detection and response, ensuring cybersecurity is built into the architecture from day one."

## AI accountability comes through outcomes and security

**SURESH RAMANI**
**CEO, TECHGYAN**

"We have moved from AI curiosity to AI accountability; experiments are easy, but outcomes that hold up in production are where the real work begins. Legacy is not disappearing anytime soon, and hybrid is reality. Our approach is straightforward: assess what stays, rationalise what doesn't, and make the data usable. Incremental modernisation works—lift where it's safe, refactor where it matters. However, AI will not fix broken processes; it will scale them, so the operating model has to change first to enable effective outcomes and ensure technology decisions are aligned to business decisions.

When evaluating AI, we do not talk features; we focus on outcomes and where impact will be seen. Typically, it starts small—faster service response, reduced manual effort, and better-qualified sales conversations. Nothing is dramatic overnight, but consistent improvements show up in cost-to-serve, cycle time, and employee productivity. Successful AI adoption is about proving business value quickly and at scale.

On risk, AI increases exposure, but the answer is not more tools; it is stronger identity. Identity is now the control plane as we move to MFA or passwordless, enforce least privilege, segment access, and continuously verify. We assume breach, monitor behaviour, and prepare response playbooks. Security is not a layer anymore; it is part of the design. Ultimately, if AI does not deliver outcomes, stop it; if it isn't secure, don't start it."

## Cutting tech debt, delivering AI outcomes and strengthening Zero Trust security

**TUSHAR PAREKH**
**MANAGING DIRECTOR, SILICON NETSECURE PVT LTD**

"One of our key priorities has been helping clients simplify and modernise their existing IT environments before adopting advanced AI solutions. Many organisations still operate on fragmented legacy systems that create operational inefficiencies and security gaps. We work closely with customers to assess their infrastructure, consolidate workloads, migrate critical applications to scalable cloud platforms and automate repetitive processes. This approach helps reduce long-term 'tech debt' while creating a more agile and AI-ready ecosystem without disrupting ongoing business operations.

Today's CIOs are extremely focused on measurable outcomes rather than technology experimentation. Our AI engagements are therefore aligned with clear business KPIs such as faster response times, reduction in manual effort, improved customer experience, higher operational efficiency and lower infrastructure costs. In several deployments, AI-led automation has helped reduce turnaround times and improve productivity across support and operations teams. By focusing on tangible business impact, we help customers view AI as a strategic investment rather than just an emerging technology trend.

With cyber threats becoming increasingly AI-driven, security can no longer be treated as a separate layer. We safeguard customers' networks from external and internal threats by integrating Zero Trust principles and strong Identity Verification frameworks directly into our core solutions. This includes multi-factor authentication, least-privilege access, continuous monitoring, endpoint security and AI-powered threat detection capabilities. Our focus is on building secure-by-design environments where users, devices and applications are continuously validated before access is granted, helping customers strengthen resilience while maintaining compliance and business continuity."

## Bridging legacy systems with AI, measurable outcomes and security

**VISHAL VASU**
**DIRECTOR & CTO, DEV INFORMATION TECHNOLOGY LTD**

"At Dev Information Technology Ltd (DEV IT), we act as strategic partners using our ABCD of Innovation (Artificial Intelligence, Blockchain, Cybersecurity, Datacenters) as a practical roadmap to help clients grow and stay resilient in an AI-first world. We believe the role of a technology partner today goes beyond supplying hardware and requires a focus on building real business value.

To help clients reduce tech debt and modernise legacy systems for advanced AI adoption, we avoid risky 'rip and replace' or 'lift and shift' projects. Instead, we deploy smart, AI-driven layers that sit on top of existing systems. This allows us to extract valuable insights from years of trapped data without tearing down the foundation. We help legacy systems 'speak' modern AI, enabling clients to gain the benefits of new technology without a full overhaul while avoiding business disruption.

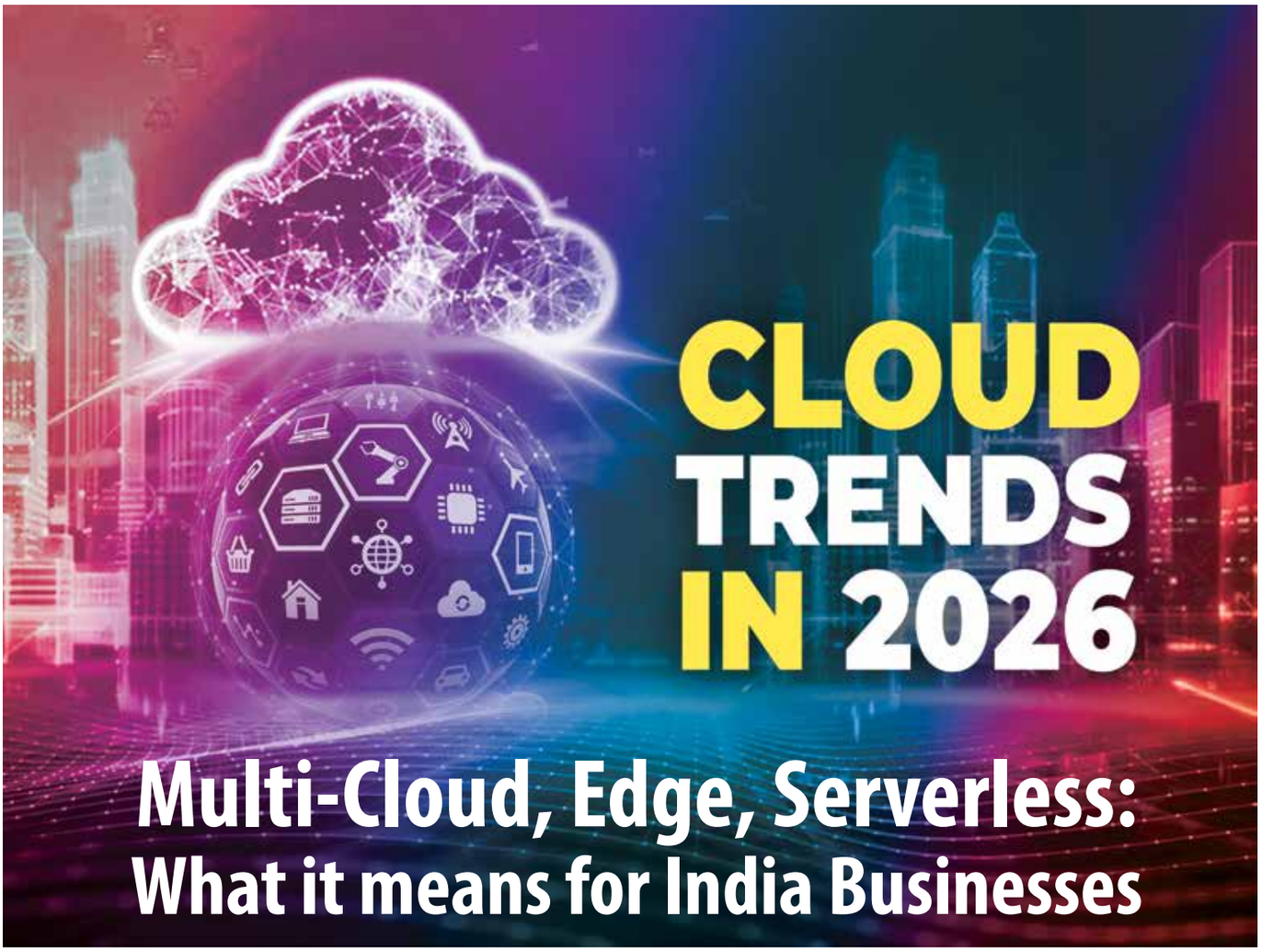
We know CIOs are focused on the bottom line, so we focus on measurable business outcomes. We track how many hours of manual work are automated, how much faster incidents are resolved, and how much the business can grow without adding headcount. We position AI as a means of creating new value. On security, we operate under the assumption that a breach is always a possibility and build security into everything we do from the ground up. We use phishing-resistant, context-aware identity verification, apply least-privilege access for both humans and AI agents, and use SIEM to monitor and validate activity in real time."

## RAH Infotech partners with Ethernexion to deliver high-performance networking solutions in India

RAH Infotech has announced a strategic partnership with Ethernexion, a global provider of high-performance networking solutions, under which it will serve as the company's authorized Value-Added Distributor (VAD) in India. The collaboration marks a significant step in Ethernexion's expansion into the Indian market and comes at a time when enterprises are accelerating investments in cloud computing, artificial intelligence (AI), and hyperscale data centre infrastructure. The partnership aims to support India's rapidly growing digital economy by providing access to advanced networking technologies designed for scalability, performance and resilience.

Through the alliance, enterprises and service providers across India will gain access to Ethernexion's portfolio of networking solutions, including network switches ranging from 1G to 800G. The offerings are designed to support a wide range of environments, including enterprise networks, campus deployments, telecom edge infrastructure and hyperscale data centres. Backed by RAH Infotech's extensive channel ecosystem and local expertise, the partnership is expected to simplify technology adoption, strengthen deployment capabilities and provide enhanced support to customers implementing next-generation network architectures.

Ashok Kumar, Managing Director and Founder of RAH Infotech, said modern businesses increasingly view networking as a strategic asset as they scale across hybrid cloud environments and support AI-driven workloads. Abdul Rahman, Managing Director of Ethernexion Singapore, described India as a key growth market and said the partnership would help bring the company's technologies closer to customers through a trusted local ecosystem. The collaboration further strengthens RAH Infotech's networking portfolio while supporting India's broader digital infrastructure and connectivity ambitions.




# Multi-Cloud, Edge, Serverless: What it means for India Businesses

In 2026, cloud computing has evolved from a storage utility into the distributed nervous system of the modern enterprise. For Indian businesses, the trend is shifting toward Sovereign Multi-Cloud and Edge intelligence, moving processing power closer to the user to meet localization demands and latency requirements. As Serverless architectures become the standard for scaling AI-driven applications, the focus has moved from simple migration to optimising for technological resilience. Navigating this complex, decentralised environment is now a boardroom priority, as digital agility becomes the primary differentiator in a hyper-competitive global market.

Enterprises are increasingly prioritizing agility, scalability, cost optimization, and real-time data processing, driving the rapid adoption of serverless architectures, multi-cloud strategies, and edge computing. Together, these technologies are reshaping how organizations build, deploy, and manage digital services.

**MODERN BUSINESSES FACE SEVERAL CHALLENGES:**

- Agility: Quickly launch new features and respond to market changes.
- Scalability: Handle growth in users and workloads without performance issues.
- Cost optimization: Reduce infrastructure and operational expenses.
- Real-time data processing: Analyze and act on data immediately rather than waiting for batch processing.

To meet these goals, organizations are increasingly adopting serverless architectures, multi-cloud strategies, and edge computing.

**HOW THESE TECHNOLOGIES WORK TOGETHER?**

Imagine a food delivery app:

- Edge computing processes customer location data near the user for instant route updates.
- Serverless functions calculate delivery fees and process orders automatically.
- Multi-cloud infrastructure distributes services across different cloud providers for resilience and flexibility.

This combination delivers - Faster user experiences, Lower operating costs, Better reliability and Easier scaling during peak demand.

As a result, enterprises can innovate more quickly, support millions of users efficiently, and deliver real-time digital experiences. These technologies are becoming foundational components of modern cloud-native architectures.

# Edge Computing, Sovereign Cloud and Serverless AI Reshaping Enterprise IT


**NEELAKANTAN VENKATARAMAN**
**VICE PRESIDENT AND GLOBAL HEAD – CLOUD, AI AND EDGE COMPUTING BUSINESS, TATA COMMUNICATIONS**


## LEVERAGING EDGE COMPUTING

For Tata Communications, we see edge computing as a critical, underlying piece of infrastructure for the next phase of digital transformation as more enterprises build on AI-based technologies that require intensive amounts of data and operate in real-time.

Industries such as manufacturing, retail, healthcare, mobility, and agriculture are increasingly leveraging edge capabilities to make faster, real-time decisions. For instance, manufacturers can monitor and optimise production lines instantly, retailers can enable intelligent in-store experiences, while healthcare providers can process sensitive patient data locally for faster diagnostics and improved data privacy. Overall, this is enabling Indian enterprises to unlock new operational efficiencies, improve customer experiences, and build resilience into their digital operations, acting as key differentiators in an increasingly competitive market.

## BALANCING CLOUD AGILITY WITH SOVEREIGN DATA COMPLIANCE

Tata Communications Vayu platform is sovereign by design. So, there is no customer data, metering or telemetry leaving India. Although we allow customers the benefit of a multi-cloud strategy with our IZO+ Multi Cloud Network, we strictly adhere to local law and jurisdiction. Tata Communications' Vayu Cloud has been designed in compliance with all the regulations set forth by the relevant regulatory authorities in India. We provide a balance between supporting a (hybrid) cloud model and allowing enterprises to easily migrate their workloads from one environment to another (primarily based on the number of workloads) while also providing them with the ability to manage complex IT landscapes through a "single-pane-of-glass" orchestration layer while providing and having the confidence that they will always be operating on a safe, sovereign foundation. This becomes especially important for Indian businesses navigating evolving regulatory frameworks while scaling globally.

## ACCELERATING AI ADOPTION THROUGH SERVERLESS INFRASTRUCTURE

Transitioning to an AI-as-a-Service model based on business outcomes rather than infrastructure ownership. The serverless option automatically allocates and bills for GPU use, making the user's IT costs from owning hardware into a variable expense (rather than fixed) by eliminating high costs in owning hardware. The Tata Communications AI Studio's fractional GPU allocation also helps startups and researchers pay only for the amount of compute they will use for their experiments. This is particularly impactful for Indian businesses, as it lowers the barrier to entry for advanced AI adoption while improving cost predictability.

The combination of these changes with predictable usage-based pricing has led to our customers experiencing an average 30% reduction in Total Cost of Ownership (TCO) and 60% customers confirm cost-effective cloud solutions.

## IBM aligning its cloud strategy with a hybrid-by-design approach

### RAVI JAIN
**VICE PRESIDENT, SYSTEMS & CLOUD SALES, IBM INDIA & SOUTH ASIA**

**BUILDING A UNIFIED, COHESIVE ECOSYSTEM**

"For enterprises in India, the conversation around multi-cloud has moved well beyond flexibility. It is now about designing intelligently and deliberately for control, compliance, and scale together. What we consistently see is that organizations do not need to choose between innovation and regulatory alignment. They need an architecture that enables both by default. This balance is achieved through a hybrid-by-design approach, where cloud is not an afterthought but a foundational design principle. It enables enterprises to determine workload placement based on sensitivity, compliance obligations, latency, and business criticality, ensuring that data and systems requiring residency in India remains securely within jurisdictional boundaries, while still leveraging public cloud for innovation and scalability. It also ensures flexibility over time throughout the entire workload lifecycle, moving them around on-premises or on cloud depending on business needs.

**ENABLING DIGITAL SOVEREIGNTY**

IBM is enabling this at scale through our portfolio of hybrid cloud and AI solutions. Clients can build portable, containerized workloads and run them consistently across environments, avoiding lock-in while improving resilience. We recently launched IBM Sovereign Core that helps enterprises deploy and operate AI-ready sovereign environments with full control over data, operations and governance. With such solutions, digital sovereignty is not a constraint on innovation or growth, rather helps scale tech deployments responsibly and in alignment with India's evolving regulatory landscape."

## Helping businesses balance flexibility and data sovereignty over architecture choices

### PRAVAL SINGH
**VP MARKETING AND CUSTOMER EXPERIENCE, ZOHO**

"Balancing flexibility and data sovereignty is one of the most important conversations Indian enterprises are having today. As businesses navigate sovereign multi-cloud, edge intelligence, and serverless architectures, the ability to operate across complex, decentralized environments while maintaining control over data has become a critical business priority.

At Zoho, we address this through a unified, full-stack platform spanning over 60 products, all built in-house on infrastructure we own and operate. Our customers get the breadth, scalability, and capability they need without depending on a fragmented mix of third-party vendors. Our approach covers architecture, interoperability, cost optimisation, and data security, in close collaboration with customer teams, giving enterprises the resilience to move fast without compromising on governance or control.

However, for enterprises that do need third-party services, our robust APIs and native integrations make that possible without compromising on governance or security.

Privacy is not a compliance requirement for us. It is a core belief. When customers bring Zoho into their environment, data privacy, backup, and API connectivity come built in. This means significantly less pressure on IT and security teams, and the confidence to operate without second-guessing data governance. On data residency, for customers on our India data centre, all data is hosted in India in line with data residency requirements. Zoho runs 18 data centres globally, including two in India, giving customers a clear choice of where their data resides. As localisation demands and regulatory expectations grow, that choice backed by infrastructure we fully own and operate is what makes digital agility sustainable."

## Edge Computing for Zoho is the foundation for reliable industrial operations

### JEGAN RAGHAVAN
**GLOBAL PRODUCT HEAD, ZOHO IOT**

"Edge Computing, for us, is the foundation for reliable industrial operations across India's highly diverse connectivity landscape. Many of the manufacturing facilities we work with operate in remote regions where unstable internet, network congestion, or complete connectivity outages are common. A setup that is overly dependent on the cloud, risks production disruptions every time the connectivity drops, leading to operational delays and financial impact.

We developed our proprietary Edge Agent to ensure operations continue uninterrupted even when the cloud is temporarily unreachable. Shop floors usually consist of multiple machines communicating through different industrial protocols, and the Edge Agent is designed to support a wide range of these protocols, allowing it to collect data from different types of machines easily and send everything to the cloud. When connectivity is interrupted, the Edge layer locally collects, processes, and stores machine and operational data, while critical workflows such as alerts, downtime monitoring, rule execution, and device actions continue to function normally.

Once connectivity is restored, the data seamlessly syncs back to the cloud for centralized analytics, reporting, and long-term intelligence. This architecture has enabled us to achieve edge-level data acquisition at intervals as low as 150 milliseconds, helping manufacturers detect production anomalies and quality issues in near real time while maintaining operational resilience and uptime."

# Advancing sovereign infrastructure built for AI-native environments

**PIYUSH PRAKASHCHANDRA SOMANI**
**PROMOTER, MANAGING DIRECTOR AND CHAIRMAN, ESDS**

To keep pace with the evolving cloud tends, ESDS is focused on architectural reinvention. Our flagship platform, the world's first Autonomous Hyperscaler Cloud Platform will be launched soon. SPOCHub, our GPU subsidiary, has contracted 8,208 NVIDIA B300 GPUs for delivery by September 2026, making ESDS the first sovereign operator of Blackwell-class compute in India. Our datacentres are strategically located in six locations: Nashik, Airoli, Bengaluru, Mohali, Noida, and Kolkata.

## EXPANDING CLOUD CAPABILITIES

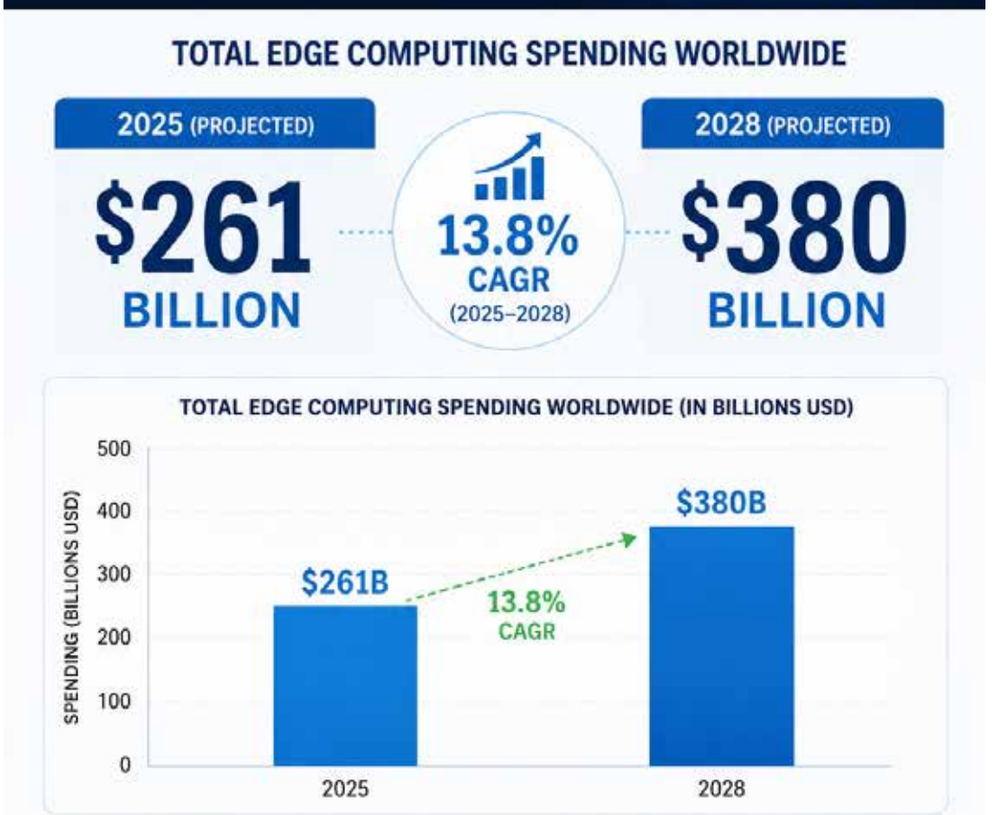
ESDS is executing a three-pillar growth strategy anchored on GPU infrastructure, community cloud specialisation, and geographic expansion. ESDS is building the sovereign, AI-native infrastructure on which that value runs. Our Banking Community Cloud serves 450+ clients; Smart City Cloud hosts 80% of India's operational smart cities; and our DC network scales to 125 MW across 11 facilities. India's digital economy will generate USD 1 trillion by 2030.

## ACCELERATING INNOVATION & DIGITAL TRANSFORMATION

The India sovereign Cloud market is expected to grow at a CAGR of 27.9% and is expected to reach a value of 21.1 billion dollars by the year 2033, as per data by Grand View Research report. Looking ahead, India's DPDPA, RBI's Cloud Framework, and MeitY's policy would mandate data residency and explainable AI, which are unique advantages of sovereign-cloud native providers like ESDS.

ESDS achieves measurable AI-Cloud outcomes in diverse sectors: Banking customers experience 65% improved fraud detection and 40% reduced opex; Smart Cities deployments reduce incident response times by 55%; Manufacturing customers experience 48% reduced downtime and 70% faster ERP performance; Healthcare customers enjoy 60% faster diagnostics; and Retail customers experience 22% more revenue per visitor.

**THE GLOBAL EDGE COMPUTING MARKET SIZE WAS ESTIMATED AT USD 23.65 BILLION IN 2024 AND IS EXPECTED TO REACH USD 327.79 BILLION IN 2033, GROWING AT A CAGR OF 33.0% FROM 2025 TO 2033, ACCORDING TO GRANDVIEW RESEARCH.**

## From Edge to Orbit: Building Sovereign AI Infrastructure

**VIJAYAKUMAR ARUMUGA NADAR,**
**CHIEF AI OFFICER, RACKBANK AND NEEVCLOUD**

### LEVERAGING EDGE COMPUTING

India is a continent-scale market with remarkable diversity in connectivity, geography, and user density and our edge computing strategy at RackBank and NeevCloud is purpose-built to serve that scale. We have established terrestrial AI data centres at strategic inland nodes; Indore, Raipur, ensuring compute is genuinely close to where India's enterprises and users operate every day.

We have also taken this vision further with Project Orion, our Orbital Real-Time Inferencing Network, which places high-performance AI inference nodes directly into Low Earth Orbit at altitudes between 350+ and 1,200 km. This constellation is engineered to deliver a global latency of under ~10 to 15 ms, covering ~98% of Earth's surface with multiple Edge orbital nodes. A single REST API intelligently auto-routes inferencing requests to the nearest orbital or terrestrial edge node, making the entire experience seamless for developers.

### BALANCING CLOUD AGILITY WITH SOVEREIGN DATA COMPLIANCE

At NeevCloud, we have built a Sovereign Multi-Cloud architecture where data sovereignty is the foundation and multi-cloud flexibility is the natural advantage built on top of it. This approach gives Indian enterprises the best of both worlds; the freedom to choose best-in-class tools across cloud ecosystems while keeping all sensitive data firmly within Indian jurisdiction, by architecture.

### ACCELERATING AI ADOPTION THROUGH SERVERLESS INFRASTRUCTURE

Serverless represents a powerful rethinking of the relationship between IT investment and business value and at NeevCloud, our infrastructure philosophy is built around exactly this principle through our pay-per-inference model with value outcome.

For Indian enterprises, where capital discipline is a core organizational strength; this approach transforms the technology investment conversation at the leadership level. It shifts the focus from infrastructure provisioning to business outcomes, empowering teams to ship faster, experiment with greater confidence, and optimize continuously with clear and immediate cost signals.

Enterprises looking for cloud environments that are sovereign, interoperable and economically sustainable at scale

## Designing Sovereign Cloud Without Compromising Flexibility and Sustainability

**JEFF LEE**
**PARTNER PROGRAM MANAGER, OVHCLOUD**

### BALANCING CLOUD AGILITY WITH SOVEREIGN DATA COMPLIANCE

Many enterprises assume they must choose between multi-cloud flexibility and data residency compliance. In practice, the market is moving toward architectures that can deliver both.

With the Digital Personal Data Protection (DPDP) Act, 2023, data residency is no longer just a regulatory checkbox. Enterprises are rethinking where critical workloads sit, who controls them, and how easily infrastructure can adapt over time without creating lock-ins.

Our Mumbai data centre provides a local foundation for sensitive workloads and customer data to remain within Indian jurisdiction. At the same time, because our architecture is built on open technologies like OpenStack and Kubernetes, customers retain the ability to move workloads across private, public, and edge environments without rebuilding applications each time. Through our local presence and open technologies, we are positioning our partners at a distinct advantage – where they can deliver ready-compliance architecture for their customers to meet stringent regional requirements.

What Indian enterprises increasingly want is compliance designed into the architecture from day one, not added later as an afterthought. They are looking for cloud environments that are sovereign, interoperable and economically sustainable at scale.

## Building Intelligent Cloud Foundations for Enterprise Scale

**GURU KANDASAMY**
**VICE PRESIDENT OF TECHNOLOGY, ILINK DIGITAL**

### LEVERAGING EDGE COMPUTING

We are helping customers build distributed architectures using cloud native platforms, custom edge server deployments and intelligent automation to process workloads closer to the source. This is especially relevant across manufacturing, healthcare and retail environments where response times directly impact operations and customer experience. In several use cases, edge enabled processing has helped reduce response times from minutes to near real time decision making.

The focus today is not only on performance, but on building resilient and always available digital ecosystems that can scale efficiently across regions.

### BALANCING CLOUD AGILITY WITH SOVEREIGN DATA COMPLIANCE

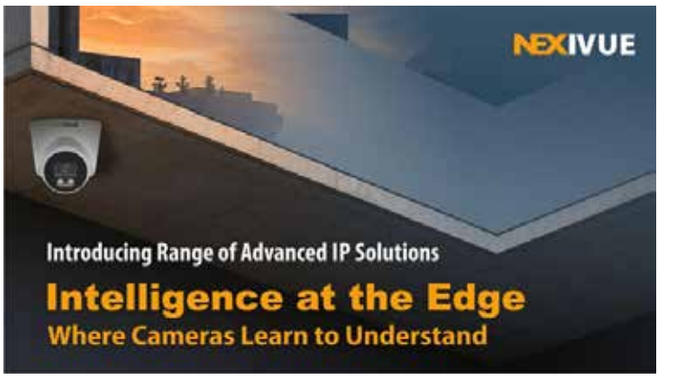
Indian enterprises are increasingly looking for the flexibility of multi cloud environments while maintaining strong control over governance, compliance and sensitive data. At iLink Digital, our approach focuses on building governance-led cloud ecosystems that provide visibility, policy enforcement and security consistently across platforms.

Rather than managing each cloud environment in isolation, we help organisations create a unified governance layer across multi cloud and hybrid infrastructures. This allows enterprises to maintain workload portability and operational agility while ensuring regulated data remains aligned with residency and compliance expectations.

# Aditya Infotech Unveils 'NEXIVUE' – Expanding the Horizons of Bharat's Surveillance Future

In a strategic move poised to redefine accessibility and market reach in the surveillance industry, Aditya Infotech Limited, the force behind India's leading surveillance brand CP PLUS, has officially launched NEXIVUE, a new surveillance brand aimed at expanding accessibility and market reach across India's rapidly evolving security ecosystem.

The launch marks a major step in the company's multi-brand strategy as it looks to address diverse market segments while maintaining the premium positioning of CP PLUS. According to the company, NEXIVUE has been designed to cater to deeper distribution channels and city-exclusive business models, particularly across Tier II, Tier III, and rural markets.




## FOCUS ON AFFORDABLE AND INTELLIGENT SURVEILLANCE

The launch comes at a time when demand for intelligent yet affordable surveillance solutions is increasing across the country. From smart cities and enterprises to small businesses and residential communities, the need for reliable security technologies has grown significantly. NEXIVUE aims to bridge this gap through technologically advanced and value-driven surveillance offerings designed for widespread adoption.

The brand's initial portfolio is expected to include smart IP cameras ranging from 2MP to 4MP resolutions, dual-light technology, weatherproof designs, AI-enabled smart features, intelligent recording systems, and high-efficiency encoding technologies. The ecosystem is also likely to feature advanced NVR solutions supporting up to 4K recording capabilities and scalable storage configurations.

## STRENGTHENING DISTRIBUTION AND REGIONAL EXPANSION

Aditya Infotech said the new brand has been conceptualized to empower channel partners and strengthen distribution-led growth by enabling deeper market penetration and regional exclusivity opportunities. The company believes this approach will further expand its nationwide presence while creating stronger business opportunities for regional partners.

The launch also reflects Aditya Infotech's broader focus on manufacturing expansion, localization initiatives, AI-driven innovation, and strengthening its distribution network. Industry observers believe the company's multi-brand strategy could accelerate market expansion amid rising demand for trusted and compliant Indian surveillance technologies.

Backed by Aditya Infotech's manufacturing ecosystem and partner network, NEXIVUE is expected to play a significant role in expanding access to intelligent and future-ready surveillance solutions across Bharat.

## Redington partners with Vehere to expand AI-powered cybersecurity offerings in India

Redington has announced a strategic partnership with Vehere, an AI-powered Network Detection and Response (NDR) solutions provider, under which it will serve as Vehere's official distributor in India. The alliance is expected to strengthen Redington's cybersecurity portfolio while expanding access to Vehere's threat detection and response capabilities for organizations across the country.

The partnership comes as enterprises increasingly operate across hybrid IT environments that combine on-premises infrastructure, cloud platforms, remote endpoints, and connected devices. This growing complexity has created new security challenges and increased the need for continuous monitoring and rapid threat detection. Vehere's AI-powered NDR platform is designed to identify and respond to threats such as ransomware, advanced persistent threats (APTs), insider attacks, lateral movement, and zero-day exploits in real time.

Through Redington's extensive partner ecosystem and market reach, Vehere aims to accelerate adoption of its cybersecurity solutions among enterprise, government, and mid-market customers. Redington will also support deployment and post-sales services, helping partners deliver advanced security capabilities across diverse IT environments.

Sridhar S, Executive Vice President at Redington, said the addition of Vehere's NDR platform enhances the company's cybersecurity portfolio and supports partners in addressing evolving cyber risks. Sanjay Bhardwaj, MD India and SAARC at Vehere, said Redington's channel relationships and nationwide reach would help accelerate the company's growth in India. The collaboration is expected to create new opportunities for channel partners and system integrators to deliver advanced cybersecurity solutions.

## Pantum teams up with Vishal Peripherals to expand market presence in India

Pantum has entered into a strategic partnership with Vishal Peripherals to expand the reach of its printing solutions across India through both online and offline channels. The collaboration is aimed at improving product accessibility, strengthening retail visibility, and enhancing customer support as Pantum seeks to accelerate growth in the Indian market.

Under the partnership, Vishal Peripherals will become an authorized online sales partner featured on Pantum India's website. Customers will be able to purchase Pantum printers and consumables through Vishal Peripherals' retail network, website, and mobile application. The alliance will also support Pantum's retail expansion across Hyderabad and other South Indian markets, improving product availability and after-sales service for consumers, small businesses, and enterprise customers.

Nitish, Country Manager, Pantum India, said the partnership aligns with the company's 2026 growth strategy and will help make its printing solutions more accessible across the country. Vikash Hisariya, Managing Director of Vishal Peripherals, said the association strengthens the company's ability to offer a wider range of technology and printing products backed by customer support and service.

Pantum also outlined plans to expand its A4 monochrome laser printer portfolio in 2026 with faster, more secure multifunction devices featuring enhanced connectivity and mobile printing capabilities. The company expects to introduce select "Make in India" models by year-end. Both companies will jointly drive retail expansion, partner training, digital marketing initiatives, and regional technology events to increase market reach and customer engagement.


# Elcom Digital Brings AI, Partnerships and Growth Focus to Synergy 2026

Elcom Digital hosted Synergy 2026 on May 8 and 9 at Indana Palace, Jaipur, bringing together vendors, partners and industry leaders to discuss AI-led transformation, operational agility, ecosystem collaboration and future-ready distribution strategies. On the sidelines of the summit, VARINDIA spoke with Elcom leadership and industry experts about innovations, partnerships, market trends and the evolving technology distribution landscape.

## SUNIL NARANG, DIRECTOR, ELCOM TRADING

"Synergy has evolved from an internal engagement initiative into a broader ecosystem platform that now brings together teams, vendors and industry stakeholders. With the market moving beyond pure hardware distribution, we are strengthening our focus on cloud, AI, backup and storage solutions, while continuing to expand our core hardware distribution business."

## SAGAR NARANG, CEO, ELCOM DIGITAL

"Synergy 2026 reflects how AI, rapid innovation and evolving market challenges are reshaping the industry. AI is no longer the future, it is the present, and we are already integrating it across our business. Our partner ecosystem remains central to our growth strategy as we focus on strengthening distribution, expanding SaaS offerings and building our own products."

## HARISH KUMAR G., DIRECTOR - BUSINESS DEVELOPMENT, VTIGER CRM

"AI and cloud technologies are reshaping how businesses engage with customers, making channel partners more important than ever. Our collaboration with Elcom Digital creates strong opportunities to combine software, hardware and local market expertise to deliver more relevant business solutions. With our upcoming AI-driven platform, we are excited to strengthen partner-led growth across markets."

## VISHESH GARG, CHANNEL SALES MANAGER, TSPLUS INDIA

"Synergy 2026 provides a strong platform for vendors, partners and distributors to collaborate, exchange ideas and build a stronger technology ecosystem. With AI, cloud and data center adoption accelerating in India, channel partnerships are becoming increasingly important in delivering flexible and affordable solutions. Elcom's extensive partner network also creates significant opportunities for market expansion and ecosystem growth."

## SOMESH NARANG, DIRECTOR, ELCOM TRADING

"Synergy 2026 focused not just on business numbers, but on growing together as an ecosystem. Over the years, the platform has evolved into a space for leadership development, partner collaboration and long-term vision building. With nearly 5,000 partners across the country, our focus remains on becoming a value-added partner delivering integrated hardware and software solutions through Elcom Digital."

## KUMAR TANKSALE, REGIONAL SALES HEAD – NORTH, LENOVO INDIA

"Synergy 2026 reflects how the industry is moving beyond pure hardware selling toward integrated hardware and software solutions. Events like these strengthen ecosystem collaboration through knowledge sharing and strategic discussions. Elcom Digital's growing focus on technology-led execution, combined with strong leadership and fresh energy, creates significant opportunities for long-term vendor partnerships and future growth."

## VARUN SETH, CEO, MATISOFT CYBER SECURITY LABS

"AI-driven cybersecurity is becoming increasingly critical as businesses face rising threats related to malware and data leaks. Our collaboration with Elcom combines deep technology expertise with strong go-to-market capabilities, creating significant growth opportunities. Events like Synergy 2026 also provide valuable market feedback that helps us build solutions aligned with customer and industry requirements."

## ASHUTOSH SHARMA, BUSINESS HEAD, SPENTRO – GYFTR LIMITED

"Events like Synergy 2026 create strong opportunities for ecosystem collaboration by bringing partners together to exchange ideas, explore new market opportunities and build stronger go-to-market strategies. As AI and cloud technologies evolve, partner networks become even more critical in driving innovation, expanding market reach and delivering greater business value across the ecosystem."

# Hikvision India Launches Intelligent Electric Lock Series for Smart Home Security

Hikvision India has introduced its Intelligent Electric Lock Series, a next-generation smart home solution designed for residential, commercial, and SME applications. The launch strengthens the company's Smart Home portfolio under the Non-CCTV product category.

The Hikvision DS-K4E100 is part of the Pro Series Intelligent Electric Motor Lock range developed for high-security applications such as residential buildings and commercial offices. One of its key highlights is its universal installation design, which allows it to be installed on left-opening, right-opening, interior, and exterior doors without requiring separate configurations for different door directions.

## SMART SECURITY AND REMOTE ACCESS FEATURES

The Hikvision Intelligent Lock Solution combines security, convenience, and remote management capabilities for homes and businesses. It supports multiple unlocking methods, including fingerprint, PIN, RFID card, mobile app, mechanical key, and remote OTP access for keyless entry.

"Today, security is all about intelligence and technology savvy solution, not just locks. With our new Intelligent Electric Lock Series, we're giving Indian homes and businesses a smarter, safer way to control access. It integrates seamlessly with Hikvision cameras, alarms, and video door phones to create a unified security ecosystem," said Bhupendra Kumar, Assistant Vice President, Video Door Phone (VDP), Prama Hikvision India Private Limited.

## ENHANCED SECURITY AND INTEGRATION CAPABILITIES

The lock features AI-powered fingerprint recognition with a reported unlocking speed of 0.3 seconds and a false acceptance rate of less than 0.001 percent. Through the Hik-Connect App, users can remotely lock or unlock doors, access logs, and share temporary PINs.

Additional features include a C-grade lock cylinder, tamper alarms, break-in alerts, anti-peep PIN technology, and auto-locking after nine seconds if no entry is detected. The product also carries an IP65 weather-resistant rating for outdoor gates and main doors.

The DS-K4E100 supports wooden, metal, and PVC doors and offers stainless steel construction with a life expectancy of more than 500,000 operations. It is also designed to integrate with Hikvision video intercom systems and access control terminals for real-time lock status detection. The product is now available in India through Hikvision's nationwide partner network.

---

# CADYCE Expands Connectivity Portfolio with New USB-C and USB to Serial Converters

CADYCE, a leading brand in computer accessories and connectivity solutions, has announced the launch of its latest range of USB-C to Serial and USB to Serial Converters aimed at enabling seamless connectivity between modern computing systems and legacy serial devices.

The latest lineup includes the CA-CS9 (3M) USB-C to Serial (RS-232) Converter, CA-CS9 (5M) USB-C to Serial (RS-232) Converter, and the CA-US9 (5M) USB to Serial (RS-232) Converter.

The company said the new products are designed to address the growing demand for integrating modern laptops and desktops with older industrial and communication equipment that still rely on RS-232 connectivity.


## DESIGNED FOR MODERN-TO-LEGACY INTEGRATION

According to CADYCE, the converters act as a reliable communication bridge between USB or USB-C enabled systems and legacy serial devices, helping ensure stable and efficient data transmission across platforms.

The products are available in extended cable lengths of 3 metres and 5 metres, allowing greater flexibility in deployment across different work environments. The company added that the converters are suitable for industrial applications, networking setups, point-of-sale systems, and automation environments where serial communication remains essential.

The converters also support easy installation and are bundled with drivers and user manuals to simplify deployment for professional users.

## FOCUS ON RELIABLE CONNECTIVITY SOLUTIONS

CADYCE stated that the new range has been developed for businesses and professionals who continue to depend on legacy serial infrastructure while adopting the latest computing platforms.

"With this launch, we continue our commitment to delivering practical and future-ready connectivity solutions. These converters ensure that businesses can operate without limitations, even when working with legacy infrastructure," a CADYCE spokesperson said.

The company believes the launch will help organisations maintain compatibility between older hardware systems and newer devices without requiring major infrastructure changes. The newly launched converters are now available through CADYCE's authorised partners and distribution network.

# The 12-Hour Clock

*CERT-In's new AI threat advisory sets patching expectations in hours, not weeks. The operating model it demands runs straight through the channel — and previews where global standards are heading.*

For most of the last two decades, vulnerability management in Indian enterprises ran on a comfortable rhythm. A vendor disclosed a flaw, the security team assessed severity, the change-advisory board met, and somewhere between two weeks and two months later the fix went in. The cadence felt aggressive because it was, against the threats it was designed for. Attackers worked at human speed. Weaponisation took weeks. Defenders on a monthly cycle were not catching up, but they were not falling decisively behind either.

That model is now formally obsolete in India.

On May 25, the Indian Computer Emergency Response Team (CERT-In) issued a 38-page advisory titled "Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure." Section nine contains a remediation table that represents the most significant change in Indian enterprise security expectations in years. It tells organisations to patch, mitigate, or remove known exploited vulnerabilities on internet-facing and crown-jewel systems within 12 hours where feasible. Critical externally exposed vulnerabilities get one day. A known exploited vulnerability on internal systems also carries a one-day expectation "unless compensating controls are implemented and documented." Critical internal vulnerabilities get three days. High-severity vulnerabilities get five.

These are advisory expectations, not statutory deadlines. But anyone watching Indian cyber regulation evolve since the 2022 six-hour incident reporting directive knows the trajectory: today's advisory expectation is tomorrow's audit question, and the year after that, the regulatory floor.

The rationale CERT-In offered is direct. "AI-assisted cyber exploitation reduces the time required for adversaries to identify, weaponize, and exploit vulnerabilities, exposed services, weak identities, insecure APIs, and misconfigured systems," it said. The agency described threat actors using AI to automate attack surface discovery, vulnerability analysis, exploit chaining, and malicious code generation. The tooling, it warned, can let "even non-expert / semi-skilled / untrained threat actors to launch sophisticated cyber-attacks at scale." Agentic AI raises the prospect of "automated multi-stage cyber operations involving reconnaissance, exploitation, persistence, lateral movement, and data exfiltration."

The asymmetry is the point. If attackers are compressing their kill chains from weeks to hours using AI, defenders running monthly cycles are no longer slow. They are structurally exposed.

## READING THE TIERS HONESTLY

The 12-hour figure is the line that will dominate coverage, and it is also the line most likely to be misread. The advisory does not demand 12-hour patching across the estate. It reserves that window for containment on internet-facing and crown-jewel systems where exploitability is already visible, then steps the obligation outwards in proportion to exposure.

That distinction is not cosmetic, said Sanchit Vir Gogia, chief analyst at Greyhound Research. The 12-hour figure covers containment on a narrow set of exposed assets, not patching across the estate. The five-day window for high-severity vulnerabilities is comfortable for most enterprises. The pressure point sits in the middle of the table. The three-day window for critical internal systems is where the pressure bites, Gogia said, because internal fixes trigger change-board friction in finance, telecom, healthcare, and OT-heavy estates where uptime sensitivity governs every decision.

For enterprises still running weekly or monthly patch cycles, the expectation forces a change in operating model, not just speed. The barriers are operational rather than technical. Most Indian organisations lack real-time asset visibility, automated prioritisation,

**CERT-IN REMEDIATION EXPECTATIONS BY TIER**
**ADVISORY ISSUED MAY 25, 2026. WINDOWS APPLY WHERE FEASIBLE.**

| | |
|---|---|
| 12 hours Containment | KNOWN EXPLOITED VULNERABILITY<br>Internet-facing and crown-jewel systems |
| 1 day | CRITICAL EXTERNALLY EXPOSED VULNERABILITY<br>Plus internal KEV unless compensating controls documented |
| 3 days | CRITICAL INTERNAL VULNERABILITY<br>High-value systems |
| 5 days | HIGH-SEVERITY VULNERABILITY<br>Based on risk prioritisation |

**No patch available: apply isolation, access restriction, WAF/API protection, enhanced monitoring, or feature disablement.**

and cross-functional response playbooks — the very capabilities the advisory now assumes as baseline.

Both the agency's framing and Gogia's reading converge on one diagnosis. The bottleneck is not patch deployment. It is visibility. Teams lose their first hours establishing whether the vulnerable asset even exists, who owns it, what it connects to, and whether isolating it breaks something else. "They are fighting organisational latency, not technical weakness," Gogia said.

## THE CONTAINMENT SHIFT

The most strategically important move in the advisory is not the clock itself but what CERT-In allows in lieu of patching. The remediation table leans heavily on compensating controls and temporary mitigations. Organisations can fall back on documented controls for internal systems. Where no patch exists, they can apply "isolation, access restriction, WAF/API protection, enhanced monitoring, or feature disablement until remediation becomes available."

On the surface, that reads as a softening. In practice, it is a structural reframing.

The reliance on compensating controls makes the timelines more achievable, because it acknowledges the realities of patching complex environments. But it shifts the real burden onto comprehensive asset visibility and real-time exposure management. The controls work only if an enterprise can already see the exposed asset, identify its owner in minutes, and push controls at speed, Gogia said. If a team cannot isolate, restrict, or monitor quickly, the problem was never patch cadence. The problem was that the enterprise did not know its own exposure. The advisory, he said, "pushes vulnerability management out of periodic compliance and into continuous exposure management."

That distinction is the one Indian channel partners need to understand most clearly. Vulnerability management is administrative. It measures backlog. Exposure management is operational. It measures survivability. The advisory has moved the goalposts from one to the other, and the gap between what most Indian enterprises run today and what the advisory expects is precisely the gap channel partners are about to be paid to close.

## WHERE INDIA STANDS AMONG GLOBAL FRAMEWORKS

CERT-In's clocks are among the most aggressive of any national framework. The international comparison sharpens the point. CISA's Known Exploited Vulnerabilities catalogue, the closest analogue, sets due dates per vulnerability — commonly around two weeks, compressing to roughly a day only for emergency edge-device situations, Gogia said. Europe is tightening through "without undue delay" duties and 24-hour reporting for actively exploited flaws under the Cyber Resilience Act, rather than fixed enterprise-wide remediation clocks.

The structural difference matters. "CERT-In has set standing clocks by asset category rather than deadlines by individual vulnerability," Gogia said. Western frameworks have largely avoided that.

The signal for global standards is the part worth sitting with. India is not diverging from the international direction of travel, Gogia argued. It is previewing it. The fixed-clock model looks aggressive today because the rest of the world has not caught up, not because India is reading the threat wrongly. As AI compresses exploit timelines globally, other regulators will be forced toward similar fixed-clock thinking.

For multinationals operating in India, the consequence is immediate. Internal global SLAs designed before AI altered exploit economics now sit below India's expectation. Those firms will need an India overlay for exposed and crown-jewel assets rather than a single worldwide standard. The SLAs that once looked prudent now risk looking structurally slow.

The advisory also aligns India with global prioritisation norms. It directs organisations to use Known Exploited Vulnerabilities (KEV) prioritisation, Exploit Prediction Scoring System (EPSS) likelihood assessment, and bill-of-materials mechanisms including SBOM, AIBOM, QBOM, and CBOM. These are international standards CERT-In has made the assumed floor.

## THE VENDOR QUESTION

The advisory's sharpest test for the channel is what happens when a fix depends on a third-party vendor who cannot deliver inside the window. The advisory's own guidance is to fall back on isolation, access restriction, and enhanced monitoring while documenting mitigation actions and escalation steps. Contractual clarity on patch timelines, the document makes clear, is no longer optional.

The enterprise still owns the exposure window even when the patch does not, Gogia said. "Procurement can no longer optimise narrowly for features, integration, and cost," he said. Vendor responsiveness during an exploit window is now part of operational resilience. The governance failure is not vendor delay. It is arriving at disclosure without the contractual right to force a response already in hand.

The implication for the channel is direct. System integrators and resellers who sit as the contractual interface between Indian enterprises and global vendors are holding a value proposition that did not exist 18 months ago: vendor responsiveness as a saleable service tier. Partners who can negotiate, enforce, and operationalise faster vendor SLAs — and layer compensating controls when those SLAs slip — are selling something the advisory has just made structurally necessary.

The organisations that struggle most, Gogia said, are rarely the technologically immature ones. They are the operationally fragmented ones, where infrastructure, SOC, application owners, cloud teams, procurement, and vendors run on disconnected clocks. Channel partners who can sell integration of those clocks — through MDR, exposure management platforms, attack surface monitoring, or tighter operational governance — are selling the resolution to the fragmentation the advisory has just exposed.

## WHAT IT MEANS FOR THE CHANNEL

Read commercially, the advisory creates demand across several product and service categories at once.

External attack surface management and exposure management platforms move from nice-to-have to baseline. The advisory's Phase I roadmap, covering zero to seven days, directs organisations to "identify critical assets and internet-facing systems" — a Phase I instruction most enterprises cannot complete with what they have on hand. Managed detection and response services gain a sharper commercial argument: the 12-hour and one-day windows assume detection and response capabilities most enterprises cannot staff internally. SBOM tooling moves up the priority list, with CERT-In naming SBOM, AIBOM, QBOM, and CBOM explicitly. Patch automation, prioritisation engines tied to KEV and EPSS, and orchestration platforms all benefit.

Underneath all of it, the consulting opportunity is the largest. Most Indian enterprises will not buy a single product to meet the advisory's expectations. They will need to redesign processes, redraw responsibilities between security and IT operations, retrain staff, and renegotiate vendor contracts. That work is the channel's, if the channel is ready to do it.

## THE SLACK IS GONE

AI did not invent vulnerability management pressure. What it has done, as Gogia put it, is remove the remaining slack from the system. The monthly patch cycle was always a compromise. AI-assisted exploitation has made that compromise indefensible, and CERT-In has now written it into national expectation.

The advisory is advisory. It will not stay that way. The Indian enterprises and channel partners that treat it as a preview of statutory obligation — and start closing the visibility, governance, and vendor-management gaps now — will be ready when it stops being voluntary. The ones that wait will find themselves explaining to auditors, regulators, and boards why their clocks ran slower than the attackers'.

That conversation is coming. The advisory has just set the date.

# CYBERSECURITY : THE ATTACK SURFACE GREW. THE INDUSTRY GREW FASTER.

*India recorded over 265 million cyberattacks in 2025. As the threat landscape grows faster than any firewall can contain it, the country is building a security architecture that is more ambitious — and more urgent — than ever before*

Every eleven seconds, a cyberattack somewhere in the world claims a new victim. In India, that rhythm has become a drumbeat. Indian organisations faced an average of 2,011 cyberattacks per week in 2025 — significantly higher than the global average — according to Check Point Software Technologies' State of Cyber Security in India 2025 report. CERT-In, India's national cyber response agency, handled over 29.44 lakh cyber incidents in 2025 alone, issuing 1,530 alerts, 390 vulnerability notes, and 65 advisories. The Union Budget 2025–26 allocated Rs 782 crore specifically for cybersecurity — a figure that signals the government's recognition of digital security as national infrastructure rather than departmental overhead.

The scale of the threat is matched, at least in ambition, by the scale of the response. India's cybersecurity market is being reshaped by regulatory pressure, AI-driven threat evolution, a deepening talent shortage, and an investment surge pulling enterprise budgets decisively toward managed, cloud-native, and intelligence-led security architectures. Fiscal 2025–26 was the year that cybersecurity stopped being an IT department conversation in India, and became a boardroom imperative.

## The Market: A Billion-Dollar Shield Being Built at Speed

India's total cybersecurity market — encompassing hardware, software, and services — was valued at $ 8.58 billion in 2025 and is projected to reach $ 16.86 billion by 2030, growing at a CAGR of 14.5 percent, according to MarketsandMarkets. Globally, IDC estimates worldwide security spending will grow 12.2 percent in 2025, reaching $ 377 billion by 2028 — with security software as the largest segment and managed security services as the fastest growing. India's growth rate at 14.5 percent runs ahead of the global average, reflecting both its rapidly expanding digital attack surface and the relative immaturity of security investments compared to more developed markets.

Breaking down India's market by component offers a clearer picture of where spending is concentrated and where it is heading. Hardware — firewalls, intrusion detection systems, and unified threat management devices — accounts for the largest share of total market revenue, driven by public sector procurement for critical infrastructure and the continued build-out of physical security layers across banking, defence, and government. Software and services together form the faster-growing layer. On the software and services side specifically, Gartner estimates India's end-user information security spending — covering security software, security services, and managed security — at $ 3.3 billion in 2025, up 16.4 percent from 2024, and projected to grow a further 11.7 percent to $ 3.4 billion in 2026. Security software alone is expected to reach $ 1.56 billion in 2026, growing 12.4 percent year-on-year, as enterprises expand investments in application security, cloud security, and data protection tools.

Within services, managed security is the fastest-growing subsegment, forecast to grow 15.1 percent in 2026 as organisations turn to outsourced threat detection and response to bridge a widening talent gap. NASSCOM data indicates a 40 percent deficit in India's cybersecurity workforce — a structural shortage that is directly accelerating adoption of managed detection and response contracts and third-party SOC operations. BFSI leads all Indian verticals in security spending, driven by the scale of UPI — which now processes over 15 billion transactions per month — and the compliance requirements of the RBI, SEBI, and IRDAI. Cloud-based security is the fastest-growing deployment model, as enterprises accelerate cloud migration and encounter its security implications in real time.

## The Threat Landscape: AI, State Actors, and Supply Chain Vulnerabilities

Fiscal 2025–26 produced a threat landscape that was qualitatively different from prior years — not just larger in volume, but structurally more dangerous in character. Three forces converged to define it.

The first was the weaponisation of artificial intelligence by threat actors. Attackers deployed AI-generated phishing campaigns with personalisation that legacy detection systems could not reliably identify. Ransomware evolved into multi-stage operations combining credential harvesting, lateral movement, and data exfiltration before triggering encryption — making the ransomware payload the last visible event in a long intrusion chain. Deepfake-enabled fraud, impersonating executives and public officials through synthetic audio and video, emerged as a significant new social engineering vector exploiting institutional trust at a scale that traditional phishing cannot achieve.

The second was a marked escalation in state-sponsored cyber activity. During India's Operation Sindoor in May 2025, a coordinated wave of cyber operations targeted Indian government websites and critical infrastructure simultaneously. Reported impacts included approximately 19 hours of distributed denial-of-service targeting the President's official website, approximately 200,000 probing and attack attempts against the power grid, and defacements across multiple ministry portals. The Seqrite India Cyber Threat Report 2026 documented a coordinated hybrid warfare campaign blending

APT36, SideCopy, and hacktivist groups targeting India's defence and government networks throughout the fiscal year.

The third was the rapid expansion of the attack surface through cloud misconfiguration and supply chain vulnerabilities. Angel One, one of India's largest stockbroking platforms, disclosed in February 2025 a breach traced to unauthorised access to AWS-hosted resources, with client data for 7.9 million users potentially exposed. A malware incident targeting a third-party vendor portal linked to ICICI Bank, claimed by the Bashe ransomware group, reflected a growing pattern of supply chain attacks entering India's banking sector through vendor access pathways rather than direct infrastructure compromise. In June 2025, Delhi hospitals Sant Parmanand and NKS Super Speciality suffered server intrusions that disrupted OPD and IPD digital workflows, forcing reversion to manual processes — demonstrating that the healthcare sector's rapid digitisation had not been matched by equivalent security investment.

## The Regulatory Architecture: DPDP, CERT-In, and New Accountability

India's regulatory cybersecurity framework underwent significant tightening in fiscal 2025–26, creating binding new compliance obligations and — in the process — new budget lines across every regulated sector.

The Digital Personal Data Protection (DPDP) Act, 2023, came into full implementation focus in 2025. The Act imposes fines of up to Rs 500 crore for personal data breaches, mandates incident reporting within six hours, requires log retention for 180 days, and demands comprehensive data protection impact assessments for high-risk processing activities. Draft enforcement rules issued in January 2025 further codified consent requirements, cross-border data transfer norms, and organisational accountability mechanisms. Gartner's Shailendra Upadhyay said in March 2026 that "the implementation of India's DPDP Act, combined with emerging AI regulations across global markets, is increasing compliance complexity and placing new accountability pressures on CISOs." Identity-based attacks, he added, were driving identity-first security up executive agendas across Indian enterprises.

CERT-In published its Comprehensive Cyber Security Audit Policy Guidelines in 2025, mandating annual cybersecurity audits for critical infrastructure operators — covering information technology, operational technology, cloud, supply chain, and physical security layers. In fiscal 2024–25, CERT-In conducted nearly 10,000 audits across critical sectors including power, transportation, and banking. The Department of Telecommunications' Telecom Cyber Security Rules required service providers to report breaches within six hours and share attack scope within 24 hours. Together, these frameworks are elevating cybersecurity compliance from a technical function to a board-level accountability across Indian enterprises and government bodies.

## Key Players: A Three-Tier Ecosystem

India's cybersecurity market operates across three distinct tiers, each playing a different and complementary role.

Among domestic IT services majors, TCS has built its Cyber Defence Suite around AI and machine learning capabilities, providing proactive threat intelligence and automated incident response across enterprise client networks. Infosys, Wipro, HCL Technologies, and Tech Mahindra have embedded cybersecurity across their digital transformation portfolios, with managed SOC operations, zero-trust architecture deployment, and DPDP compliance services as growth areas. Tata Communications has partnered with Palo Alto Networks to deliver secure hybrid IT environments, leveraging its national network backbone alongside Palo Alto's cloud-native security platform. Wipro has partnered with Okta to integrate identity and access management into zero-trust frameworks for enterprise clients.

Among homegrown cybersecurity specialists, Quick Heal Technologies — India's most established domestic security product company — continued to serve enterprise and consumer segments through its Seqrite brand, which also produces the India Cyber Threat Report, one of the country's most authoritative annual threat intelligence publications. Innefu Labs, ESEC Forte Technologies, and CyberNX Technologies represent an emerging tier of Indian-origin firms building AI-driven security analytics, managed SOC services, and identity security solutions tailored to India-specific threat patterns. In March 2025, Zero Defend Security unveiled Vastav AI — described as India's first deepfake detection system — a cloud-based platform using machine learning, forensic analysis, and metadata inspection to identify AI-generated media with a reported accuracy of 99 percent.

Among global technology vendors, Palo Alto Networks announced a strategic partnership with a leading Indian telecommunications provider in October 2025 to integrate its security solutions into telecom infrastructure. Check Point Software Technologies launched an India-based data residency instance of its Harmony SASE platform in May 2025, designed for localised, cloud-delivered network security compliant with India's regulatory environment. Fortinet launched an AI-driven security suite specifically for Indian SMEs in September 2025 — addressing a segment that global enterprise security vendors have historically underserved. CrowdStrike, Cisco, Zscaler, Trend Micro, and Darktrace maintained strong enterprise presences, competing on AI-enhanced detection, extended detection and response (XDR) platform depth, and cloud-native integration capabilities.

## The Road Ahead: AI-First, Identity-Led, and Compliance-Driven

Three strategic shifts will define Indian cybersecurity through the remainder of the decade. The transition to AI-native security — where detection, response, and remediation are automated and intelligence-driven — is no longer a future state. Indian SOCs are deploying machine learning to process the volume of alerts that human analysts alone cannot manage, moving security operations from reactive to predictive.

Identity-first security is becoming the defining architectural choice. The rise of agentic AI — autonomous systems acting on behalf of users across enterprise applications — has created new non-human identity vectors that traditional IAM tools were not designed to govern. Gartner's Alex Michaels noted in March 2026 that the rise of agentic AI "introduces new challenges that expose gaps in traditional identity and access management approaches," as enterprises must now govern not just human users but AI agents operating with enterprise credentials.

Compliance will continue to be a structural demand driver. With the DPDP Act's enforcement machinery now operational, and sector-specific mandates from RBI, SEBI, IRDAI, and the NCIIPC tightening in parallel, security budgets in India's regulated sectors face sustained upward pressure regardless of broader IT spending cycles. Gartner projects India's information security spending to grow at double-digit rates through the forecast period — a trajectory that reflects both the deepening threat environment and the irreversibility of India's digital transformation.

India is simultaneously one of the most targeted and most rapidly adapting cybersecurity markets in the world. The gap between the two — between the pace of attack and the pace of defence — is what the industry exists to close.

**India Cyber Threat Scale 2025**

| Metric | Figure | Source |
|---|---|---|
| Average cyberattacks per organisation per week | 2,011 | Check Point India 2025 |
| Total cyber incidents handled by CERT-In | 29.44 lakh | PIB / CERT-In |
| Govt cybersecurity budget allocation | Rs 782 crore | Union Budget 2025–26 |
| CERT-In audits conducted in FY2024–25 | ~10,000 | CERT-In guidelines |

## AMD assigns Vinay Awasthi as Senior Vice President, Sales for APJ

AMD announced the appointment of Vinay Awasthi as Senior Vice President, Sales, Asia Pacific and Japan (APJ). In this role, he will lead the regional sales strategy and execution for AMD across one of the company's fastest-growing regions.

Based in Singapore, Vinay will focus on deepening customer engagement, strengthening OEM and channel partnerships, and aligning go-to-market strategies across APJ's diverse markets to support continued growth across cloud, enterprise, AI, commercial and consumer segments.

Vinay brings more than two decades of global sales leadership experience in the technology industry. Prior to joining AMD, he served as Senior Vice President and Global Head of Compute Sales at Qualcomm. Before that, he spent 21 years at HP, where he held multiple senior leadership roles with both regional and global scope. Throughout his career, Vinay has built strong customer and partner relationships while driving sustained growth across complex international markets.

## Lenovo promotes Ashish Sikka as Executive Director– PCSD Category

Lenovo has elevated Ashish Sikka to the position of Executive Director – PCSD Category. Ashish is associated with the company for almost 21 years and prior to the elevation he was serving as Director – PCSD Category. He played an instrumental role in driving Lenovo's commercial strategy, category growth, and market leadership across multiple business segments.

Ashish brings a rare combination of deep institutional knowledge, market insight, and proven business leadership. His elevation comes at a pivotal time as the PC and smart devices ecosystem undergoes rapid transformation, driven by AI-powered computing, enterprise modernization, hybrid work models, and evolving channel dynamics.

He began his career in the company in a frontline sales role, managing key IT/ITES and telecom accounts, where he developed strong capabilities in enterprise engagement, customer acquisition, and strategic account management.

## Samsung India promotes Shirish Agarwal as Head of Marketing for its MX business

Shirish Agarwal has been promoted to Head of Marketing for Samsung India's entire MX business. This promotion follows Shirish's nearly three-year-long tenure with Samsung India, where he served as Director of Marketing since 2023. He will lead Samsung's marketing strategy and brand initiatives for mobile experiences in India. Prior to his promotion as Head of Marketing, he served as Director of Marketing for the company.

Shirish first joined Samsung India in 2009 as Deputy General Manager, Marketing, and spent nearly a decade with the company. After that, he also worked with companies like HP as a Marcom Specialist in the Imaging & Printing Group, Times Internet as a Product Manager, and CyberMedia as an Assistant Manager.

Shirish Agarwal has built strong experience and expertise in handling brand communication, consumer behaviour, and marketing strategies over the years.

## IAS Priyank Bharti appointed DG of NIC, takes on Additional Secretary role in MeitY

Priyank Bharti, IAS, has officially taken charge as Director General (DG) of the National Informatics Centre (NIC), marking a significant administrative development in India's digital governance landscape. Presently, he is serving as Administrative Secretary, Science, Technology and Environment, Government of Punjab.

A 2001-batch IAS officer from Punjab cadre, Bharti was appointed as the Additional Secretary in the Ministry of Electronics and Information Technology (MeitY) by the Appointments Committee of the Cabinet (ACC). Additionally, he will also serve as the DG of NIC.

As Additional Secretary at MeitY, Bharti will contribute to critical areas such as digital infrastructure policy, technology governance, e-governance initiatives, digital public service delivery, innovation frameworks, and large-scale digital transformation programmes.

As DG of NIC, he will oversee key government digital infrastructure and IT systems that support governance operations across both central and state governments.

## Rajeev K Abichandani joins Palo Alto Networks as Director - Channels, India & SAARC

Rajeev K Abhichandani has joined Palo Alto Networks as Director - Channels, India & SAARC, strengthening the company's channel leadership as it continues to deepen its presence across the region's cybersecurity market.

Prior to this, Rajeev was associated with Fortinet for over five years as Head – Enterprise Channels & MSSP, India & SAARC, where he played a pivotal role in driving revenue growth, expanding market presence, and strengthening the company's partner ecosystem across the region.

In a post on LinkedIn, he wrote, "After 5.5 incredible years at Fortinet, I bid farewell with immense gratitude for a journey that has shaped my career and personal growth in so many meaningful ways.

Looking back, this phase has been filled with learning, teamwork, success and countless memorable moments. From building a strong partner relationships to leading and mentoring a talented team, every experience has contributed to my journey as a professional and leader."

## Tata Communications names Ganapathi S. Lakshminarayanan as CEO and MD

Tata Communications has positioned Ganapathi S. Lakshminarayanan as Chief Executive Officer and Managing Director for a period of five years, effective from May 20, 2026 and subject to shareholder approval.

Prior to Tata Communications, Lakshminarayanan was associated with ServiceNow as Managing Director and Group Vice President, India and the SAARC region. He led regional operations and business expansion initiatives. In his career, he held many leadership positions at Airtel which includes CEO of Airtel Business in India and CEO of the Enterprise Business Unit. In these roles he managed enterprise services business operations and customer focused technology solutions across markets. He has an experience of over 30 years across multinational corporations enterprise businesses and technology driven organisations. His expertise covers digital transformation, enterprise communications, and business growth strategy.

Instant On

# HPE Networking Instant On Secure Gateways

## Your first line of defense

## Features

- Protect your network from external threats
- Centralize control of traffic
- Free firmware updates and security patches
- Control the network from a single dashboard
- No subscriptions or fees
- Lower TCO
- Ensure efficient data flow

## Instant Setup, Instant Protection. Finally, a security gateway that speaks SMB.

HPE Networking Instant On — Empowering SMBs with Secure, Smart, and Scalable Solutions.

Hewlett Packard Enterprise | savex TECHNOLOGIES

**For more details contact**
Neel Parmar | +91 9909542542 | neel.parmar@savex.in

RNI - NO 72399/1999

Reg. No: DL-SW-01/4030/24-26
Posted at LPC Delhi RMS Delhi - 110006

Date of Posting 20 & 21
Date of Publishing / Printing: 18 & 19