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

VOLUME XXVII ISSUE 07 MARCH 2026 PRICE RS. 50

FACEOFF

OPINION MATTERS

Delaware, USA | New Delhi, INDIA

FaceOff delivers privacy-by-design through zero-trust authentication, encrypted biometrics, deepfake detection, and federated AI—turning regulatory compliance into enforceable, resilient digital trust architecture.

KEY SOLUTIONS:

BFSI	GOVERNANCE & RISK	LAW ENFORCEMENT AGENCY

WWW.FACEOFF.WORLD

॥ श्रीहरि: ॥

मा सैव्यम् पराजितः

Security You Can **Actually Depend On.**

Hack Proof, Tamper Proof and Cyber Secure.

ctc TECHNOLOGY

CP PLUS TRUSTED CORE **TECHNOLOGY**

- **Secure Boot**
- **Tamper Proof**
- **Secure Transmission**
- **Strong Cryptography Algorithms**
- **Data Security**

CIN No.: L74899DL1995PLC066784

www.cpplusworld.com | sales@cpplusworld.com

CP PLUS

ER CERTIFIED BY STQC
गुणोत्कर्षे समृद्धि

POWERED BY ctc TECHNOLOGY

MADE IN Bharat

Sales Enquires & Support No.
1800-102-6526

Technical Support No.
8800952952

Microsoft | savex TECHNOLOGIES

Control the breach with

Microsoft Security

You cannot defend what you cannot see

Microsoft Security delivers end-to-end protection with AI-powered defense and Zero Trust, safeguarding identities, data, and devices to keep businesses resilient and future-ready.

Power of Microsoft Security

End-to-End Protection

Zero Trust

AI-Powered Defense

Advanced Security and Compliance for SMBs

M365 Business Premium - $22.00

- Cloud Services
- M365 Apps Desktop, Web & Mobile
- Microsoft Entra ID P1 ($6)
- Intune ($8)
- M365 Defender for Business
- M365 Defender for Office P1

+

Defender Suite for Business Premium $10pupm*

- Microsoft Defender for Office 365 Plan 2 ($5)
- Microsoft Defender for Cloud Apps ($3.50)
- Microsoft Entra ID P2 ($9)
- Microsoft Defender for Identity ($5.50)
- Microsoft Defender for Endpoint P2 ($5.20)
- Microsoft Defender for IoT – EIoT ($0.85*)

+

Purview Suite for Business Premium $10pupm*

- M365 E5 eDiscovery & Audit $6/u/m
- M365 E5 Insider Risk Management $6/u/m
- M365 E5 Info Protection & Governance $7/u/m

+

Defender & Purview Suite for Business Premium $15pupm*

- Microsoft Defender for Office 365 Plan 2 ($5)
- Microsoft Defender for Cloud Apps ($3.50)
- Microsoft Entra ID P2 ($9)
- Microsoft Defender for Identity ($5.50)
- Microsoft Defender for Endpoint P2 ($5.20)
- Microsoft Defender for IoT – EIoT ($0.85*)
- M365 E5 eDiscovery & Audit $6/u/m
- M365 E5 Insider Risk Management $6/u/m
- M365 E5 Info Protection & Governance $7/u/m

For Microsoft Business Related Enquiry:

mehul.ved@savex.in | +91 9326999819

nitesh.pawar@savex.in | +91 7385559968

sasanka.sandha@savex.in | +91 7853014143

Linkedin

Visit us on www.savex.in

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

VOLUME XXVII ISSUE 07 MARCH 2026 PRICE RS. 50 SUBSCRIPTION COPY NOT FOR SALE

THE NEW CLOUD PLAYBOOK: AI, MULTI-CLOUD AND ZERO-TRUST TAKE CENTER STAGE

PAGE 34

Govt approves 75 ECMS projects to boost electronics manufacturing, jobs

India has taken a major step to strengthen its electronics manufacturing ecosystem, with Union IT Minister Ashwini Vaishnaw announcing approval of 75 projects under the Electronic Components and MSME (ECMS) programme. With a total investment of ₹61,671 crore, the initiative is expected to generate around 65,000 jobs. The projects focus on producing critical components like PCBs, rare-earth magnets, and inductors, supporting domestic semiconductor growth, reducing import dependence, and enhancing India's self-reliance in electronics.

Microsoft Copilot gets multi-model AI upgrade for more accurate, reliable outputs

Microsoft has unveiled new features in its Copilot research assistant, enabling users to run multiple AI models simultaneously. The new "Critique" feature combines outputs from OpenAI's GPT and Anthropic's Claude, with GPT generating responses and Claude reviewing them for accuracy and quality. Microsoft plans to make the workflow bi-directional in the future. The multi-model approach aims to reduce AI errors, enhance reliability, and improve productivity, while the new "Model Council" lets users compare outputs side-by-side.

MULE NETWORKS: INDIA'S BIGGEST FRAUD THREAT

Mule networks are built to look legitimate at every stage, spreading funds across vast linked accounts—making detection nearly impossible without cross-platform visibility.

The India Fraud Report 2026, the report highlights a seismic shift in the nation's criminal landscape. As digital transactions become the heartbeat of the economy, fraud has transitioned from isolated incidents into a highly organized, industrialized enterprise. The scale of this crisis is underscored by the RBI Annual Report 2024-25, which recorded banking sector fraud losses surging to ₹36,014 Crore. This financial bleeding is driven by exploiting real-time payments and instant onboarding systems, allowing fraudsters to scale attacks with unprecedented speed and precision.

In 2025, identity became the primary entry point for fraud in India's digital economy, with fragmented, reusable data exploited at scale. As a result, decision errors emerged as the biggest risk, making it harder to distinguish genuine users from fraudsters.

The report identifies mule networks as the most significant challenge, with 48% of Indian enterprises naming them their top threat. These industrialized networks utilize clusters of interconnected accounts to mimic legitimate activity, making them far harder to detect than social engineering, which was cited by 33% of organizations. Without integrated, cross-platform visibility, these sophisticated "hide-in-plain-sight" operations remain largely invisible to traditional, siloed defense systems.

A significant portion of the struggle lies in the operational inefficiency of current risk teams. The report reveals that 58% of organizations struggle primarily with false positives, meaning security professionals are bogged down investigating legitimate users while actual threats slip through. This "decision error" has become the primary risk factor as identity data becomes increasingly fragmented and reused at scale. When risk teams cannot accurately distinguish a genuine customer from a fraudster, the resulting friction harms the user experience and leaves the enterprise vulnerable to high-velocity attacks.

The evolution of Generative AI has further tilted the scales in favor of criminals. Advanced AI tools can now create hyper-realistic fake documents, images, and synthetic identities that easily bypass traditional verification methods. Compounding this is the rise of Fraud-as-a-Service (FaaS) on the dark web. These ready-to-use kits provide even low-skill actors with malicious APIs, stolen personal data, and automated scam scripts. This democratization of cybercrime has lowered the barrier to entry, turning fraud into a scalable, plug-and-play industry.

The report reveals a major strategic disconnect, with 50% of Indian firms viewing compliance solely as a protective shield against penalties or reputational harm. Only 20% of organizations leverage compliance as a proactive tool to drive risk investment. This reactive approach creates a dangerous "exposure gap," leaving defenses static while fraud tactics evolve, specifically endangering first-time digital users who lack the protection of adaptive anti-fraud infrastructure.

Experts emphasize that the solution lies in the "network effect" of defense. Since fraudsters reuse successful patterns and tools across different platforms, defenders must look beyond isolated data points. By analyzing identities and devices across entire ecosystems, organizations can build contextual intelligence. This allows for identifying signals that should not logically repeat—such as the same hardware identifier appearing across unrelated systems—enabling risk teams to flag and neutralize threats in real time.

A recently uncovered operation involving 2,700+ linked users across multiple platforms highlights the limits of isolated transaction monitoring. Effective detection requires combining identity, device, and behavioral signals. To counter such coordinated networks, enterprises must adopt graph analysis to map relationships and expose hidden criminal clusters.

The 2026 report makes it clear: incremental, point-based controls can no longer close the security gap. As fraud moves across networks, isolated defenses fail. Enterprises must adopt lifecycle-based risk orchestration—continuously monitoring users from onboarding through every transaction, making security an ongoing process, not a one-time check.

Furthermore, the report advocates for a new era of intelligence sharing between institutions. Because modern fraud operates as an interconnected industry, the defense must be equally collaborative. Sharing anonymized threat data and fraud patterns across the banking and digital sectors can create a collective immunity, making it much harder for mule networks to hop from one victim to another without detection. Breaking down the silos between competitors is essential to creating a safer digital economy for all participants.

The message is clear: digital trust needs a complete rethink. Anti-fraud can no longer be treated as a cost or checkbox—it must be a core business enabler. As criminals scale with AI and organized networks, enterprises must adopt coordinated, adaptive, and scalable defenses to match their sophistication and protect India's digital future.

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

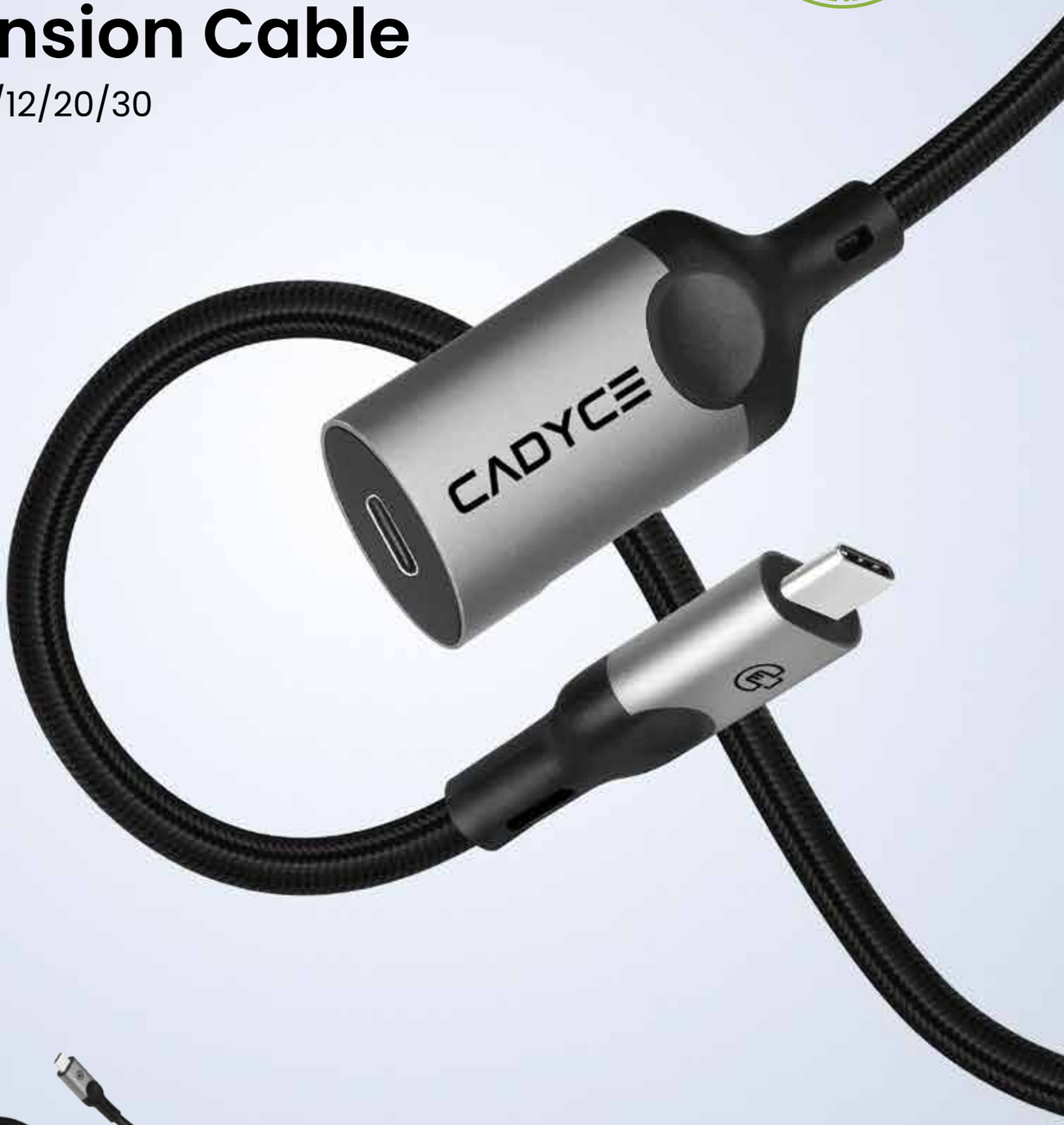
CADYCE

Life Aasaan Banaao
www.cadyce.com

PICKUP FREE DELIVERY

USB-C® Male to USB-C® Female Extension Cable

CA-CX5/12/20/30



Enjoy high-speed data and reliable connectivity with CADYCE USB-C® Extension Cables, available in 5m, 12m, 20m, and 30m lengths.

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
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

INDUSTRY EVENT / 28pg

WIITF 2026: Reiterating the role of VARs in shaping the future of India's Technology landscape

Omada
by tp-link

Not Just Devices.
A Complete Network Strategy

Omada SDN unifies Gateways, Switches, Access Points, and Controllers into one intelligent ecosystem.

Disconnected tools create complex networks.
Omada simplifies everything.

One platform. One dashboard. One ecosystem.

- ✓ Access Points for seamless roaming
- ✓ Switches for scalable aggregation
- ✓ Gateways for secure routing & VPN
- ✓ Controllers for centralized management

From single-site offices
to multi-location enterprises
to nationwide deployments

Omada adapts. Expands. Evolves.

- Zero-Touch Provisioning
- Multi-Site Management
- Cloud & On-Prem Control
- Unified Monitoring
- Secure VPN Architecture
- Enterprise-Grade Reliability

Build once. Scale infinitely.

Call for Product Demo!

Discover the Omada Ecosystem. Visit : OmadaNetworks.com/in

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

Banglore
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**

Rate Payer Protection Pledge: An Affirmative Step Less Talked about Amidst Middle East War

DR. ASOKE K. LAHA
Chairman-Emeritus and Founder, InterraIT

I have spent quite some time pondering my column for this month. Several ideas have come to me including that of the ongoing war in the Middle East, but I was imbued with a lurking fear that by the time the article sees the light of the day, either in print or digital format, my narratives would become archaic since the war dynamics are of a catastrophic dimension and mostly unpredictable.

I abandoned the idea of writing about the war with hope that it should be over soon since the ordinary people across the world are suffering. Supply chains are affected for almost all commodities, fuel occupying the top slot. Almost all countries are yelling at the top of the voice the limited supplies of fuel, cooking gas, essential commodities including food items since haulage of goods are affected considerably due to closure of Strait Hermes, through which more than 20% of the goods pass through. Some of the food importing countries in Africa and elsewhere are complaining about inadequate food stocks that can last only for a short time.

I have decided to write on a subject that is not discussed much in the media and is oblivion to most of the people. It is about the data centers, which the government announced as a major decision in the last general budget (2026-27). Here again, I want to be politically correct and not join issues with any political parties. I do not feel that by opening up the running of data centres to foreign companies, we are not compromising with political sovereignty nor I do not think by extending tax holidays to them till 2047, Indian IT companies are put into a disadvantageous position. My apprehensions are different and more to do with economics rather than politics.

Let me explain. I do not know how many of my esteemed readers are aware of or have taken note of the Rate Payer Protection Pledge. It urges America's largest AI firms to build or procure their electric supply for data centers that power AI. The non – binding pledge asks major AI companies including Alphabet, Microsoft, Amazon, Meta, Oracle and XAI to pay the full cost of energy generation and grid upgrades to run their facilities. They are warned not to pass such costs on to ordinary consumers.

What does this mean for these companies? Companies running data centers must cover the additional expenses incurred for such centres. They must finance every additional expense for running and expanding the projects, including electricity and water, and agree to cover the cost of additional datacenter operating expenses. Firms will finance or build new power generation and delivery infrastructure to support data centers. The other responsibility is training local talents in communities to take up the responsibilities, thereby creating local jobs.

The initiative is part of the broader strategy to promote AI leadership while addressing concerns about energy affordability. While the pledge has been praised by tech executives as a step toward responsible energy use, some experts remain sceptical as the actual implementation will depend on agreements with utilities and regulators. In summary the growth of AI infrastructure does not burden households with higher electric bills.

Why is this important for India? Let us scan through some of the initiatives including India's AI strength. Recently, an AI Conference was held in Delhi inviting delegates from over 160 countries, AI expert, social scientists etc, which had unveiled a plan to deepen AI penetration in India and at the same time warding off some of its fallout to insulate the economy from falling job opportunities and to open up innovation and disruption on a mass scale, seen never before.

Also, prior to that, a string of new policies was unveiled to enhance the production of semiconductors by setting up foundries and manufacturing smartphones in the country. Through various schemes, the government is also promoting production of various components and ancillaries that go into the production. Going by the scale in which our ICT production is going up, we will be facing a massive problem of side effects of excessive solid waste and other related issues

The first casualty will be on our environment. For instance, maintaining data centers and setting up production bases for chips need a clean environment. Also, these are energy guzzling industries. Where will we find such large requirement of power to run these units without additional generation? By pinning on the government to invest in energy generation overlooking other pressing sectors is thinly spreading the limited resources which are not the pressing need of the people. Also, such industries need large quantum of water for coolers and other processes, which entails investments.

It is the right time for India to also embark on a similar pledge from industry, particularly the large ones to bear the cost of the projects that are needed to run their establishments without hiccups whether it is for additional energy, water or for other utilities. These multi-billion companies can absorb such costs. This would also help the government spend its budgets directed at the target groups, the vulnerable sections of the society.

I also feel the same set of norms should apply to running data centers, which are now open to FDI investments with additional tax incentives like tax holidays until 2047. Such centres need a large quantum of investment for generating electricity and sourcing water. Let them bear that cost and plug loopholes that tempt them to avail such essential ingredients from the common pool.

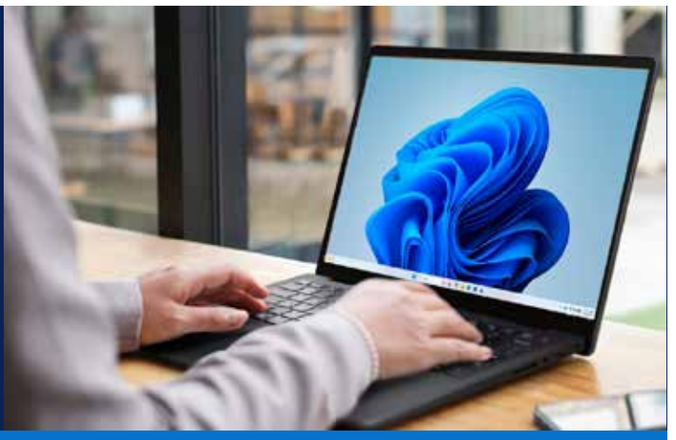
The other important area is environment. Excessive use of raw materials and production of ICT devices and equipment will result in a large quantum of solid waste. The OECD countries have come out with their calibrated policy to reduce environment degradation through solid wastes. They have evolved a norm to recycle 24% of the electronic gadgets through repair and retrofitting and making them reuse. This is a laudable policy that should be adapted in India, where there is a large scope for re-using some of the solid wastes. Also, rare earths like lithium, used for manufacturing batteries for electric vehicles can be recycled to utilize such rare earths, which are again in short supply. These are some of the steps that we can carry out with little effort but with a larger impact.

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

FAIITA urges 'force majeure' relief as global chip shortage disrupts India's PC supply chain

The Federation of All India IT Associations has raised concerns over a severe global shortage of DRAM and SSD components, warning of major disruptions in desktop supply chains. In a representation to the Government e-Marketplace (GeM), the body, led by President Navin Gupta, urged authorities to declare the situation a 'force majeure' event to shield IT businesses from contractual penalties.

The shortage is driven by semiconductor capacity shifting toward AI infrastructure, causing sharp price hikes and delays. Since mid-2025, RAM and SSD prices have surged significantly, while delivery timelines have extended up to eight months, making contract fulfilment increasingly challenging for vendors and resellers.

FAIITA has sought urgent policy relief, including price variation clauses, protection of seller ratings, and the creation of a monitoring task force. The move aims to safeguard small and medium IT firms from financial losses during a crucial procurement period.

Karnataka proposes draft policy to limit student screen time to one hour daily

Karnataka is preparing a draft Policy for Responsible Digital Use Among Students, aiming to curb technology addiction and protect mental health. The proposal recommends limiting recreational screen time to one hour per day for students from Classes 9 to 12, excluding academic use. It also suggests age-appropriate devices, audio-only mobile options, and automatic data shutdown by 7pm to reduce late-evening exposure.

Prepared by the Department of Health and Family Welfare with KSMHA, NIMHANS, and the Department of Education, the policy includes training for teachers and parents on digital well-being. Schools will integrate digital literacy, online safety, consent, and privacy into curricula while curbing unnecessary browsing.

The draft mandates each school to implement a Digital Use Policy addressing cyberbullying, device limits, and teacher-student communication protocols. Guidelines for AI use in assignments, including plagiarism checks, are also proposed. The policy follows Chief Minister Siddaramaiah's announcement to restrict social media use for children under 16.

Apple brings enterprise tools under one roof with new 'Apple Business'

Apple has launched an all-in-one enterprise platform, "Apple Business," that combines its key business tools into a single interface. The platform is designed to help organisations manage devices, connect with customers, and streamline daily operations. Notably, mobile device management, previously a paid feature under Apple Business Essentials, is now offered free across more than 200 countries.

The new platform merges Apple Business Manager, Apple Business Essentials, and Apple Business Connect, creating a unified ecosystem. Apple said existing user data will be automatically migrated, ensuring a seamless transition while simplifying access to app deployment, device management, and brand presence tools.

Apple Business also integrates email, calendar, and directory services, allowing companies to use custom domains and manage workflows efficiently. The move aims to deliver a secure, scalable solution for businesses of all sizes.

RBI eyes AI-driven digital infrastructure to boost India's payments ecosystem

The Reserve Bank of India is expanding its digital public infrastructure (DPI) by leveraging artificial intelligence (AI) and APIs to strengthen the country's payments ecosystem. The move aims to enhance user experience as digital transactions continue to grow rapidly across India.

Speaking at an industry event recently, RBI Executive Director P Vasudevan said AI could streamline customer journeys and automate grievance redressal. Systems may automatically identify failed transactions and trigger resolution mechanisms, reducing manual intervention and improving efficiency amid surging transaction volumes.

The central bank is also emphasizing interoperability between platforms to create a seamless ecosystem. Vasudevan noted that enhanced integration could spur innovation by startups and tech players, helping deliver faster, reliable, and more holistic financial services. RBI's AI-driven infrastructure push is set to shape the future of India's digital payments landscape.

Sarvam AI to set up sovereign AI park in Gujarat

The Gujarat government has signed a Memorandum of Understanding (MoU) with Sarvam AI to set up a sovereign AI park, strengthening its push to become an emerging technology hub. The agreement was formalised during an AI Startup Dialogue at the Chief Minister Bhupendra Patel's residence, where innovations across sectors such as agriculture, healthcare, education, and industry were showcased.

The proposed park will feature advanced computing infrastructure, research and innovation centres, and skill development facilities. It will also support AI-driven governance solutions and technologies aimed at improving citizen services through an integrated campus approach.

The initiative is expected to generate significant employment over the next five years while building a robust AI ecosystem. The state will fast-track approvals and provide policy support, with the Chief Minister emphasising innovation, transparency, and efficient delivery of government services through AI.

Google Play to label verified investment apps as Sebi tightens grip on frauds

In a bid to curb rising investment fraud, Google will introduce a verified badge for legitimate trading apps on its Play Store in India. Securities and Exchange Board of India (Sebi) Chairperson Tuhin Kanta Pandey said apps of Sebi-registered intermediaries will carry the label, helping users identify authentic platforms while reducing impersonation risks.

Pandey highlighted the growing threat of fake investment apps, noting that fraudsters often promise assured returns and mimic trusted platforms to deceive users. By the time investors realise the fraud, significant financial losses have already occurred, along with a loss of confidence in digital investment ecosystems.

The initiative comes as Sebi intensifies its crackdown on unauthorised advisers, finfluencers, and fraudulent platforms. Separately, the regulator has allowed members of the Institute of Cost Accountants of India to conduct audits of research analysts and investment advisers, expanding the pool beyond existing eligible institutions.

CONTEXT

Navigating the Next Phase of Global Distribution: **Insights from Howard Davies**

As we move into Q2 2026, the global IT channel is dealing with two forces at once: sustained component shortages and a sharp shift in how AI is being deployed. Together, they are changing where value sits across the market.

For CONTEXT, and particularly with our growing footprint in India, this is not just a market shift. It's a structural change in how distribution operates and where margin is made.

A RAM shortage that is reshaping the market

The most immediate pressure point is memory. This is not a short-term supply issue. Current data suggests constraints will continue well into 2027, with a direct impact on pricing, product mix, and availability.

Vendors are prioritising higher-margin configurations, which is pushing supply away from the mid-range. As a result, average selling prices are rising while unit volumes, especially in consumer segments, remain under pressure.

For India, this creates a more complex picture. It is a price-sensitive market, but also one of the fastest growing for enterprise IT investment. The implication is clear: success will not come from moving more units, but from placing the right inventory with customers who are investing in performance and longevity.

AI is driving a different kind of demand

At the same time, AI is moving from experimentation into operations. This is no longer about content generation. AI is being embedded into workflows, security operations, and managed services. It is starting to take decisions, not just support them.

That shift is already visible in buying behaviour. Consumer demand is slowing in response to higher prices, but business demand is holding up. In many cases, it is increasing.

AI-capable hardware is no longer a discretionary upgrade. It is becoming part of core infrastructure. In India's key technology hubs, AI readiness is quickly becoming a baseline requirement rather than a differentiator.

Building a stronger view of the Indian market

Against this backdrop, CONTEXT is strengthening its focus on India through the launch of the India Distributor Panel. This is a move away from simply observing the market towards actively shaping understanding within it. The aim is to bring leading distributors together to share insight, improve transparency, and address challenges that cannot be solved in isolation.

India's distribution landscape is large and fragmented, and access to consistent, comparable data has historically been limited. By building a structured forum, we are creating a clearer view of how supply constraints, AI demand, and logistics pressures are playing out locally.

Just as importantly, the panel provides a forward-looking perspective. It allows us to assess how allocation decisions are made, how risk is managed, and how the Indian channel positions itself within a global supply chain that is becoming more selective.

A shift from volume to value

The underlying direction is clear. The channel is no longer driven by volume alone. Value is shifting towards those who can interpret demand, anticipate constraints, and align supply with where margin sits. For vendors, that means stronger control over allocation and clearer positioning around performance and AI capability. For distributors, it means using data to guide decisions rather than relying on scale.

CONTEXT's role is to make those shifts visible. Through our data and through initiatives like the India Distributor Panel, we are helping partners see where the pressure is building and where the opportunity sits. India is not just participating in this change. It is becoming a central part of it. The next two years will reward those who adjust early.

About Howard Davies

Howard Davies is the CEO and Co-Founder of CONTEXT, the world's leading IT market intelligence company. With over 30 years of experience in the channel, Howard is a frequent commentator on the intersection of macroeconomic trends and technology distribution. CONTEXT has expanded its footprint across Europe, Asia, and the Americas, providing data that powers the world's largest IT vendors and distributors.

Redington signs landmark five-year strategic collaboration with AWS India

Redington has signed a five-year Strategic Collaboration Agreement (SCA) with Amazon Web Services India, one of the largest in the Asia Pacific and Japan (APJ) region. The partnership comes as enterprises accelerate cloud migration and explore generative AI to modernize applications, improve efficiency, and develop new digital services.

The SCA positions Redington as a key orchestrator in technology ecosystems, expanding its role in cloud, managed services, ISV, and AI solutions. It includes establishing a Generative AI Customer Experience Center, enabling business leaders to explore production-ready AI use cases, while developers gain access to AI-powered development environments. Redington will also enhance Greenfield adoption, public sector engagement, and partner capabilities across India and APJ.

To support execution, Redington will set up a dedicated Migration and Modernization CoE in Hyderabad and expand VMware modernization initiatives. Both companies aim to accelerate generative AI adoption, streamline AWS Marketplace usage, and create scalable, repeatable partner programs, delivering measurable business outcomes across enterprise, startup, and public sector segments.

Govt unveils AI skilling programme in partnership with Google and YouTube

The Ministry of Information and Broadcasting has launched a nationwide AI skilling initiative to train 15,000 professionals and students in animation, visual effects, gaming, comics, and media technology. Union Minister Ashwini Vaishnaw said the programme aims to build future-ready talent and strengthen India's position in global digital content creation.

The programme, led by the Indian Institute of Creative Technologies in collaboration with Google and YouTube, will provide a curriculum blending advanced AI tools with creative production techniques. It builds on the "Create with AI" initiative, offering participants practical skills in digital storytelling, gaming, and content creation workflows.

Rolled out in two phases through 2026, the first phase focuses on foundational AI literacy with scholarships for Google Career Certificates, while the second phase offers project-based, hands-on training across major creative hubs. Participants will learn AI tools like Gemini and Vertex AI, enhancing productivity and innovation in media production.

Dell expands AI portfolio as AI Factory with NVIDIA marks two years

Dell Technologies has expanded its enterprise AI portfolio as its AI Factory with NVIDIA completes two years. The company said over 4,000 customers have adopted the platform, with some reporting up to 2.6x return on investment, signalling a shift from AI pilots to large-scale deployments.

Dell introduced updates to its AI data platform to help enterprises manage and activate large datasets for advanced use cases. It also expanded infrastructure offerings, including AI workstations, advanced servers, and liquid-cooled systems designed for high-performance workloads across environments.

The company also unveiled new AI solutions and services to simplify deployment and accelerate outcomes. With modular architectures and automation tools, Dell aims to help organisations scale AI initiatives efficiently, supporting the development of robust, future-ready AI ecosystems.

Altos launches 'Make in India' AI server portfolio to boost local infrastructure

Altos Computing, a subsidiary of Acer, has unveiled its 'Make in India' AI server portfolio to support the country's growing demand for advanced computing infrastructure. The launch features the flagship BrainSphere R300 AI Series Server, designed for high-performance workloads across enterprises, research institutions, government bodies, and data centres.

The R300 series offers high-density GPU support, scalable memory, and enhanced thermal efficiency to handle AI model training and inference. The move highlights Altos' focus on local manufacturing, enabling faster deployment and improved accessibility of AI infrastructure in India while supporting the 'Make in India' initiative.

The company also showcased additional solutions, including the R370 and R680 AI servers, alongside real-world AI applications such as predictive analytics and smart manufacturing. The initiative aims to strengthen India's AI ecosystem by empowering enterprises, startups, and public sector organisations with scalable, high-performance computing capabilities.

India weighs multi-ministry powers to speed up online content takedowns

India is considering a policy shift to strengthen action against harmful online content by expanding takedown powers beyond the Ministry of Electronics and Information Technology (MeitY). The move comes amid rising concerns over misinformation, illegal content, and AI-driven deepfakes, with the government aiming to improve response time and enforcement.

Under the proposal, ministries such as Defence, External Affairs, and Home Affairs may be authorised to directly issue takedown orders to social media platforms. This would decentralise powers currently held under Section 69A of the IT Act, enabling quicker action, particularly in sensitive and security-related cases.

The plan, still under discussion, may be implemented through amendments to IT Rules. It follows recent mandates requiring platforms to remove unlawful content within three hours and label AI-generated material, signalling a push for stronger digital governance and accountability.

RAH Infotech partners with PointGuard AI to strengthen AI security in India

RAH Infotech has announced a strategic collaboration with PointGuard AI, a Silicon Valley innovator in AI security and application posture management. The partnership aims to accelerate secure adoption of AI, autonomous systems, and modern application security technologies across enterprise, government, and emerging tech sectors in India.

PointGuard AI provides comprehensive visibility and governance for AI systems, datasets, and connected applications, while enforcing policy guardrails, prioritizing risks, and automating remediation. Ashok Kumar, MD and Founder of RAH Infotech, said the collaboration equips businesses with scalable solutions to secure AI-driven transformations and ensure compliance across complex digital environments.

Pravin Kothari, Founder and CEO of PointGuard AI, added that the partnership combines advanced AI security with RAH Infotech's regional expertise, enabling organizations to adopt AI responsibly. Together, they aim to deliver secure, compliant, and accountable AI deployments while empowering enterprises and channel partners across India's evolving digital landscape.

DELL Technologies AMD

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 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.

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
Mobile : +91 86579 78028 | Email ID: Dell.amd@rptechindia.com

Dell introduces new commercial PC portfolio with new sleek and powerful designs

Dell Technologies has introduced a transformed commercial portfolio spanning Dell Pro notebooks, Dell Pro Precision workstations, desktops, monitors and client peripherals. Thinner, lighter and more powerful, the new lineup brings a bold, refined design language to commercial devices—prioritizing sleeker silhouettes, premium materials and modern details that elevate everyday productivity. With advances in cooling, power efficiency and support for on-device AI, the portfolio delivers improved performance and long battery life in more portable form factors, enabling a consistent, elevated experience for everyone from frontline workers to senior executives.

Users want sleek, powerful devices. IT needs security, manageability and budget discipline. Dell's reimagined commercial portfolio delivers both. Advanced engineering—modular architecture, improved thermals, AI-ready silicon—allows thinner, lighter designs that maintain enterprise-grade performance and control. Organizations can now deploy modern hardware that professionals prefer without compromising on the standards IT demands.

Check Point launches AI Defense Plane to secure the agentic enterprise at scale

Check Point Software Technologies has announced the Check Point AI Defense Plane, a unified AI security control plane designed to help enterprises govern how AI is connected, deployed, and operated across the business. As AI systems move from assistants to autonomous actors that access data, invoke tools, and take action, the AI Defense Plane provides the intelligence layer needed to secure the agentic era.

"The enterprise is entering the agentic era. AI is no longer limited to generating content. It is beginning to access systems, use tools, chain actions, and operate with increasing autonomy. That changes the security model," said David Haber, VP, AI Security at Check Point Software Technologies. "The challenge is no longer just what AI says, but what AI can do. Organizations need more than model safety. They need runtime control over how AI behaves inside real environments. The AI Defense Plane provides that control across employees, applications, and AI agents."

Tenable introduces Hexa AI engine to drive faster security outcomes and risk reduction

Tenable has announced Tenable Hexa AI, the agentic AI engine of the Tenable One Exposure Management Platform that automates security workflows and transforms exposure intelligence into coordinated action to reduce cyber risk. AI-powered cyberattacks, rapid vulnerability discovery and the explosion of AI-driven tools are expanding the attack surface faster than security teams can keep up.

Tenable Hexa AI is the orchestration engine inside the Tenable One platform that turns exposure intelligence into coordinated action. Powered by Tenable's Exposure Data Fabric, the industry's most comprehensive repository of contextualised exposure data and intelligence, Tenable Hexa AI understands how vulnerabilities, identities, assets, configurations and AI systems interact across the modern attack surface. This authoritative context enables Tenable Hexa AI to determine what matters most, validate the real state of the environment and orchestrate the steps required to minimise exposures. The result is a security operation that moves beyond reactive response to consistent, machine-speed risk reduction.

Arm unveils 'AGI CPU', signaling major shift toward in-house chip manufacturing

Arm Holdings has introduced a new artificial intelligence-focused data center processor, marking a decisive move beyond its traditional licensing business and into full-scale chip production. The processor, dubbed the AGI CPU, is designed to support emerging "agentic AI" systems—software capable of independently carrying out tasks with minimal human intervention. This represents a shift from conventional AI models that primarily respond to user prompts, such as chatbots.

The announcement reflects a broader surge in demand for high-performance computing infrastructure, particularly central processing units from firms like Intel and Advanced Micro Devices, as enterprises race to deploy more autonomous AI systems. The launch of the AGI CPU marks the company's first major step into designing and producing its own chips, a capital-intensive effort that can cost hundreds of millions of dollars. The initiative follows earlier signals from Arm that it was investing heavily in internal chip development and recruiting experienced leadership to support the transition.

Lenovo unveils 2.6kg premium keyboard

Lenovo introduced the Yoga Creative Keyboard AngryMiao Edition, a mechanical keyboard that stands out for one reason above all: weight. Tipping the scales at 2.6 kg (about 5.7 pounds), the device is built for maximum stability and a firmly "planted" typing experience. Designed in collaboration with Angry Miao, the keyboard features a high-density aluminum base and a frosted polycarbonate top plate. The heavy construction minimizes movement during intense typing or creative sessions, appealing to users who value precision and tactile feedback. Its 98-key layout offers near full-size functionality while remaining more compact than a traditional 104-key keyboard.

A defining visual element is the oversized control knob positioned at the top right. Primarily intended for precise volume control, the knob adds a tactile, premium feel aimed at creative professionals and hardware enthusiasts who appreciate physical controls over touch-based adjustments.

CrowdStrike launches the Charlotte AI AgentWorks Ecosystem for building secure agents

CrowdStrike introduced the Charlotte AI AgentWorks Ecosystem in collaboration with launch partners including Accenture, Amazon Web Services (AWS), Anthropic, Deloitte, Kroll, NVIDIA, OpenAI, Salesforce, and Telefónica Tech. The ecosystem enables customers to leverage CrowdStrike's no-code development platform and frontier AI models to securely build, orchestrate, and scale custom security agents, while opening new opportunities for partners to create agentic security businesses on the Falcon platform. Without writing a single line of code, Charlotte AI AgentWorks enables every security team to build, test, and deploy custom agents directly in the Falcon platform with enterprise-grade security and governance.

"AgentWorks enables every Falcon user to build their own agentic security workforce," said Daniel Bernard, chief business officer at CrowdStrike. "The future of security operations isn't humans replaced by agents. Its humans amplified by them. Our ecosystem makes the next-generation of security's workforce available for organizations of all sizes today."

Apple unveils new MacBook Neo

Apple has unveiled MacBook Neo, an all-new laptop that delivers the magic of the Mac at a breakthrough price, making it even more accessible to millions of people around the world. MacBook Neo starts with a beautiful Apple design, featuring a durable aluminium enclosure in an array of gorgeous colours — blush, indigo, silver, and a fresh new citrus. Its stunning 13-inch Liquid Retina display brings websites, photos, videos, and apps to life with high resolution and brightness, and support for 1 billion colors.

Powered by A18 Pro, MacBook Neo can fly through everyday tasks, from browsing the web and streaming content, to editing photos, exploring creative hobbies, or using AI capabilities across apps. In fact, it's up to 50 percent faster for everyday tasks like web browsing and up to 3x faster when running on-device AI workloads like applying advanced effects to photos, compared to the bestselling PC with the latest shipping Intel Core Ultra 5.

Palo Alto Networks introduces the most secure workspace for small business

Palo Alto Networks has announced the launch of Prisma Browser for Business, the most secure workspace for small business. This new offering enables small business owners to easily configure and manage the apps and AI tools their business relies on, while allowing employees to work securely from any device, anywhere. Prisma Browser for Business also protects against phishing, ransomware and fraud threats and provides built-in AI controls to prevent business information from ending up in the wrong hands.

Today, small businesses depend on an average of 36 applications running in the browser, which is where most work gets done. However, with 95% of companies experiencing a security incident originating in the browser, the need for a secure workspace has never been greater. At the same time, employees are rapidly adopting AI, making it harder than ever for small businesses to tame the workspace chaos, keep their business protected and prevent unintended AI actions.

Oracle unveils AI Database agentic innovations for business data

Oracle has announced new agentic AI innovations for Oracle AI Database that will help customers rapidly build, deploy, and scale secure agentic AI applications that are suitable for full-scale production workloads. Oracle AI Database architects agentic AI and data together across operational databases and analytic lakehouses.

"The next wave of enterprise AI will be defined by customers' ability to use AI in business-critical production systems to safely deliver breakthrough innovations, insights, and productivity," said Juan Loaiza, executive vice president, Oracle Database Technologies, Oracle. "With Oracle AI Database, customers don't just store data, they activate it for AI. By architecting AI and data together, we help customers quickly build and manage agentic AI applications that can securely query and act on real-time enterprise data with stock exchange-level robustness in every leading cloud and on-premises."

SentinelOne unveils new AI security offerings to give defenders a decisive advantage

SentinelOne has just revealed a new line up of AI security offerings, all designed to give defenders a decisive advantage. Covering both security for AI and the use of AI to automate and transform security operations, the new offerings build on SentinelOne's market-leading AI security portfolio. From securing autonomous agents to executing full agentic investigations with a single click of a button.

As organizations race to embrace AI to speed innovation, scale operations and boost productivity, AI itself has become the new attack surface and primary source of risk. Not surprisingly, Gartner has reported that AI cybersecurity – defined as both securing AI and AI-amplified security – will be amongst the most significant and fastest growing markets in all AI spend over the next few years. In a January 2026 forecast, Gartner projected that AI cybersecurity spend will grow at an impressive 73.9% CAGR from 2024-2029, more than double that of AI spend overall.

Qualys debuts industry's first AI agent

Qualys has launched Agent Val within Enterprise TruRisk Management (ETM) to bring safe, agent-led exploit validation and autonomous risk remediation to the Risk Operations Center (ROC). Agent Val represents a fundamental shift in vulnerability and exposure management from assumption-driven prioritization to evidence-based execution, accelerating response, reducing wasted effort, and delivering measurable reductions to cyber risk.

Research shows that known exploited vulnerability volume has grown 6.5 times in the past four years, while the percentage of critical vulnerabilities still open at Day 7 has increased — proof that manual remediation has hit a hard ceiling. To make matters worse, the time to exploit has now shrunk to minus one day, meaning attackers are exploiting them before patches exist. For CISOs, the challenge is closing the gap between vulnerabilities that look severe on paper and those truly exploitable in production environments, so teams are not wasting valuable time remediating low-impact issues and missing other dangerous exposures.

Panasonic launches SIP based Video Intercom System

Panasonic has launched its new VL-VQ Series SIP based IP Video Intercom System in India, aimed at enhancing security, communication, and access management across modern residential and large-scale housing projects. With the rapid expansion of gated communities, high-rise apartments, and integrated townships across urban India, the need for intelligent and scalable security solutions has become increasingly critical. Addressing this evolving demand, the new system offers three-layered security through a unified platform that manages multiple access and communication touchpoints with centralized control through Panasonic's Center Management Software (CMS), enabling smarter and more efficient residential security management.

Designed for apartments, gated communities, and large-scale housing projects, the VL-VQ Series goes beyond a standard video door phone by enabling a three-layered security framework across residences, building entrances, and central security operations.

MediaTek to support wireless emergency alert messages via satcom with Starlink Mobile

MediaTek is collaborating with Starlink to support wireless emergency alert messages via satellite communication. Through this joint effort, more mobile users worldwide will be able to receive alerts from the Commercial Mobile Alert System (CMAS), Wireless Emergency Alerts (WEA) framework, and the Earthquake and Tsunami Warning System (ETWS), providing critical communications during natural disasters or other potential life-threatening situations.

At Mobile World Congress 2026, MediaTek demonstrated the Starlink Mobile service on a device powered by the MediaTek M90, the world's first 5G modem with integrated satellite technology. Direct to Cell utilizes the S-Band to ensure consumers can use their mobile devices to be informed of emergencies in a timely manner, anywhere in the world. The collaboration has already enabled WEA services in the United States, Canada and Japan, and more than 4.4 million people have connected to Starlink Mobile during emergencies.

Airtel and Google to advance spam protection in India with secure RCS messaging

Bharti Airtel and Google have announced a collaboration to offer a secure and engaging messaging experience for millions of users in India. By combining Airtel's network intelligence with Google's Rich Communications Services (RCS) platform and spam filtering, users get to experience RCS messaging with high-quality photo/video and interactive elements like message reactions, all while benefiting from enhanced protections that significantly reduce mobile spam and digital fraud.

Over the last 1.5 years, Airtel has led India's fight against spam and digital fraud through a series of industry-first, AI-powered initiatives aimed at protecting customers across calls and messages. Proving a track record in protecting customers, Airtel has, to date, through all its innovative spam fighting initiatives, blocked a staggering 71 billion spam calls and 2.9 billion spam SMSes that has led to a huge 68.7% decrease in the value of financial losses on its network.

VIAVI launches test platform for 1.6T ethernet networks

Viavi Solutions has introduced the TestCenter D2 1.6T Appliance, a new testing platform designed to support the development and deployment of next-generation high-speed Ethernet networks. The system is aimed at cloud providers, hyperscalers, emerging cloud infrastructure companies and network equipment manufacturers working on advanced data centre and AI network architectures. The appliance forms part of VIAVI's broader portfolio of network testing solutions covering multiple layers of network validation, including physical layer testing, AI fabric validation and performance testing for complex network environments.

The launch comes at a time when the networking industry is preparing for a transition from 800G to 1.6T Ethernet technologies, particularly in infrastructure supporting artificial intelligence workloads. The shift is expected to gather momentum this year as cloud service providers build larger and more complex AI clusters to handle growing computational demands.

Vi 5G goes live at The Golden Temple in Amritsar

Vi has announced the launch of its 5G services at the iconic Golden Temple in Amritsar, further expanding its 5G footprint in Punjab. The rollout is designed to support seamless high-speed connectivity in a location that sees over 1.5 lakh devotees and visitors every day. As one of the most visited religious shrines globally and home to the world's largest community kitchen (Langar), the Golden Temple witnesses extremely high footfall, resulting in significant data demand within a concentrated area.

To manage this heavy network traffic load and ensure stable, high-speed connectivity even during peak hours, Vi has undertaken focused network augmentation and deployed dedicated 5G infrastructure within and around the Golden Temple premises. With this targeted network densification, Vi users visiting Golden Temple- Amritsar, can experience enhanced mobile broadband speeds, lower latency and more reliable connectivity, and everyday mobile usage in a high-footfall environment.

HPE expands NVIDIA AI portfolio to accelerate large-scale AI and supercomputing

Hewlett Packard Enterprise (HPE) has expanded its AI Computing portfolio with NVIDIA, introducing new innovations aimed at large-scale AI factories and supercomputing environments. The full-stack solutions combine compute, GPUs, networking, liquid cooling, software, and services to enable faster deployment and improved time-to-insight for enterprises and research institutions.

The company has enhanced its HPE Cray Supercomputing GX5000 platform with NVIDIA Vera CPU-based compute blades and advanced networking options such as Quantum-X800 InfiniBand. These upgrades are designed to support intensive AI and high-performance computing workloads, helping organisations scale efficiently while accelerating scientific discovery and innovation.

HPE has also strengthened its AI Factory portfolio with next-generation systems based on NVIDIA Vera Rubin and Blackwell architectures. New high-density GPU servers, expanded multi-tenancy capabilities, and integrated software solutions aim to streamline deployment, improve efficiency, and support sovereign as well as enterprise AI environments.

Broadcom announces VMware Telco Cloud Platform 9 for sovereign-ready telco infrastructure

Broadcom has unveiled the future of VMware Telco Cloud Platform, a private cloud platform for telco data centers designed to help global telco operators drive greater hardware efficiency and lower operational costs when delivering sovereign and AI services. VMware Telco Cloud Platform 9, built on VMware Cloud Foundation 9 with its own additional telco specific capabilities, will empower telcos with a unified and horizontal infrastructure foundation.

"Hardware costs are spiraling out of control, and the global demand for memory resulting from AI will further accelerate rising server prices. VMware Telco Cloud Platform, built on the industry's most widely-deployed private cloud platform technology, helps telcos dramatically reduce both their CAPEX and OPEX," said Paul Turner, chief product officer, VMware Cloud Foundation Division, Broadcom. "VMware Telco Cloud Platform 9 will empower telco operators to deliver the secure, sovereign, AI-native infrastructure that drives next-gen technology adoption, revenue acceleration and lowers costs."

PRAMA showcases smart and safe city solutions at Municipalika 2026

Prama India participated in the 18th edition of 'Municipalika-2026', highlighting its advanced smart city and safe city solutions for urban governance bodies. Held from February 25–27 at Bharat Mandapam in New Delhi, the event was inaugurated by Manohar Lal Khattar, the Union Minister for Housing, Power and Urban Affairs. Recognised as one of India's largest platforms for sustainable urban

development, the exhibition attracted policymakers, urban planners, and technology providers. Prama India's booth witnessed strong engagement from stakeholders across infrastructure, housing, and smart city ecosystems.

The company showcased a wide portfolio of solutions, including Integrated Command & Control Centres, AISense Technology, transportation systems, mobile enforcement tools, and network infrastructure. A company spokesperson said the platform enabled the firm to present innovative, 'Made-in-India' solutions aligned with the Smart City Mission and Safe City initiatives, reinforcing its commitment to urban security and efficiency.

Prama India also contributed to knowledge sessions at the event. Representatives shared insights on city resilience, surveillance, and disaster response during panel discussions and conferences. With participation from multiple countries, states, and cities, Municipalika 2026 served as a key networking and knowledge-sharing platform for addressing emerging urban challenges.

Ingram Micro's Sanjib Sahoo honoured at World Leaders Summit for AI-driven transformation

Sanjib Sahoo, President of the Global Platform Group at Ingram Micro, has been recognised as a "Global Icon for AI, Platform & Business Transformation" at the World Leaders Summit 2026, held at the Library of Congress in Washington D.C. The honour highlights his role in advancing AI-driven platforms that are transforming global business operations and enabling measurable outcomes through technology-led innovation.

At the summit, which brought together global policymakers, industry leaders, and innovators, Sahoo delivered a keynote on the evolving role of artificial intelligence in global commerce. He emphasised that organisations must focus on solving business challenges rather than adopting technology in isolation, while also highlighting the importance of human-centric transformation. His address underscored how AI is rapidly becoming a foundational layer for decision-making, operational models, and economic systems worldwide.

Sahoo was also recognised for his leadership in developing Xvantage, Ingram Micro's AI-powered digital platform designed to streamline complex workflows using advanced data and machine learning models. He noted that meaningful transformation requires purpose and mindset alongside technology. The award, part of the World Leadership Legacy Series, honours leaders shaping the future of industries and global collaboration.

BMC Helix hosts SPEX 2026, showcases agentic AI vision to global partners

BMC Helix brought together over 75 leaders from top global system integrators at SPEX — Service Provider Exchange 2026 in Phuket. The invite-only event saw participation from partners across India, Malaysia, Singapore, the US, and the Netherlands. It served as a platform to present the company's latest innovations, including its agentic AI roadmap, while strengthening collaboration within its global partner ecosystem.

At the event, company leaders highlighted the growing importance of intelligent and autonomous operations in modern enterprises. The discussions focused on how agentic AI is enabling organisations to move towards self-optimising systems and improved service delivery. SPEX 2026 also marked a significant milestone following the separation of BMC Helix from BMC, reinforcing its positioning as an independent player in IT Service Management and AIOps.

The event featured training sessions, hands-on labs, and product demonstrations, offering partners direct exposure to evolving capabilities. Attendees included representatives from leading firms such as Infosys, TCS, and Accenture. SPEX 2026 concluded with an awards ceremony recognising partner achievements and contributions over the past year.

Sonata Software earns Microsoft Frontier Partner badge for AI-led innovation

Sonata Software has been recognised as a Microsoft Frontier Partner, reinforcing its position as an AI-first modernisation engineering firm. The recognition highlights the company's ability to deliver a human-led, AI-driven approach across cloud, AI platforms, business solutions, and security. A long-standing partner of Microsoft, Sonata continues to support enterprises in scaling digital transformation through advanced AI capabilities and innovative solutions.

The Microsoft Frontier Partner badge is awarded to organisations demonstrating excellence across multiple cloud and AI domains. It recognises partners building cutting-edge solutions using technologies such as AI, Copilot, and agentic architectures to transform business processes and employee experiences. Rajsekhar Datta Roy, Chief Technology Officer at Sonata Software, said the recognition reflects the company's strong investments in Microsoft AI ecosystems and its focus on enabling enterprises to accelerate AI adoption and achieve measurable outcomes.

Anthony Lange, Chief Revenue Officer at Sonata Software, said the recognition strengthens Sonata's position as a trusted growth partner. The company continues to expand its portfolio with offerings such as Harmoni.AI and AgentBridge, supporting responsible AI adoption and workflow automation. With multiple advanced specialisations, Sonata Software remains aligned with Microsoft's AI-first vision for global enterprises.

Keysight to start local manufacturing in India to boost innovation ecosystem

Keysight Technologies has announced plans to begin local manufacturing in India, expanding its global production footprint to serve mission-critical sectors. The move will help deliver advanced test and measurement solutions more efficiently to industries such as aerospace, defense, government research, and academia. It also aims to simplify procurement and strengthen support for existing customers in the country.

The expansion comes as India's electronics manufacturing sector is projected to cross $300 billion by 2026, driven by rising demand for advanced technologies. Keysight's phased rollout will focus on producing test equipment for both domestic and global markets, while improving supply chain resilience. The initiative aligns with national programs like Make in India and Semicon India.

The facility will support key areas including semiconductors, quantum technologies, aerospace and defense, and next-generation AI and wireless systems, reinforcing India's growing role as a global innovation hub.

Sandisk invests $1 billion in Nanya to strengthen chip market position

Sandisk is expanding its footprint in the semiconductor space with a $1 billion equity investment in Taiwan-based memory manufacturer Nanya Technology. The deal involves acquiring nearly 139 million newly issued shares through a private placement, giving Sandisk a minority stake of just under 4% in the Taiwanese firm. The investment is part of a broader strategic collaboration between the two companies.

The move comes as demand for memory chips surges, driven by artificial intelligence, cloud computing, and data-heavy applications. Industry leaders like Samsung Electronics and SK Hynix continue to dominate the competitive landscape.

With global tech firms expected to ramp up investments in computing capacity, demand for advanced memory solutions such as DRAM and NAND is set to rise, intensifying pressure on chip production.

World's first quantum battery prototype marks energy breakthrough

Australian researchers at CSIRO have created the world's first proof-of-concept quantum battery, marking a breakthrough in next-generation energy storage. Led by James Quach, the prototype was wirelessly charged using a laser and successfully completed a full cycle of charging, storing, and discharging energy—demonstrating all key battery functions in a single device.

Quantum batteries, first proposed in 2013, use principles of quantum mechanics to enable ultra-fast charging through collective interactions between cells. The new prototype builds on earlier research and can now release stored energy, charging in femtoseconds and holding energy briefly. However, its current capacity remains extremely small, far from practical use in consumer devices.

Despite early limitations, the technology could enable wireless energy transfer for drones, sensors, and electric vehicles. Researchers will now focus on scaling capacity and extending storage duration to support real-world applications.

ChatGPT gets new Library feature to store and reuse files

OpenAI has introduced a new "Library" feature for ChatGPT, designed to help users store and manage files created or shared during conversations. The feature is rolling out globally for Plus, Pro, and Business users, excluding select European regions, and aims to offer a centralized space for documents, images, spreadsheets, and more.

Currently available on the web version, the Library appears in the sidebar, allowing users to organise, search, and reuse files easily. Files are automatically saved, and users can access them using the "Add from Library" option during chats. However, temporary chats are excluded, and generated images remain in a separate tab.

OpenAI said users retain full control, with options to delete files anytime, which are permanently removed within 30 days. File size limits include 512MB for documents and 20MB for images, with privacy settings allowing users to manage data usage preferences.

HP unveils NearSense to enable seamless cross-device connectivity

HP has introduced NearSense, a new cross-device connectivity solution, at HP Imagine 2026 to improve interoperability between PCs, Android devices, and workplace hardware. Developed in collaboration with Google, the solution is built on an extended Device-to-Device Infrastructure framework, enabling seamless data transfer without cables, cloud services, or manual pairing, with a focus on improving productivity.

NearSense allows nearby devices to automatically discover and connect, enabling real-time file sharing through simple actions like drag-and-drop. It also uses contextual awareness to detect proximity, helping users switch between devices and tasks more smoothly. Features include PC-to-PC sharing, meeting room access, content casting, and simplified printing without drivers.

The feature will debut on select HP AI PCs in Spring 2026 and expand across desktops, printers, and conferencing systems later in the year, supporting broader ecosystem integration.

Samsung plans $73 billion investment to lead AI chip race

Samsung Electronics has announced plans to invest over 110 trillion won, or about $73 billion, in 2026 to boost semiconductor innovation and expand into AI-driven technologies. The move is part of its strategy to strengthen its global chip leadership by building a comprehensive ecosystem across memory, foundry, and advanced packaging.

A significant portion of the investment will focus on high-performance memory, especially high bandwidth memory, which is critical for AI workloads. As competition intensifies, Samsung aims to position itself as a full-stack semiconductor provider, delivering integrated solutions for next-generation computing and data processing needs.

Beyond chips, Samsung is exploring growth in robotics and potential acquisitions in sectors like medical technology, automotive electronics, and HVAC. The company also reaffirmed its commitment to shareholder returns through dividends and buybacks, while targeting long-term growth in AI-led markets.

RP tech

Rashi Peripherals Limited

Now Listed on NSE and BSE

Incorporated in 1989, Rashi Peripherals Limited is among the leading national distribution partners for global technology brands in India for information and communications technology ("ICT") products in terms of revenues and distribution network. With a pan India distribution network of 52 branches, 50 service centers and 68 warehouses, we cater to the technology requirements of 10225 customers in 708 locations across India.

36 Years of Experience

70 Global Technology Brands

10,255 Customers

708 Locations

52 Branches

68 Warehouses

23.5% CAGR FY 21-25

www.rptechindia.com

Foxconn and SAP join forces to accelerate enterprise AI adoption in APAC

Foxconn (Hon Hai Technology Group) has partnered with SAP SE to drive next-generation enterprise AI adoption across the Asia-Pacific region. Announced at NVIDIA GTC 2026, the collaboration builds on Foxconn's AI Factory initiative, aimed at transforming manufacturing and supply chain operations while enabling faster deployment of AI-driven solutions across industries.

The partnership will combine Foxconn's AI computing capabilities with SAP's enterprise software expertise to accelerate go-to-market strategies and support digital transformation. It will also explore new use cases in Physical AI, smart manufacturing, and supply chain management, helping organisations improve efficiency, scalability, and operational performance.

Both companies aim to create a blueprint for AI-powered manufacturing by integrating enterprise intelligence with advanced AI infrastructure. The collaboration is expected to help businesses in the region adopt AI more effectively and unlock new opportunities in the evolving industrial landscape.

New Relic to open first Japan data center to meet data residency needs

New Relic has announced plans to launch its first data center in Japan, marking a strategic expansion to better serve local customers. Scheduled to go live in Tokyo in July 2026, the facility aims to address data residency needs while enhancing performance and governance for enterprises operating in highly regulated sectors.

The new data center will enable domestic data collection, storage, and processing, ensuring compliance with Japan's strict security and privacy requirements. It will also offer ultra-low latency, allowing businesses to gain real-time insights and make faster decisions. Industries such as finance, manufacturing, and telecommunications are expected to benefit from improved observability capabilities.

Japan remains a key growth market for New Relic, with rising demand across sectors including public services and infrastructure. The company said the investment will strengthen its presence in the region and support enterprises in accelerating digital transformation while maintaining high standards of data control and compliance.

Micron sees surge in revenue on soaring AI memory demand

Micron Technology has reported a sharp surge in performance, with revenue nearly quadrupling in its latest quarter, driven by strong demand for memory used in artificial intelligence systems. The company has stood out among major U.S. tech firms, supported by rising demand for high-performance memory powering advanced AI chips, including those from Nvidia.

The growth reflects increasing demand for DRAM and NAND memory, as supply constraints continue across data centers and AI workloads. Micron expects revenue to exceed $33 billion this year, significantly outperforming earlier projections. Profitability has also improved, with margins rising due to stronger pricing and a shift toward high-bandwidth memory solutions.

The company is seeing strong momentum across cloud, mobile, and client segments, while investing in expanding production capacity. With AI driving memory-intensive computing, Micron aims to strengthen its role as a key enabler of next-generation technology growth.

Trump administration proposes national AI policy to replace state rules

The Donald Trump administration in the US has unveiled a legislative framework to establish a single national policy on artificial intelligence, aiming to create uniform safety and security standards while limiting state-level regulations. The proposal outlines measures covering AI products and infrastructure, including child safety rules, data center permitting and energy use, and protections for political expression.

The plan also calls on Congress to address intellectual property challenges and prevent misuse of AI for censorship. Officials said the administration aims to turn the framework into law within the year, with Donald Trump expected to sign the bill. However, gaining bipartisan support could be challenging in a divided Congress.

The move comes as states like California and New York push their own AI rules. Industry leaders have opposed such efforts, warning that a fragmented regulatory approach could slow innovation and impact global competitiveness.

Nvidia launches NemoClaw to secure enterprise AI agent deployment

Nvidia has introduced NemoClaw, an enterprise AI agent platform designed to enhance security and control as businesses scale AI adoption. Built on the OpenClaw framework, the platform addresses growing concerns around data leakage, unauthorized actions, and system vulnerabilities by offering a more governed environment for deploying AI agents.

NemoClaw introduces policy-driven execution, enabling organisations to define strict rules around data access, permissions, and agent actions. It also offers full-stack observability, allowing enterprises to track decision-making processes and data usage. These features are especially critical for sectors like banking, healthcare, and government, where compliance and transparency are essential.

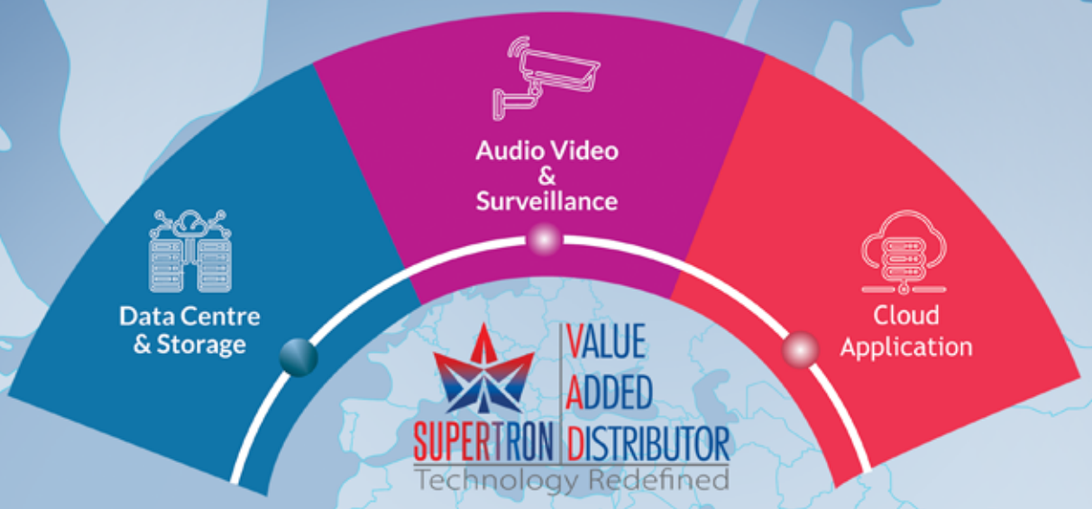
By integrating with Nvidia's broader AI ecosystem, including GPUs and software frameworks, NemoClaw is optimised for performance and scalability. The platform positions Nvidia as a full-stack AI provider, bridging the gap between rapid AI adoption and the need for stronger security and governance.

Alibaba launches 'Wukong' AI agent platform as China's AI race intensifies

Alibaba Group has introduced Wukong, a new enterprise-focused AI platform aimed at automating complex business workflows. Currently in invitation-only beta, the platform enables multiple AI agents to coordinate tasks such as document editing, spreadsheet management, meeting transcription, and research within a single interface.

Developed under Alibaba's new Alibaba Token Hub, Wukong is positioned as a flagship offering in the company's push into enterprise AI. It is available as a desktop application and integrates with tools like DingTalk, as well as platforms such as Slack, Microsoft Teams, and WeChat to streamline workplace productivity.

The launch comes amid rising competition in China's AI agent market, with companies like ByteDance and Tencent entering the space. While adoption is accelerating, regulators have raised concerns over potential security risks associated with AI-driven automation.



VALUE ADDED DISTRIBUTOR
SUPERTRON
Technology Redefined

Empowering Patnerships
Enhancing Growth
Endless Possibilities

KEY DIFFERENTIATOR

Value: Consulting Approach | Solution Design | CoE Center | Proof of Concept (PoC) Capabilities

Expertise: Pro AV & Surveillance | Data Storage | Cloud Application

Success: 100% Partner Centric Model

AVer™ KanexPro Motorola Solutions Elite Distributor Motorola Solutions Avigilon axxonsoft Infortrend PROMISE TECHNOLOGY

TELTONIKA ManageEngine protean Virtuozzo Vigyanlabs HALO SMART SENSOR WAVE PTX PELCO

Supertron Electronics Pvt. Ltd. (Value Added Distribution Venture)

701 7th Floor, Icon 351, Western Express Highway, ICICI Bank, Andheri East, Mumbai, Maharashtra - 400069,
Ph: 9147377795, Toll Free:1800 5716767, Email: marketing@sevadv.com, Website: www.sevadv.com

RSAC 2026: Unity in the Age of AI

The RSA Conference 2026 (RSAC 2026), held from March 23–26 at the Moscone Center in San Francisco, brought together nearly 44,000 attendees under the theme “Power of Community.” This year strongly highlighted the shift of AI in cybersecurity from experimentation to real-world deployment, with a growing focus on agentic AI and securing non-human identities.

RSA continues to be a cornerstone event for cybersecurity and privacy, going beyond tools to foster meaningful conversations, learning, and industry collaboration.

Techstrong once again co-located its DevOps event at RSAC, hosting a practitioner-focused seminar on the transition to AI-native development and security. Titled "AI NativeDev and the Next Evolution of DevOps," the full-day session provided a concentrated "center of gravity" within the expansive RSAC conference.

Featuring candid discussions from thought leaders like David Brin and Chenxi Wang, the event explored critical themes such as agentic development, non-determinism, and the necessity of redesigning security workflows for an AI-driven era rather than merely automating legacy tasks.RSAC this year underscored its strong emphasis on AI, alongside unexpected implications for how CISOs approach governance, organizational design, and board reporting.

Kevin Mandia of Ballistic Ventures argued for a shift toward an “AI versus AI” paradigm, where human intervention is minimized. He noted that AI agents are now embedded in red teaming operations, enabling large-scale, high-speed execution. Although AI compresses attack timelines, it also strengthens defense by automating response functions, reducing response times from five days to five minutes.

Palo Alto Networks has launched Prisma Browser for Business, a secure browser specifically designed to protect SMBs from browser-based threats, including risks associated with AI application usage. The browser features built-in defenses against phishing, ransomware, and fraud, alongside data security controls to prevent theft or leakage. According to CEO Nikesh Arora, the tool aims to simplify security decisions for smaller businesses, ensuring that secure AI adoption is accessible across the entire business landscape rather than just for large enterprises.

TOP HIGHLIGHTS:

Agentic AI & Autonomous SOC: The rise of agentic AI is transforming SOC operations from reactive to proactive, with AI agents handling triage and response.

Security for AI: Focus on securing AI systems against threats like prompt injection, over-privileged agents, and unmanaged “shadow AI.”

Non-Human Identity Governance: Increasing need to manage bots and machine identities with least-privilege and continuous monitoring.

Post-Quantum Cryptography (PQC): Urgency is growing to address quantum risks and “harvest now, decrypt later” threats.

CTEM & Risk Quantification: Shift toward prioritizing risks based on business impact rather than just technical scores.

Innovation: Geordie AI was named the most innovative startup at RSAC 2026.

KEY ANNOUNCEMENTS:

Arctic Wolf launched the Aurora Agentic SOC

Wiz (Google Cloud) introduced AI-APP for AI security

Cisco announced Zero Trust Access for AI Agents

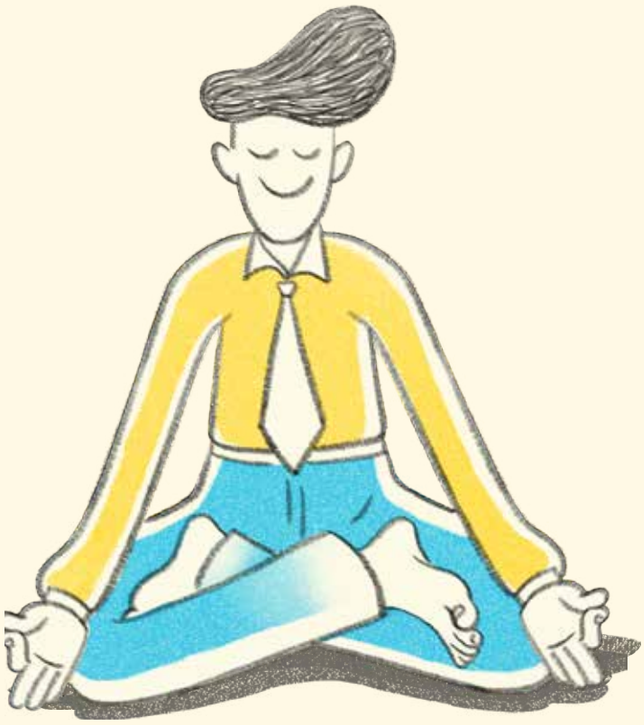
Rubrik unveiled its Semantic AI Governance Engine

FaceOff showcased a PQC-powered approach to combat deepfake and synthetic fraud

RSAC 2026 highlighted the "Power of Community," serving as a massive gathering for the cybersecurity industry. As an editorial representative for a cybersecurity events organizer, it was heartening to witness the collective energy of the field. Ultimately, the event demonstrated the enduring human need to gather and collaborate on a global scale.

Organizations are deploying AI into workflows faster than they can establish necessary rules, controls, and accountability. While these systems act with the autonomy of privileged employees—accessing data and making critical decisions—many companies lack clear policies regarding agent permissions, monitoring, and liability. Rather than advocating for a slowdown, the focus should be on implementing guardrails to mitigate avoidable security, compliance, and operational risks. In this context, governance serves to align organizational safety and reality with technical ambition.

Tally Prime 6.0



Everything tallies

with the power of PrimeBanking

- **Automated Accounting with Bank Statements**
- **Smart Bank Reconciliation**
- **Integrated Payments and Accounting**
- **Connected Banking**

Buy /Upgrade

TallyCare:
1800 309 8859/+91 80 25638240
help.tallysolutions.com | tallysolutions.com

Chat with us on **+91 90199 10043**

Hikvision Unveils Millimeter Wave Body Scanning System for Threat Detection at Security Checkpoints

Hikvision has unveiled a new millimeter wave (mmWave) body scanning security system for deployment at security checkpoints, aimed at addressing evolving threats through real-time detection and management. With security risks becoming more complex, the company highlighted the growing importance of advanced technologies such as millimeter wave scanners in strengthening safety frameworks across public and private spaces.

The newly introduced system is designed to deliver a fast, reliable, and user-friendly screening process. Hikvision said the solution enhances the effectiveness and efficiency of security measures while offering a robust layer of protection for personal safety, public infrastructure, and private property. The integration of such technology into organizational security strategies is seen as a critical step toward building safer environments.

MILLIMETER WAVE BODY SCANNER

A millimeter wave body scanner is used at security checkpoints to detect objects such as metal, plastic, ceramic, and similar materials concealed on individuals. The term "millimeter wave" refers to radio waves in the 30 to 300 GHz frequency range, positioned between microwave and infrared waves in the electromagnetic spectrum.

These wavelengths enable deep scanning through clothing to identify hidden objects. Hikvision's system provides high-resolution imaging and uses a dummy body model instead of real images to indicate threat locations, ensuring privacy protection. This approach allows security personnel to focus only on suspicious objects, improving both speed and accuracy in screening processes.

WORKING PRINCIPLE AND DETECTION CAPABILITIES

The system operates by transmitting high-frequency electromagnetic waves toward the human body and analyzing the reflected signals. These reflections are processed using specialized software to generate images and identify abnormal or potentially dangerous objects.

Millimeter wave scanners function passively, relying solely on reflected waves and avoiding the use of ionizing radiation such as X-rays. The technology supports high-resolution detection, enabling precise identification of object size and location, while scan times are typically completed within seconds—an advantage in high-traffic areas.

The system can detect a wide range of items, including metal objects like weapons, non-metal objects such as explosives or plastic devices, as well as other prohibited items including electronic devices, making it suitable for diverse security scenarios.

Aditya Khemka Honoured with Hurun Industry Achievement Award 2025–26 for Security Leadership

Aditya Khemka, Managing Director of Aditya Infotech Ltd., has been honoured with the Hurun Industry Achievement Award 2025–26 in the Electronics Surveillance & Security category at Hurun India's Most Respected Entrepreneurs' Awards. The recognition celebrates leaders who have demonstrated vision, resilience, and measurable impact in building businesses of national significance, while contributing meaningfully to industry growth.

The award highlights Khemka's role in strengthening India's electronic surveillance ecosystem and establishing CP PLUS as one of the country's most trusted and widely adopted security technology brands.

Under his leadership, Aditya Infotech Ltd. has expanded its presence across surveillance, smart security, and integrated solutions, addressing the needs of enterprises, public infrastructure, and smart city projects. The company has prioritised domestic manufacturing, localisation, and technology innovation, supported by investments in scalable production capabilities, STQC-certified product lines, and strong research and development initiatives. This approach has enabled the company to deliver advanced, reliable, and cost-effective solutions aligned with India's rapidly evolving security and surveillance requirements.

Commenting on the recognition, Aditya Khemka said, "This recognition reflects the collective effort of our teams, partners and stakeholders who have contributed to building technology solutions that address India's growing security needs. We remain committed to advancing indigenous innovation, strengthening manufacturing capabilities and delivering future-ready security solutions."

Over the years, CP PLUS has played a critical role in supporting enterprises and government-led initiatives with AI-powered surveillance systems and integrated platforms, reinforcing India's push towards self-reliance in electronics and security technologies.

CADYCE Launches CA-CSPLITTER – A Smart 2-in-1 USB-C Charging Solution for Modern Professionals

CADYCE has come up with its latest innovation, the CA-CSPLITTER (C-SPLIT), a USB-C Splitter 2-in-1 charging cable (1 meter) designed to simplify connectivity and maximize productivity. The device is engineered for modern multitasking professionals, enabling users to charge two USB-C devices simultaneously from a single power adapter.

The CA-CSPLITTER supports up to 100W power delivery and intelligently distributes power between connected devices. This allows users to charge devices such as laptops, tablets, and smartphones together without compromising performance or safety. The company said the product is aimed at reducing the need for multiple chargers while ensuring efficient power management across home, office, and travel environments.

SIMPLIFY CHARGING, AMPLIFY POWER

The C-SPLIT features built-in intelligent power distribution technology that dynamically detects connected devices and balances power output for optimal efficiency. This ensures that each device receives the precise power required. In addition to charging, the splitter supports USB 2.0 data transfer, enabling reliable data connectivity alongside power delivery.

The device offers universal compatibility with Mac OS, Windows, iOS, and Android platforms, making it suitable for a wide range of users. Its durable 1-meter cable construction is designed to provide flexibility, strength, and long-lasting performance.

BUILT FOR EFFICIENCY WITHOUT COMPROMISE

The CA-CSPLITTER features a USB-C male to dual USB-C male connector with a high-current 5A design, supporting up to 100W output. According to CADYCE, the product helps eliminate clutter by transforming a single USB-C port into a dual-charging solution.

"Today's professionals carry multiple USB-C devices. With C-SPLIT, we've created a compact yet powerful accessory that enhances productivity while maintaining safety and performance standards," a company spokesperson said.

TP-Link VIGI Cameras Secure BIS-ER Certification, Strengthening Surveillance Portfolio

TP-Link, a global leader in networking and connectivity solutions, has announced that its VIGI C340 and VIGI C440 security cameras have secured the Government of India's BIS-ER certification, marking a significant milestone for its surveillance product portfolio. The certification underscores compliance with stringent regulatory standards and places the company among a select group of manufacturers in India to achieve this benchmark for security devices.

The BIS-ER certification is a rigorous, process-oriented framework that evaluates not just the end product, but also its entire supply chain, components, and software integrity. This comprehensive assessment ensures high standards of quality, reliability, and security. According to the company, achieving this certification reflects its commitment to delivering technologically advanced surveillance solutions that meet evolving regulatory and market requirements, particularly as demand for secure and compliant systems continues to grow across sectors.

Both VIGI models are equipped with advanced features designed to address modern surveillance challenges. The VIGI C340, an outdoor full-colour bullet network camera, delivers 4MP resolution and maintains clear, detailed imaging even in low-light conditions through its high-sensitivity sensor and supplemental lighting. Meanwhile, the VIGI C440 turret camera offers intelligent detection capabilities, including human and traffic classification, along with two-way audio for remote communication. It also supports H.265+ video compression, helping reduce storage requirements while maintaining video quality, thereby enhancing overall operational efficiency and security performance.

TP-Link India, a subsidiary of US-headquartered TP-Link Systems Inc., is a global leader in networking and connectivity solutions, offering routers, switches, security cameras, and smart home devices. The company has been consistently ranked by IDC as the No. 1 provider of Wi-Fi devices, with a presence in over 170 countries. Backed by a strong focus on innovation, reliability, and performance, TP-Link continues to enable seamless connectivity for consumers and enterprises worldwide.

WIITF 2026: Reiterating the role of VARs in shap

VARINDIA once again strengthened its position as a leading platform for knowledge exchange, innovation, and networking within Western India's IT ecosystem with the successful hosting of the 16th edition of the Western India Information Technology Fair (WIITF), 2026. The VAR summit emerged as a dynamic forum for collaboration, insights, and inspiration, energizing the tech community and fostering industry growth.

The evening began with a warm welcome for guests and participants, underscoring the importance of collaboration and partnerships in the technology sector. Built around the theme, "Evolving BFSI Landscape," the summit provided a platform to explore the latest trends and innovations in IT. It also celebrated the contributions of VARs in India's ICT industry, recognizing their pivotal role in shaping the future of technology.

The summit began with the ceremonial lamp lighting, marking an auspicious start before the corporate presentations. The revered guests who graced the event included distinguished names like Abhay Mishra, Distribution Accounts Manager – Acronis; Sushil Kumar Patil, Accleration Solutions Engineer- Riverbed; Priyanka Arora, Solution Sales Lead – Microsoft; Dr. Arindam Sarkar, Chief Architect - FaceOff Technologies and Dr Deepak Kumar Sahu, Chief Editor – VARINDIA.

The keynote address was delivered by Dr. Deepak Kumar Sahu, Editor-in-chief, VARINDIA in which he highlighted the fact that India stands at a critical moment in its technology journey today, with the country building a $250 billion IT industry and becoming a global leader in software services. However, its domestic IT spending accounts for only about 1% of global technology investments. He further cited that bridging this gap will be essential if India wants to play a leading role in the emerging AI-driven economy.

The corporate presentations for the evening commenced with an insightful address by Abhay Mishra, Distribution Accounts Manager – Acronis, who spoke about data availability and integrity. With strong expertise in cybersecurity, data protection, and channel development, he spoke about

The next speaker, Sushil Kumar Patil, Accleration Solutions Engineer- Riverbed presented his valuable perspectives on how Riverbed views technology, innovation, while also elucidating the company's market growth.

Priyanka Arora, Solution Sales Lead- Microsoft was the next presenter to address the audience in which she emphasized on the growing menace of cybercrime and how cyber-attacks have grown 5x and at projected $10.5 trillion annual cost of cyber-crime, how it could become a third largest economy.

Dr. Arindam Sarkar, Chief Architect- FaceOff Technologies in his presentation specifically talked about how neuro-AI, quantum-safe cryptography, and cognitive security have become the need of the hour.

The event featured an insightful Panel Discussion Session moderated by Dr. Deepak Kumar Sahu, Editor-in-chief-VARINDIA. The panelists who joined the session were - Dr. Pawan Chawla, CISO & DPPO- Tata AIA Life Insurance; Sarita Padmini, Sr Director-Protiviti India Member Firm; Priyanka Arora, Solution Sales Lead- Microsoft; Dr. Puneet Kaur Kohli, CTIO - Generali Central Life Insurance and Bhaskar Rao, CISO - The Bharat Co-operative Bank.

ping the future of India's Technology landscape

PRODUCT DISPLAY KIOSK

CONTEXT

TP-LINK

FACEOFF TECHNOLOGIES

ACRONIS

EXCLUSIVE DINNER ROUND TABLE WITH ACRONIS

The world is entering a major investment phase in AI infrastructure

DR. DEEPAK KUMAR SAHU
CHIEF EDITOR – VARINDIA

"As cyberattacks become more sophisticated and humanlike, digital identity is emerging as the weakest link in enterprise security. Stolen credentials and outdated authentication methods remain the leading cause of data breaches, especially as attackers increasingly use AI to launch highly convincing phishing and social-engineering attacks. India stands at a critical moment in its technology journey. While the country has built a $250 billion IT industry and become a global leader in software services, its domestic IT spending accounts for only about 1% of global technology investments. Bridging this gap will be essential if India wants to play a leading role in the emerging AI-driven economy. One of the most important steps is investing in accelerated computing infrastructure, particularly GPU-powered systems that form the backbone of modern artificial intelligence. Unlike traditional computing, which improves gradually over time, accelerated computing dramatically increases performance and efficiency.

Cloud adoption, open banking, and remote work are transforming security in financial institutions. Identity has become the new security perimeter, making Identity and Access Management (IAM) central to modern banking cybersecurity. Banks must ensure that the right individuals have the right access at the right time. To address this, financial institutions are strengthening IAM frameworks with automated identity lifecycle management, role-based access controls, behavioral analytics, and risk-based authentication to detect anomalies and reduce insider threats while protecting sensitive financial data. The attack highlights the need for strict control over privileged access and stronger protection of enterprise management platforms through multi-layer authentication and continuous monitoring to detect intrusions early. Organizations must also prepare for destructive cyberattacks beyond ransomware by segregating critical systems, maintaining secure offline backups, and strengthening incident response, employee awareness, and proactive threat intelligence to respond quickly to large-scale disruptions.

India emerges as a new hotspot for cyber criminals with 4,168 crore calls in a year. Over 175,000 AI servers are currently exposed on the internet, many with weak or no authentication. Most run on GPU cloud instances with production models loaded. One open port can lead to massive cloud bills, stolen model weights, hijacked compute, or even poisoned models and remote code execution. We are also seeing how Tech companies are suddenly launching campaigns focused on adopting and promoting AI across their products and services."

Acronis ensuring not only Data Availability but also Data Integrity

ABHAY MISHRA
DISTRIBUTION ACCOUNTS MANAGER – ACRONIS

"Considering the fact that we are running business organizations in an era of digitalization, each organization today wants to enhance their business excellence or operational efficiency. At the same time, organizations today are constantly on their toes to onboard new customers, and remain competitive in this competitive environment. Now, considering this, organizations are seen adopting multiple tools and technologies which generate a huge amount of structured or unstructured data. Now what is critical here for the organization is if there is any disaster kind of a scenario and still you need to ensure that the availability of that data is there. So, Acronis is dedicated to the mission where we ensure that not only the availability of the data is there, but we also ensure the integrity of that data. We are working on both part, whether it is related to the security of the data or the availability.

As an organization you might be securing your data in some secure location and keeping backup repository. But the main worry for the customer is to ensure that that backup does not get tempered, or does not get changed if in case there is any unauthorized access. So the question is - can Acronis secure that? The Acronis Cloud Platform provides you with that flexibility, which we called as immutability. So if you are keeping your data on Acronis hosted storage, this functionality comes by standard, which is a standard feature. If there is any accidental deletion of that data, your data repository still will be available on Acronis Cloud, which you can restore at the time of disaster. Another case or scenario of worry for the customer can be any ransomware attack taking place. Acronis ensures that the data center is built on top of active protection, so whatever the backup repositories or data you are keeping on Acronis Cloud, it is protected from any type of ransomware attacks. If we see from an operational efficiency perspective, the Acronis Cloud platform is a single integrated platform which is our unique selling point. The backup here is basically integrated, either with the cybersecurity tools or remote management. We offer a functionality called 'Do the scanning of a malware for the backups'. This will allow you to recover the clean files, besides also ensuring that the malware should not get spread into the devices which are connected into the network.

In other words, Acronis Cyber Cloud is a platform that enables service providers to deliver cyber protection in an easy, efficient and secure way. With a single platform, you and your customers gain access to hybrid cloud backup, disaster recovery, ransomware protection, file sync and share, and blockchain-based file notarization and e-signature services, all managed from a centralized console."

GenAI helping threat actors create more sophisticated impersonation attacks

PRIYANKA ARORA
SOLUTION SALES LEAD - MICROSOFT

"Both cyber security and AI complement each other today. Cybercrimes have grown 5x. If you look at the projected annual cost of cyber crime, it is $10.5 trillion. It could become the third largest economy for that matter. In fact, cybercrimes basically include data theft, compromised credentials, business losses, businesses getting disrupted, reputational damage of the organizations, and so on. This figure is very daunting at this point of time. Let us look at some other facts. The median time for an attacker to penetrate inside the customer environment has reduced even further. It was one hour 12 minutes but currently powered by Gen AI, it has come down to less than 32 minutes. If we compare the last two years, the password attacks per second has surged from a 4000 to a 7000. Threat actors which are being tracked by Microsoft has also increased from a 300 to a 1500+. During Operation Sindoor, there was an organization which was tracked down in Bihar which was committing phishing and ransomware attacks on organizations. And all of these threat actors are operating in the Indian sub-continent. Having said this, security has become a serious conversation today. Phishing and ransomware attacks are increasing as we speak.

Today, organizations are facing a challenge of disconnected tools. A typical organization is using between 6-15 different tools to protect every single thing - their endpoints, devices, data, cloud, and so on and so forth. Secondly, there is a dearth of cyber security professionals. Gen AI is certainly for good, but Gen AI is also supporting threat actors in terms of creating better impersonation attacks, and create malwares which can be embedded in an email or a link. This is why we need to be ahead of these threat actors as defenders and our defense mechanism has to be much quicker. So AI is certainly expanding the attack surface with Gartner estimating that by the end of 2026, Gen AI will basically account for 10% of all the data which is being produced, and all of that could become vulnerable if we are not protected adequately. It is important to defend our email endpoints, devices, apps, and cloud data. But do we introspect and realize that we are defending all of these in silos. Threat actors are approaching us in a very connected fashion, and they are traversing across our network. For example, a user gets a phishing mail or clicks on a link which has a malicious code, and then the identity gets compromised. The attack then moves towards their endpoint device before traversing across the network. The threat actor can literally remain in the network as much as they want without being identified. We literally suffer with alert fatigue because we have created silos."

A unified framework combining neuro-AI, quantum-safe cryptography, and cognitive security is imperative

DR. ARINDAM SARKAR
CHIEF ARCHITECT - FACEOFF TECHNOLOGIES

"We are all talking about AI. Everyone is trying to design a system that should be AI based, but MIT says that 95% of Enterprise AI fails, with only 5% doing the right thing. So where lies the problem? Whenever we are considering any design, how do we decide how are we collecting and connecting the dataset? What about the poisonous data? Why the training and testing data ratio should be 80:20, 75:25, and not 60:40? We should also introspect and see whether we are using ZKP (zero knowledge proof), SMPC (Secure Multiparty Computation), differential privacy or for that matter post quantum cryptography. FaceOff has designed one engine called Adaptive Cognito engine (ACE). This ACE has 10 different avatars. In 10 different domains, ACE can serve you which is actually a multimodal AI engine. Now this Adaptive Cognito engine can give you different solutions. This multimodal trust-verification system fuses visual, audio, behavioral, and contextual intelligence to establish identity authenticity with cryptographic precision.

While legacy KYC and facial-recognition systems depend on probability models, FaceOff ACE delivers deterministic verification through neural cryptography and quantum-safe encryption. It analyzes more than eight physiological and behavioral signals — from deepfake detection and micro-expressions to voice sentiment, gaze tracking, and rPPG heart-rate — to generate a real-time Trust Score for every interaction. ACE doesn't just authenticate — it learns, adapts, and detects anomalies before they escalate. ACE features an AI-orchestrated multi-cloud layer that autonomously reroutes workloads during outages — ensuring always-on verification across banking, telecom, and defense environments. Rooted in Indian innovation and designed for global scalability, FaceOff Technologies exemplifies the nation's leadership in deep-tech identity intelligence. Its solutions — spanning FacePay, national e-KYC, border security, and enterprise onboarding — are redefining trust, transparency, and digital sovereignty in the era of synthetic intelligence.

As the world moves toward quantum computing, traditional encryption and conventional AI security models face an existential challenge: quantum systems can break today's cryptographic standards in minutes, and adversarial attacks can manipulate machine learning systems with subtle digital distortions. RSA or ECC will not protect you anymore. So the tagline should be HAR BYTE MEIN BHAROSA. FaceOff's Neuro-Quantum Safe technology represents the next evolution of secure intelligence—where neuroscience-inspired AI, post-quantum cryptography, and adversarial neural defense converge to protect global digital ecosystems from both present and future threats. At the core of this framework is Neuro-Cognitive Shielding, inspired by how the human brain performs pattern recognition, context reinforcement, and anomaly rejection. Instead of relying solely on static encryption or fixed decision boundaries, FaceOff's system thinks like a human: it interprets data contextually, detects subtle manipulations, and adapts autonomously as attackers evolve."

Application performance is key to business success for any organization

SUSHIL KUMAR PATIL
ACCLERATION SOLUTIONS ENGINEER- RIVERBED

"Today cybersecurity is paramount for any industry, especially the BFSI. The first word that comes in mind along with applications and adoption of digitalization and AI is cyber security. Apart from the cyber security aspect, applications which are there are becoming more and more smarter. So application acceleration as a solution is becoming very important. Riverbed is an organization which is two decade old, and is a leader in WAN Optimization or application acceleration solutions. We also have an observability portfolio. Along with the acceleration, the observability keeps an eye on your network, infrastructure and application and understands them. It monitors, collects all the data, and it ensures that all these data are logically put across into a report or an analytical format. As a result, the analyzers who are there can extract information out of it. In today's increasingly complex IT landscape organizations struggle to maintain peak performance across diverse environments. Application and data resilience is business is seen as resilience. Slow loading applications and network inefficiencies lead to frustrated users, lost productivity and business interruptions. With Riverbed Acceleration, your applications run faster, more reliably and securely, all through a comprehensive platform approach. The riverbed platform is dedicated to improving user experience by enabling IT to prevent, identify and resolve issues and to ensure applications run faster anywhere, over any network and on any device. Riverbed Acceleration enables business resiliency by delivering apps and data at peak performance. With Riverbed, IT teams can improve application performance, migrate to the cloud with confidence and deliver resilient data to the cloud and the edge to power AI.

SteelHead, our industry leading solution for over 20 years, optimizes application performance, reduces latency and transfers data securely at scale. This means faster response times delighted users and business results. Steelhead Cloud helps you overcome the latency and bandwidth challenges of cloud transitions, ensuring your apps run optimally in the cloud. The precision of your AI is only as good as your data. With SteelHead RS, you can move massive volumes of data between data center and edge efficiently and securely and with resilient networking at the edge, you can maintain local operations even when disconnected from the data center. The choice is yours – on premises, at the edge or in the Cloud without compromise, you can empower your IT teams to drive your business forward. So in essence, application performance governs your business performance. This is true for any sector – BFSI, manufacturing, or the healthcare sector."

WIITF: Witness Revenue Leak Roundtable

Many marketing teams hit lead targets but struggle to prove real revenue impact. Boards ask for ROI, while teams rely on activity metrics. Sales often blames "low-quality leads," and pipeline gaps between MQL and closed deals remain unclear. A key issue is speed. Around 60% of pipeline is lost between initial signal and conversion, with most teams taking days to respond while top performers act within minutes.

The exclusive session was organized by Wyzard, where Mr. Rahul Jain, Founder and CEO, addressed marketing leaders in the tech industry. Ms. Amita Bhowmick, Global Head of Alliances at Wyzard, spoke about how the industry is evolving and adapting.

This private roundtable brings together 15 senior marketing leaders for a focused 90-minute discussion. It covers practical ways to prove marketing's revenue contribution, fix pipeline leaks, and improve attribution. Attendees gain a clear framework, real benchmarks, a 90-day action plan, and peer insights to drive measurable growth.

L to R: Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA; Dr. Pawan Chawla, CISO & DPPO, Tata AIA Life Insurance; Bhaskar Rao, CISO, Bharat Co-operative Bank (Mumbai) Ltd; Sarita Padmini, Senior Director, Protiviti India Member Firm; Dr. Puneet Kaur Kohli, CTIO, Generali Central Life Insurance; and Priyanka Arora, Solution Sales Lead, Microsoft

BFSI 2026: AI, EMBEDDED FINANCE, AND THE NEW ERA OF DIGITAL TRUST

The panel discussion at the event, moderated by Dr. Deepak Kumar Sahu, Editor-in-Chief, VARINDIA, focused on the theme, "BFSI 2026: AI, Embedded Finance and the New Era of Digital Trust." The session featured prominent industry leaders, including Dr. Pawan Chawla, CISO & DPPO, Tata AIA Life Insurance; Sarita Padmini, Senior Director, Protiviti India Member Firm; Priyanka Arora, Solution Sales Lead, Microsoft; Dr. Puneet Kaur Kohli, CTIO, Generali Central Life Insurance; and Bhaskar Rao, CISO, Bharat Co-operative Bank (Mumbai) Ltd.

The discussion explored how artificial intelligence is transforming the BFSI landscape through predictive fraud detection, hyperautomation, and enhanced customer experience. Panellists highlighted the growing role of embedded finance in integrating financial services into digital ecosystems, while stressing the need for robust digital trust. Key themes included real-time fraud management, data privacy, API security, and protecting human and machine identities, alongside the importance of responsible AI adoption and strong governance frameworks.

Dr. Pawan Chawla, CISO & DPPO, Tata AIA Life Insurance, emphasized that AI adoption in organizations is still evolving and must be approached cautiously, particularly from a security standpoint. While AI and hyperautomation hold promise for improving fraud detection, emerging risks such as deepfakes and AI-generated content misuse make detection increasingly complex. He noted that organizations must carefully evaluate, integrate, and control AI within their ecosystems before large-scale deployment. On digital twins, he stressed the need for a "privacy by design" approach, ensuring clear oversight of data collection, storage, and access. He highlighted the importance of least-privilege access, encryption, data classification, and strong governance, especially as data fiduciaries remain accountable for breaches under regulations. He concluded by advising a phased adoption strategy aligned with business needs, underscoring the dual focus on "AI for security and security for AI."

Sarita Padmini, Senior Director, Protiviti India Member Firm, highlighted that while fraud detection has existed for years, the focus has now shifted from merely identifying fraud to improving the accuracy and efficiency of detection through AI-driven hyperautomation. She noted that earlier systems struggled with high false positives, but AI has significantly reduced these, enabling a more targeted approach to identifying critical fraud cases. She emphasized that banks must move beyond isolated deployments and adopt a holistic, ecosystem-wide security approach, even when solutions are hosted on private clouds or internal data centers. Stressing that data is a highly valuable asset, she called for strong data governance and "privacy by design," with clear visibility into data flows. She reiterated that data fiduciaries remain ultimately accountable for protection, and highlighted eKYC and AML-driven fraud detection as key emerging use cases.

Priyanka Arora, Solution Sales Lead, Microsoft, noted that AI is transforming BFSI from a reactive to a predictive model, enabling real-time fraud detection and improved customer experience through hyperautomation. She explained that AI can instantly flag anomalies such as location mismatches and block suspicious transactions, significantly enhancing speed and scale. She added that leveraging customer data is key to improving experiences, but must be governed by responsible AI practices to ensure data security and trust. Arora also pointed to the growing importance of securing both human and machine identities, as organizations increasingly adopt AI-driven agentic architectures involving bots and automated systems handling sensitive data. Looking ahead, she underscored the role of AI in enabling hyper-personalisation, improving risk control, and supporting confident, data-driven decisions while ensuring safer digital transactions for customers.

Dr. Puneet Kaur Kohli, CTIO, Generali Central Life Insurance, said that while AI significantly enhances fraud detection, automation has long supported the process, with AI now improving precision and depth. In insurance, tools like video KYC help identify fraudulent claims, including AI-generated clones, though human oversight remains critical. She pointed out that AI can detect subtle indicators such as lip sync, behavioral patterns, and sentiment, aiding in validating authenticity. She also underlined AI's role in hyper-personalisation, leveraging historical data to understand customer preferences, buying behavior, and risk profiles. On securing bots and APIs, she stressed rigorous pilot testing, correct parameter setting, and continuous evaluation of external integrations for compatibility. Kohli added that digital twins are gaining traction in BFSI for assisted financial planning, while AI is expected to drive automation, compliance, and budgeting efficiencies in the coming years.

Bhaskar Rao, CISO, Bharat Co-operative Bank (Mumbai) Ltd., stated that AI has become essential for banks, particularly in fraud risk management, as the industry shifts from a reactive to a proactive approach. He explained that with the rise in digital transactions, banks are deploying AI-based FRM solutions to detect fraud in real time, generate instant alerts, and automatically block suspicious transactions using predefined frameworks. He added that AI enables analysis of transaction behavior, geolocation patterns, and anomalies, which would be difficult to manage manually. Rao also highlighted the importance of "security by design" and "privacy by design," especially given the extensive use of customer data and third-party APIs. He noted that banks are implementing API security and DLP solutions to monitor and control data flows, while AI also helps reduce false positives and efficiently manage large volumes of security alerts.

The New Cloud Playbook: AI, Multi-Cloud and Zero-Trust Take Center Stage

As enterprises enter 2026, cloud computing is evolving from a foundational IT layer into a strategic platform driving innovation, resilience, and competitive differentiation. The growing integration of artificial intelligence is enabling predictive scaling, intelligent resource management, and real-time decision-making, helping organisations enhance performance while optimising costs. At the same time, security has taken centre stage, with zero-trust frameworks becoming essential to protect increasingly distributed and complex digital environments through continuous verification and identity-led controls.

Industry leaders also highlight a decisive shift towards hybrid and multi-cloud architectures, where enterprises balance agility with control by operating across public clouds, private infrastructure, and on-premises systems. This evolution, while enabling flexibility and scalability, has intensified the need for unified orchestration, observability, and governance. Experts across cloud, OEM, and solution provider ecosystems emphasise that the focus is now on simplifying complexity, embedding AI into core operations, and ensuring data sovereignty in line with emerging regulatory requirements.

Against this backdrop, VARINDIA spoke to a cross-section of Cloud & Data Center companies, OEM players, and solution providers/ partners to understand how they are aligning strategies, investments, and platforms to power the next phase of enterprise digital transformation in an AI-driven world.

Building a unified connectivity cloud to enable AI, edge, and secure innovation

GORAN RISTICEVIC
VP & MD, ASIA PACIFIC, CLOUDFLARE

"At Cloudflare, we are seeing cloud evolve from a collection of services into a more unified, intelligent layer that connects users, applications and data seamlessly. Our focus has been on building a connectivity cloud that integrates networking, security, and compute into a single platform, reducing fragmentation and enabling organizations to operate more efficiently. As AI adoption accelerates, particularly in markets like India, there is a growing need for infrastructure that supports real-time processing and low-latency experiences. We are investing in edge capabilities that allow businesses to run applications and AI inference closer to users, improving performance and responsiveness, while supporting context aware workloads.

Our strategy is rooted in simplifying the cloud experience while expanding what organizations can build on it. Many businesses today navigate complex multi-cloud and hybrid environments, dealing with multiple vendors across networking, security, and compute. We address this by converging these capabilities into a unified platform that is easier to deploy, manage, and scale. We continue to expand our global and regional network footprint, including across India, where we are present in 14 cities, to ensure low-latency access and consistent performance.

Cloudflare's connectivity cloud removes barriers that slow down innovation. By combining high-performance networking, integrated security, and edge computing, we enable faster deployment while maintaining reliability. With always-on security and strong DDoS mitigation, organizations can scale confidently and focus on building digital experiences rather than managing infrastructure."

AI-smart, governed cloud platforms are driving secure enterprise transformation in India

HARSH VAISHNAV
SR DIRECTOR AND HEAD – CHANNELS, INDIA, ASEAN AND HONG KONG, NUTANIX

"Organizations today are navigating three converging shifts: the rise of AI, the risks of ungoverned 'shadow AI,' and increasing demand for data sovereignty. In India, the stakes are high. Our Nutanix Enterprise Cloud Index shows 96% of IT leaders see AI used outside official oversight as risky, and 73% report AI adoption emerging from non-IT functions. This drives a focus on centralized governance and cross-functional alignment. At Nutanix, we are evolving from providing infrastructure to delivering a governance framework. Container adoption is accelerating, ensuring cloud-native applications are secure, portable, and manageable across any environment. Our aim is to turn AI from a risk into a competitive advantage.

Our growth strategy focuses on helping enterprises become AI-Smart rather than AI-First. We are expanding hybrid multi-cloud capabilities that combine public cloud agility with on-premises control and support AI workloads and automated data services. Investments in R&D centers in Bengaluru and Pune ensure our roadmap meets the scale and complexity of the Indian market, enabling secure, efficient use of next-generation AI.

Nutanix accelerates digital transformation by reducing technical debt and complexity. Our unified platform runs traditional systems alongside modern AI workloads without costly re-platforming. Automation, security, and policy controls enable confident experimentation with GenAI and edge computing. This foundation gives organizations freedom of choice, accelerates innovation, maintains control, and prepares them for edge AI, quantum-ready infrastructure, and stricter data localization requirements."

Cloud is becoming the core operating model for innovation in 2026

MANGESH SURVE
SR. DIRECTOR – SOLUTION ARCHITECTURE AND TECH SALES, RED HAT INDIA

"Cloud has moved well beyond infrastructure economics. What we are seeing in 2026 is the cloud becoming the core operating model for innovation, the platform on which enterprises are building their next competitive positions. Companies are not debating whether to transform; they are asking how to do it without losing control of their data, infrastructure, or vendor relationships.

That is where Red Hat's open hybrid cloud model becomes relevant. India's enterprise reality is not uniform—whether it is a large public sector bank, a telecom operator building AI-driven self-healing networks, or a manufacturing company running edge workloads at disconnected sites, all have different infrastructure realities. This is where Red Hat OpenShift comes into play, enabling customers to build, modernize, and deploy applications at scale on their choice of hybrid cloud infrastructure.

On the AI front, about 70 to 80 percent of enterprises have already run pilots, and the decisive shift from experimentation to production will define 2026 and 2027. With Red Hat AI Enterprise, our metal-to-agent platform, enterprises can develop and scale AI across any hybrid environment. Through enterprise open source and Kubernetes, we help organisations standardise operations and orchestrate workloads, while open source ensures a transparent security posture. India is not just another cloud market; it is one of the most consequential digital transformation stories, and we aim to be the platform enabling it."

India must own its digital future through AI-first, sovereign cloud infrastructure

NARENDRA SEN
FOUNDER & CEO, RACKBANK AND NEEVCLOUD

At NeevCloud, we believe India must own its digital future. The cloud industry is shifting toward a phase that demands sovereignty, speed, and AI-native infrastructure, and we have re-architected our approach. Our offerings are AI-first by design, as traditional cloud architectures were not built for high-intensity, continuous AI workloads. We have redesigned facilities with advanced cooling, accelerated compute fabrics, and AI-optimized data center designs, enabling us to go from groundbreaking to operational in 6–8 months, compared to the industry standard of 24 months.

We are championing the "Sovereign AI SuperCloud" movement. Data centers are the new sovereign territory, and AI is the new electricity. As India's first AI Supercloud, NeevCloud enables enterprises to train and scale Large Language Models (LLMs) with full data locality, security, and compliance. Our strategy focuses on making world-class AI infrastructure accessible, affordable, and sovereign through vertical integration, Giga-Scale AI Campus and AI SEZs, and the AI SuperCloud platform, helping Indian enterprises innovate without relying on foreign providers.

Innovation requires high-performance compute and ease of access. Enterprises can deploy LLMs, generative AI, analytics, and HPC workloads at hyperscaler speeds within India, enabling faster AI deployment, reduced timelines, cost efficiencies, and data sovereignty. We integrate AI at the orchestration layer for self-optimizing operations while embedding zero-trust security and full tenant isolation. With BYO-GPU, low-latency interconnects, and Kubernetes-native interoperability, enterprises can operate seamlessly across public, private, or sovereign environments without disruption.

AI must be native to cloud to deliver intelligent, cost-effective infrastructure

NEELAKANTAN VENKATARAMAN
VP & GLOBAL HEAD – CLOUD, AI AND EDGE COMPUTING BUSINESS, TATA COMMUNICATIONS

"As enterprises advance in 2026, cloud platforms must operate with intelligence, autonomy, and built-in optimisation, helping organisations extract sustained business value rather than manage infrastructure complexity. At Tata Communications, AI is native to our cloud, integrated across infrastructure and processes via Vayu Cloud. Combining FinOps, AIOps, and automated workflows, it continuously optimises resources, right-sizes workloads, and prevents incidents proactively. Together with IZO+ Multi Cloud Network, Edge Distribution Platform, and ThreadSpan, our AI-ready digital fabric unifies networks, cloud, and security, enabling enterprises to scale AI workloads efficiently. Using general-purpose and NVIDIA GPU-accelerated compute across bare metal, virtual machines, and Kubernetes, and through AI Studio, we help customers move from proof-of-concept to production in days with governance, explainability, and security built in.

Security is integral. Zero-trust starts with full-stack, sovereign architecture. Vayu Cloud ensures customer data stays within India using layered controls, WAF, key management, and continuous monitoring. ThreadSpan enables role-based provisioning and micro-segmentation across hybrid and multi-cloud environments, supported by 24x7 NOC, SOC, and DevSecOps, allowing enterprises to adopt zero-trust progressively without disrupting operations or compliance. Our hybrid-by-design approach modernises enterprises at their own pace. Vayu Cloud orchestrates multi-tenant public clouds, private clouds, and edge infrastructure through a single interface, allowing workloads to shift, scale, or burst seamlessly between on-premises, Tata services, and hyperscalers. Cloud enables continuity and incremental innovation, while unified control and workload mobility define the next phase of enterprise cloud strategy."

AI-native, high-performance cloud is key to accelerating digital transformation in India

PIYUSH GUPTA
VP – INDIA, APAC & MIDDLE EAST, VULTR

"At Vultr, we are proactively adapting our cloud offerings to the evolving AI-native and distributed computing landscape. As enterprises move from centralized models, our 32 global data centers—including Mumbai, Bangalore, and Delhi NCR—are built to handle high-performance AI workloads. With India's IT spending projected at $176.3 billion in 2026 (Gartner), driven by cloud and data center investments, businesses are increasingly focused on AI. Local latency and data residency are now critical. We are expanding VM and bare-metal CPU and GPU compute capacity, investing in Kubernetes and managed container offerings, and ensuring data sovereignty is integral to our infrastructure strategy.

Our growth strategy rests on three pillars. First, product depth: customers can scale from their first VM to multi-region deployments without switching providers. Second, building the developer community through education, engagement, and accessible onboarding. Third, strengthening our partner ecosystem with system integrators and managed service providers who understand Indian enterprises' legacy infrastructure and compliance requirements. Transparent pricing underpins all three pillars, addressing one of the biggest confidence concerns for businesses.

Vultr propels customers from AI experimentation to production-scale digital transformation. Gaming, healthtech, and fintech firms benefit from lower latency, cost efficiency, and high availability. Predictable infrastructure frees teams to focus on building. Our goal is to shorten the distance between ideas and deployment, expand capabilities for Indian businesses, and make infrastructure a solved problem—the only question that remains is what to build next."

Sovereign, AI-native cloud platforms enable secure and scalable digital transformation

PIYUSH PRAKASHCHANDRA SOMANI
PROMOTER, MANAGING DIRECTOR AND CHAIRMAN, ESDS

"The global cloud computing market is undergoing structural expansion, driven by AI workload demand, sovereign compliance pressures, and real-time data proliferation. At ESDS, our response is architectural reinvention through our flagship platform, the world's first Autonomous Hyperscaler Cloud Platform, delivering 8-layer, 189-module AI orchestration and patented vertical auto-scaling. Our GPU subsidiary, SPOCHub, 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 data centers strategically span six locations: Nashik, Airoli, Bengaluru, Mohali, Noida, and Kolkata.

ESDS executes a three-pillar growth strategy anchored on GPU infrastructure, community cloud specialisation, and geographic expansion. SPOCHub provides 17.83 PB VAST storage with competitive GPU billing versus hyperscalers. Our Banking Community Cloud serves 450+ clients, Smart City Cloud hosts 80% of India's operational smart cities, and our data center network scales to 125 MW across 11 facilities. This sovereign, AI-native infrastructure will power India's USD 1 trillion digital economy by 2030.

Our cloud solutions deliver measurable AI outcomes: banking sees 65% improved fraud detection and 40% lower opex; Smart Cities report 55% faster incident response; manufacturing achieves 48% reduced downtime and 70% faster ERP performance; healthcare enjoys 60% faster diagnostics; retail gains 22% more revenue per visitor. With India's DPDPA, RBI Cloud Framework, and MeitY policy mandating data residency and explainable AI, sovereign-cloud native providers like ESDS offer enterprises optimized resources, stronger security posture, and uninterrupted service delivery."

AI-ready, intelligent data infrastructure is driving enterprise cloud transformation in India

PREMALAKSHMI RAMAKRISHNAN
MD & AREA VP, INDIA AND SAARC, NETAPP

"At NetApp, we are aligning our cloud strategy with enterprises increasingly operating in hybrid and multi-cloud environments. In India, nearly 70–75% of organisations are in such setups, creating challenges around data fragmentation, cost, and complexity. Our focus is on delivering intelligent data infrastructure that enables seamless management of data across on-premises, private, and public clouds. Through deep integrations with hyperscalers like AWS, Microsoft Azure, and Google Cloud, we ensure consistent performance, security, and accessibility across environments. Beyond traditional storage, we help enterprises make data AI-ready, actionable, and strategically valuable.

Our growth strategy is centred on ecosystem-led innovation and platform enhancements. Collaborations with hyperscalers, including Google Cloud, enhance NetApp Volumes to support enterprise-grade workloads with greater flexibility and simplicity. Unified data platforms eliminate silos, enable seamless data mobility, optimise costs, and scale efficiently. Partnerships with IT services firms such as TCS further strengthen our ability to deliver these capabilities reliably at scale.

NetApp accelerates digital transformation by simplifying data access and management across hybrid and multi-cloud environments. Solutions like Cloud Volumes ONTAP enable seamless integration, reduce latency, and support AI workloads effectively. Built-in data protection, ransomware resilience, and automated tiering ensure security, efficiency, and cost optimisation. By combining performance, security, and intelligent automation, we empower enterprises to focus on insights, drive innovation confidently, and maintain uninterrupted business operations across environments."

AI-ready, high-performance cloud is driving enterprise digital transformation in India

RANJIT METRANI
PRESIDENT, MANAGED SERVICES, CTRLS DATACENTERS

"CtrlS is aligning its cloud ecosystem with AI-led workloads, hybrid/multi-cloud adoption, and edge computing by building AI-ready, high-density hyperscale infrastructure and strengthening the connectivity layer. Our GPU Private Cloud is designed for AI and ML workloads, with GPU clusters, full-stack management, 24/7 support, and data sovereignty from Rated-4 data centers. We enable multi-cloud adoption through CtrlS Cloud Connect, providing private, secure connections to major cloud providers. Cloud Optimize ensures enterprises manage GPU-intensive workloads efficiently while maintaining cost, performance, and AI-readiness.

Our growth strategy follows a multi-pronged approach: investments in AI and cloud-ready hyperscale capacity, enhancing cloud interconnects, forming strategic technology partnerships, and verified peering. We are also investing in renewable energy and sustainable infrastructure, and developing an edge-to-core architecture integrating hyperscale campuses with distributed edge infrastructure for low-latency access and seamless workload distribution. These initiatives help enterprises adopt flexible, high-performance multi-cloud architectures and support large-scale AI-driven digital transformation. CtrlS accelerates innovation by providing secure, high-performance, always-on-demand cloud and managed services that reduce time, cost, and complexity. Our IaaS, Virtual Desktop Infrastructure, Disaster Recovery, Backup, Security Operations, and Remote Infrastructure Management solutions improve productivity, resilience, and continuity. By supporting mission-critical environments such as the Bombay Stock Exchange, handling 700 crore transactions daily, CtrlS ensures high-volume digital systems operate reliably. Quick provisioning, operational support, and business continuity allow customers to focus on new digital services, enhance user experience, and respond faster to market needs."

Full-stack AI and cloud platforms are simplifying enterprise digital transformation in India

RENU RAMAN
FOUNDER & CEO, PROXIMAL CLOUD

"Our approach is rooted in building infrastructure that evolves alongside the workloads it supports. As a company developing platforms for AI and data-intensive applications, we design our solutions based on the operational challenges our customers face. We follow a three-part approach: adopt Open Source wherever possible, partner with leading infrastructure providers such as TrueFoundry and Divyam.ai for non-core components, and develop our own components using modern AI tools and methods, including code generators, observability tools, validation tools for A/B testing, and red-teaming.

We actively use our platform during development and deployment to ensure our architecture meets real enterprise requirements, particularly around predictive scaling, efficient resource utilisation, and low-latency responses to complex queries. Our offerings come in both appliance (physical) and virtual forms on multiple cloud partners, with reference designs and validations. The AI delivery model has shifted from traditional ITops to DevOps/SRE to Forward Deployment Engineers (FDEs), closing skill gaps while bringing engineering closer to customer workflows and requirements.

With over 60 million SMEs and a growing mid-market, we provide a full-stack platform spanning language interfaces, data processing, and backend infrastructure. By enabling multi-language support, cost-efficient compute, deeper insights, and low latency, we help enterprises unlock value from data and navigate complexity. Our unified data foundation and modern AI compute for structured and unstructured data, knowledge graphs, and LLMs enable enterprises to adopt AI confidently, improve productivity, and accelerate digital transformation practically, scalably, and measurably."

Flexible, AI-ready cloud platforms are enabling faster enterprise digital transformation in India

SASHISHEKAR PANDA
EXECUTIVE VP - CLOUD AND MEDIA SERVICES, YOTTA DATA SERVICES

"To stay aligned with evolving industry trends, we continue to enhance our cloud offerings around four strategic pillars: flexibility, compliance, business continuity, and AI readiness. Our architecture supports public, private, hybrid, and multi-cloud environments, giving customers the freedom to adopt the model that suits their requirements while maintaining control and avoiding vendor lock-in. To foster open innovation, we developed a marketplace that brings together a diverse ecosystem of ISV solutions, enabling customers to discover, integrate, and scale applications on our platform.

We provide seamless hybrid cloud integration with leading global platforms through private, low-latency connectivity, while ensuring data residency and compliance standards. This allows organizations to burst workloads on demand, scale efficiently, and maintain performance and availability. Our platforms are designed with integrated lifecycle management, advanced observability, and resilient architecture. Platform-led services such as Drishticam, Urja, and Sudarshan simplify operations, enhance efficiency, and unlock new monetization opportunities.

Our multi-pronged strategy focuses on AI-ready infrastructure, GPU-enabled environments, hybrid and multi-cloud architectures, and strengthening the marketplace ecosystem. SLA-driven managed services and FinOps-led cost optimization enable enterprises to focus on core business. Our flexible, scalable, high-performance cloud foundation accelerates digital transformation, enabling customers to integrate new workloads, modernize applications, and innovate confidently while maintaining cost, performance, and compliance."

ORIGINAL EQUIPMENT MANUFACTURERS (OEMS)

Hybrid AI infrastructure is transforming enterprise cloud and digital strategies in India

SRINIVAS RAO
MANAGING DIRECTOR - INDIA, LENOVO ISG

"Enterprise cloud strategies today are evolving from a 'cloud-first' mindset to hybrid AI-driven models, distributing workloads across public cloud, edge, and on-premises environments based on performance, latency, and regulatory requirements. Our Lenovo CIO Playbook 2026 shows 90% of Indian organisations prefer hybrid or multi-environment AI deployments. Lenovo's Hybrid AI Advantage combines AI-optimised infrastructure, software, and lifecycle services to enable seamless AI deployment and scaling. Partner collaborations reveal a move toward inference-led architectures, running AI continuously across environments, helping enterprises modernise IT while maintaining control, security, and operational efficiency.

Our strategy focuses on AI-optimised infrastructure, flexible consumption models, and ecosystem collaboration. Lenovo TruScale allows organisations to scale compute resources on demand while keeping workloads in preferred environments. Hybrid AI Advantage accelerates AI deployment and real-time inferencing, delivering measurable returns within months. Investments in high-performance AI infrastructure and advanced cooling technologies like Neptune 6th Gen enhance efficiency and sustainability. With 99% of Indian enterprises increasing AI investments, scalable hybrid AI platforms are critical to support enterprise AI adoption. Lenovo's hybrid cloud solutions enable enterprises to extract value from data and run AI closer to where data is generated, improving real-time performance. AI-driven automation, hybrid cloud orchestration, and zero-trust security ensure optimal performance, operational resilience, and cost efficiency across edge, on-premises, and multi-cloud environments. Through ThinkSystem servers, ThinkEdge platforms, and integrated services, Lenovo helps enterprises scale AI, analytics, automation, and generative AI adoption while maintaining seamless operations."

Hybrid AI-ready cloud is powering enterprise innovation and growth in India

SUDHIR GOEL
CHIEF BUSINESS OFFICER, ACER INDIA

"As organizations increasingly adopt AI, data analytics, and hybrid IT environments, cloud infrastructure must evolve to support complex and performance-intensive workloads. At Altos, we focus on high-performance computing, AI-optimized infrastructure, and scalable cloud-ready platforms that seamlessly support hybrid and multi-cloud environments while ensuring security, operational efficiency, and reliability. Energy-efficient architectures, advanced GPU-enabled systems, and flexible deployment models allow enterprises to scale based on evolving business needs, enabling AI training, data processing, and mission-critical workloads both in the cloud and at the edge. To expand cloud capabilities and drive growth, we invest in high-performance GPU-accelerated systems, advanced data processing solutions, and cloud-ready server architectures designed for AI, analytics, and enterprise workloads. Flexible deployment models enable businesses to operate across on-premises, hybrid, and multi-cloud environments without compromising performance or control. Collaboration with ecosystem partners and technology providers accelerates AI adoption and digital transformation, combining hardware innovation, optimized AI platforms, and integrated solutions to help enterprises scale, innovate, and grow sustainably. Our cloud solutions accelerate innovation by providing scalable, AI-optimized infrastructure that supports large-scale enterprise applications, hybrid and multi-cloud integration, and GPU-accelerated computing. By enabling faster AI experimentation, efficient resource utilization, and seamless deployment of digital services, we help enterprises shorten development cycles, extract insights from data, and drive meaningful digital transformation. Coupled with AI-driven optimization, zero-trust security, and flexible hybrid cloud adoption, our platforms provide a resilient, future-ready foundation that ensures secure and seamless business operations across industries."

AI-ready hybrid cloud infrastructure is powering enterprise scale and innovation in India

VENKAT SITARAM
SR DIRECTOR AND COUNTRY HEAD - INFRASTRUCTURE SOLUTIONS GROUP (ISG), DELL TECHNOLOGIES INDIA

"At Dell Technologies, our approach is centred on simplifying complexity while enabling innovation at scale across both cloud and AI. Through our long-rooted collaboration with Microsoft and NVIDIA, we deliver integrated hybrid and multi-cloud solutions—from Dell Private Cloud and PowerStore with Azure Local to the Dell AI Factory with NVIDIA—that help organisations seamlessly manage data and workloads across environments. PowerStore continues to evolve beyond storage to serve as a foundational platform for modern, future-ready private cloud environments, enabling enterprises to simplify infrastructure, strengthen resilience, and scale with confidence.

At the same time, with over 4,000 customers adopting the Dell AI Factory, we are enabling businesses to move AI from pilot to production by combining AI-ready data platforms, scalable infrastructure, and end-to-end solutions that accelerate time to value and deliver measurable ROI. By bringing together automation, AI-driven capabilities, and built-in cyber resilience, we empower organisations to optimise performance, strengthen zero-trust security, and ensure seamless operations across hybrid and multi-cloud environments.

This ultimately helps enterprises unlock the full value of their data, confidently navigate an increasingly dynamic digital landscape, and accelerate innovation at scale. By supporting AI workloads, robust security, and operational efficiency, Dell Technologies provides a future-ready foundation that enables organisations to scale intelligently, innovate faster, and maintain uninterrupted business continuity."

SOLUTION PROVIDERS / PARTNERS

AI-led platformization and zero trust reshape cloud security for the control era

HUZEFA MOTIWALA
SR DIRECTOR, TECHNICAL SOLUTIONS, INDIA AND SAARC, PALO ALTO NETWORKS

"Cloud has reached an inflection point. What was once a question of scale is now a question of control, as the gap between visibility and action has emerged as the defining challenge. At Palo Alto Networks, our response has been to collapse that gap by bringing cloud security, threat intelligence, and operations into a unified platform, enabling near real-time decision-making. AI plays a critical role, not as an overlay but as a core enabler of predictive and preventative security, while aligning with cloud-native models to ensure security is integrated into how applications are built and deployed.

In cloud environments today, complexity has become a silent constraint on growth, reflected in delayed decisions, fragmented visibility, and inconsistent outcomes. Our strategy addresses this through platformization, consolidating capabilities into a cohesive system that allows organizations to move from managing tools to managing risk. With deeper integration across cloud ecosystems and AI applied to reduce noise and prioritize what matters, many environments have seen up to a 75 percent reduction in alert volumes, enabling faster, more precise responses.

Innovation slows due to uncertainty around risk. By embedding security across the lifecycle and ensuring continuous runtime visibility, we provide clarity at every stage. As AI adoption grows, Prisma AIRS delivers end-to-end security across the AI lifecycle. Built on a zero-trust foundation, where trust is never assumed but continuously verified, our approach supports hybrid and multi-cloud environments, where resilience depends on how quickly and consistently you can act."

AI-powered IaC and Zero Trust drive smarter, resilient cloud operations

INDU MALHOTRA
VP, CLOUD INFRASTRUCTURE SERVICES – INDIA, CAPGEMINI

"Cloud platforms are well positioned to leverage AI to optimize infrastructure and enhance operational efficiency. At Capgemini, AI-assisted Infrastructure as Code (IaC) helps reduce the time to provision and manage environments, standardizes implementation patterns, and enables repeatable deployments, while accelerating detection and remediation of configuration drifts. Security is embedded and verified through improved prioritisation, context, and least-privilege enforcement, helping reduce attack surface without slowing delivery. AI also boosts developer and operations productivity through always-on assistants and by catching risky changes earlier in the delivery pipeline, including LLM-driven reviews of infrastructure pull requests within CI/CD.

Another area is AI log summarisation that turns high-volume, low-signal log streams into readable interpretations, highlighting anomalies, change, and capacity shifts, and triggering predictive insights-driven actions such as auto-healing and auto-scaling. Predictive FinOps ensures cost governance and real-time interventions to avoid bill shock. AI makes cloud operations proactive, predictive, and resilient through automated triage and remediation, translating into faster onboarding, more consistent and secure operations, and better change quality.

Zero Trust starts with the assumption that breaches can occur anywhere, so every access request must be continuously verified. This shifts the perimeter to identity, enforced through strong authentication, least-privilege access, IAM hardening, and micro-segmentation. Hybrid and multi-cloud adoption follows an incremental approach with discovery, unified identity, and 'R' strategies, supported by landing zones, Kubernetes, Terraform, GitOps, and consolidated monitoring to ensure portability and minimal disruption."

AI-driven GPU cloud and Zero Trust enable efficient, secure hybrid operations

KESAVA REDDY
CRO, E2E NETWORKS

"At E2E Networks, AI is deeply embedded into our cloud infrastructure to deliver intelligent, high-performance environments for modern AI workloads. We leverage AI-driven orchestration to optimise utilisation of large-scale GPU clusters, including H100, H200, and B200 deployments, dynamically scheduling workloads based on priority, utilisation patterns, and concurrent users to ensure maximum throughput and minimal idle capacity. Predictive analytics enables auto-scaling of GPU and compute resources during training or inference spikes without manual intervention, while systems continuously monitor infrastructure health, detect anomalies, and proactively resolve performance bottlenecks. Our AI models also help customers right-size infrastructure, reduce wastage, and achieve better price-to-performance.

Security is not an afterthought—it is architected into every layer of our cloud platform. We guide customers toward zero-trust frameworks that treat every access request as untrusted by default. Our approach is built on identity-centric access control, network micro-segmentation, and continuous monitoring with AI-powered threat intelligence that analyses traffic patterns, flags anomalies in real time, and triggers automated responses. We also offer dedicated, isolated infrastructure for sensitive AI workloads, eliminating noisy-neighbour risks while supporting data sovereignty.

For hybrid and multi-cloud adoption, we support seamless transitions without disrupting operations. Our platform integrates with hyperscalers like AWS, Azure, and Google Cloud, enabling customers to balance performance, cost, and compliance. Through phased migration, unified visibility, and technical enablement, we help organisations manage and scale hybrid environments with confidence."

AI-driven unified security and Zero Trust drive hybrid cloud transformation

MANISH ALSHI
SENIOR DIRECTOR, CHANNELS & ALLIANCES, CHECK POINT SOFTWARE TECHNOLOGIES INDIA & SOUTH ASIA

"In India, where organisations face a weekly average of 3,195 cyberattacks—a 2 percent increase in 2025 compared to 2024, according to Check Point Research—at Check Point Software Technologies we are strengthening cloud-native, unified security across hybrid and multi-cloud environments. As enterprises accelerate adoption of AWS, Azure, and private cloud, we secure networks, workloads, applications, and APIs through a single platform with consistent policy enforcement. Our approach embeds Zero Trust, automated threat prevention, and real-time visibility, helping organisations reduce misconfigurations, secure assets at scale, and support digital transformation without increasing complexity.

Our business strategy focuses on platform consolidation, AI-driven security, and partner-led growth. With adoption accelerating across BFSI, healthcare, and government, we enable partners to deliver managed cloud security services and recurring revenue models. Our Hybrid Mesh Network Security architecture secures data centres, cloud, and edge under a single platform. Combined with AI-driven automation and exposure management, this helps enterprises reduce response times and manage risk at scale, while our 100% channel-driven model continues to drive cloud-led growth.

With India's digital economy projected to account for about 20% of GDP by 2030, security must keep pace. Our cloud solutions embed AI-driven security directly into environments, with automation handling detection, vulnerability management, and response. Unified security across multi-cloud, SaaS, and on-prem eliminates fragmentation. Through a unified, prevention-first platform with identity-based access and AI-driven optimisation, we enable seamless hybrid and multi-cloud operations via a single control plane."

AI moves beyond infrastructure to drive workflow-led cloud efficiency and governance

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

"Most conversations about AI and cloud stop at the infrastructure layer—smarter autoscaling, cost anomaly alerts, and rightsizing recommendations—but those are table stakes. At Quadra, we are seeing real operational impact when AI is embedded into the workflow layer, automating how infrastructure decisions get made, not just flagging them. Our managed services use AI-driven monitoring that moves from reactive to predictive, detecting performance degradation or security drift before it surfaces as an incident. Through our Max-IT platform, customers get continuous FinOps intelligence that not only reports cloud spend but recommends architectural interventions, delivering 30–40% reductions in cloud wastage.

Zero trust is widely understood but inconsistently implemented, with enterprises often deploying fragmented controls without architectural coherence. Our approach starts with identity as the perimeter, using Microsoft Entra ID as the backbone to enable continuous verification across every access request across hybrid environments. We layer in Privileged Identity Management, Data Loss Prevention, and cloud workload protection to close gaps left by point solutions, positioning zero trust as a business resilience programme.

The challenge with hybrid and multi-cloud isn't technology—it is orchestration and governance. Our approach establishes a unified control plane before migration, standardising observability, security policy, and cost governance across Azure, AWS, and on-premises. Migration is sequenced by business risk, while our managed services absorb operational complexity, ensuring teams can scale without disruption."

Secure, AI-ready cloud adoption accelerates enterprise digital transformation

PRAVIR DAHIYA
CTO, TATA TELESERVICES

"Cloud computing has evolved from a foundational IT layer into a strategic enabler of innovation, scalability, and resilience in today's digital economy. At Tata Tele Business Services, we focus on simplifying cloud adoption for businesses across sectors by delivering integrated solutions that bring together secure connectivity, cloud platforms, collaboration tools, and cybersecurity within a unified ecosystem. As organisations move toward AI-driven operations and hybrid or multi-cloud environments, managing these ecosystems becomes increasingly complex. Our approach removes this complexity through fully managed services that ensure cloud adoption remains seamless, secure, and outcome driven. We enable data-driven decision-making, automation, and operational agility, helping businesses leverage cloud capabilities without the burden of managing underlying infrastructure.

Our solutions, including Smart Internet and SD-WAN, provide a resilient, high-performance network backbone, while our cloud communication suite, Smartflo, enables businesses to enhance customer experience through intelligent, scalable, and seamless engagement. Together, these offerings empower organisations to operate efficiently while staying agile and customer centric. With security-first architectures and simplified deployment, we ensure businesses are protected against evolving cyber threats while maintaining ease of management.

A 'cloud smart' mindset enables organisations to innovate faster, collaborate effectively, and scale with confidence. By combining simplified deployment with end-to-end managed support, Tata Tele Business Services helps enterprises and SMEs unlock the full potential of cloud while accelerating their digital transformation journey in a secure and sustainable manner."

AI-driven cloud and Zero Trust power secure hybrid multi-cloud transformation

RAJSEKHAR DATTA ROY
CTO, SONATA SOFTWARE

"Through 2026, enterprises will reposition cloud computing from a foundational infrastructure layer to a strategic engine for innovation and competitive differentiation. This shift is defined by the convergence of AI-driven operations, resilient security architectures, and flexible multi-cloud strategies—enabling organizations to accelerate innovation while sustaining operational discipline. At Sonata Software, we embed AI across the cloud lifecycle through AI-first platforms, including Harmoni.ai, AgentBridge, and our Agentic AI Engineering delivery model, integrating human expertise with AI-driven automation. AI-assisted tools such as Claude Code, GitHub Copilot, and Kiro help enterprises assess legacy landscapes, modernize applications, and optimize cloud performance.

Security remains foundational as enterprises expand digital footprints. Sonata enables adoption of Zero Trust architectures aligned with leading hyperscaler frameworks, leveraging identity governance, threat intelligence, and continuous compliance monitoring. Secure AI coding practices are embedded into development pipelines, making security integral—not incremental—to DevSecOps workflows. This ensures continuous verification and robust protection across users, devices, and workloads in highly distributed environments.

Hybrid and multi-cloud adoption is a defining enterprise priority. Sonata supports this through standardized landing zones, API-driven integration, and unified governance, enabling phased migrations, workload coexistence, and consistent operations. AI-enabled FinOps continuously monitors usage, optimizes costs, and improves financial transparency, helping organizations integrate AI-driven operations, robust security, and adaptive multi-cloud strategies to scale innovation and lead in the digital economy."

AI-driven cloud optimisation and Zero-Trust security define enterprise strategy in 2026

ROHAN GUPTA
VP CLOUD, SECURITY & DEVOPS, R SYSTEMS

"After years of aggressive cloud adoption, the conversation with most clients in 2026 has shifted. It is less about moving to the cloud and more about making it work cost-effectively, securely, and manageable at scale across environments, especially as architectures become more complex. In this context, leveraging AI for cloud optimisation, the challenge is rarely a lack of data, but the absence of structured processes to act on. For most enterprises, AI is not about fully autonomous infrastructure yet, but about enabling disciplined, data-driven decision-making on an ongoing basis.

Alongside efficiency, security has become a parallel priority. From a security standpoint, zero-trust is often misunderstood as a product-led approach. At R Systems, we find that foundational gaps persist, such as unreviewed IAM policies and service accounts with excessive permissions. Our approach begins with a comprehensive access and posture audit, followed by a phased implementation: strengthening identity controls, introducing robust secret management, and progressively enforcing workload-level policies. In sectors like financial services and healthcare, accelerating regulatory timelines are making organizational alignment more straightforward due to clear compliance mandates.

Increasing architectural complexity is also shaping cloud strategy. Our priority is to establish operational visibility through a unified observability layer, standardising infrastructure-as-code practices, and defining a cloud operating model that balances central oversight with autonomy. Ultimately, organisations making meaningful progress are those treating cloud as an ongoing operating discipline grounded in consistency and continuous optimisation."

AI-driven observability and Zero-Trust security empower hybrid cloud transformation

ROHIT SHUKLA
SR SALES DIRECTOR, INDIA AND SAARC, SOLARWINDS

"As organizations rapidly adopt hybrid and multi-cloud architectures, SolarWinds is expanding its observability platform to provide integrated visibility across on-premises and leading cloud environments. By embedding artificial intelligence and automation through innovations like the SolarWinds AI Agent and Root Cause Assist, we accelerate troubleshooting and correlate events to highlight probable causes. This helps enterprises shift from reactive monitoring to predictive operations. As cloud environments scale, we allow organizations to adopt capabilities incrementally while maintaining operational simplicity and flexibility across hybrid IT infrastructures.

A key pillar of our growth is sustained investment in R&D, particularly through our expanded footprint in India. Our new Bengaluru office serves as a strategic innovation hub for next-generation observability and AI-driven IT operations. Furthermore, through the SolarWinds Partner Program and 2026 Partner Summit initiatives, we are empowering our global ecosystem with certification tracks and platform modernization. This ensures partners effectively accelerate the adoption of cloud solutions, improving agility and innovation for enterprises undergoing digital transformation.

SolarWinds enables AI-driven cloud optimization and secure operations by following 'AI by Design' and 'Secure by Design' principles. Our platform unifies observability across on-premises systems and major public clouds, ensuring operational consistency and zero-trust security. By correlating telemetry data in real time, IT teams detect anomalies and resolve issues faster, reducing mean time to resolution. Ultimately, providing this comprehensive visibility is foundational for enterprises to optimize resources and scale confidently."

AI-driven platforms and Zero-Trust security enable scalable hybrid and multi-cloud transformation

SONIA AHLUWALIA
VP – CLOUD PRACTICE, KYNDRYL INDIA

"Kyndryl is shifting to an AI-driven, platform-based cloud model, leveraging hyperscaler innovation and platform engineering to move from fragmented setups to integrated, business-focused environments. In this model, AI and agentic AI are embedded into operations to modernize and automate IT. Rather than treating cloud as an end in itself, we position it as a foundational layer enabling AI adoption at scale. By adopting site reliability engineering and collaborating with hyperscalers like AWS, Azure, and Google Cloud, Kyndryl manages increasing multi-cloud complexity while delivering ongoing business value.

Our strategy is built around a structured transformation framework and an end-to-end services portfolio covering the full cloud lifecycle. We prioritize platform-first transformation, aligning cloud initiatives to business outcomes through scalable platforms supported by governance and automation. To support growth, Kyndryl integrates FinOps practices for cost visibility and leverages a global, cloud-certified workforce to deliver complex programs. This approach helps deepen customer relationships and supports long-term revenue growth by enabling consistent, enterprise-scale modernization within a hybrid IT model.

Kyndryl helps organizations achieve faster time-to-market by modernizing legacy systems and enabling cloud-native development. We provide a unified operating model that integrates AI-driven optimization, full-stack observability, and zero-trust security. By embedding centralized governance and consistent policy enforcement across dynamic infrastructures, we ensure secure hybrid and multi-cloud adoption. This allows customers to manage workloads across environments with consistent visibility, ensuring reliable, seamless operations and the ability to innovate continuously without added complexity."

AI operations and Zero-Trust security drive reliable hybrid cloud

SURESH RAMANI
CEO, TECHGYAN

"In 2026, cloud strategy has matured into a leadership test: can we run technology with predictable uptime, controlled risk, and explainable costs? The conversation is no longer 'where do we host' but 'how do we operate'—with AI-assisted operations, identity-first Zero Trust, and hybrid/multi-cloud as the default reality. On operations, the fastest wins come from better signal quality and repeatable response. We use Azure Monitor alerting with dynamic thresholds and machine learning to flag anomalies, reducing noise. Where fixes are well understood, we implement automation-assisted remediation through runbooks, ensuring response becomes consistent, auditable, and less dependent on individual heroics.

For capacity, we apply predictive autoscale, providing clearer operational KPIs and improved recovery confidence anchored in monitoring and governance through DataCenter 365. On cost control, we focus on governance that finance can trust, using budgets and alerts to create accountability. On security, SecureIT 365 prioritises MFA, Conditional Access, and continuous verification, while the Threat Protection Envisioning format surfaces misconfigurations across email, devices, and identities.

For hybrid and multi-cloud, we reduce disruption by standardising foundations, using Azure Arc to extend management across locations. Finally, responsible AI is a change program; our Copilot Workshops focus on readiness and governance, while the Data Security Immersion Briefing anchors compliance in Microsoft Purview concepts. In 2026, CIOs will be judged by how reliably they run cloud—securely, measurably, and repeatably."

Balancing Growth with Security: Cyber Readiness in an evolving Tech environment

AS ORGANIZATIONS EXPAND THEIR DIGITAL FOOTPRINT—ESPECIALLY BY ADOPTING DIGITAL PLATFORMS AND ERP SYSTEMS—THEY BECOME MORE EFFICIENT, CONNECTED, AND DATA-DRIVEN. HOWEVER, THIS EXPANSION ALSO INCREASES THEIR EXPOSURE TO CYBER THREATS.

WITH BUSINESSES INTEGRATING AI, CLOUD SERVICES, AND COMPLEX, INTERCONNECTED DIGITAL TECHNOLOGIES, THE ATTACK SURFACE HAS EXPANDED, WITH 81% OF SECURITY LEADERS EXPECTING TO BE TARGETED AGAIN WITHIN THE NEXT 12 MONTHS, ACCORDING TO A RECENT REPORT. AT THE SAME TIME, ATTACKERS ARE BECOMING MORE ADVANCED BY USING AI AND MACHINE LEARNING (ML) TO - AUTOMATE ATTACKS, CREATE HIGHLY CONVINCING PHISHING OR IMPERSONATION ATTEMPTS AND FIND VULNERABILITIES FASTER THAN TRADITIONAL METHODS.

KEY ASPECTS OF CYBER READINESS

- Shifting to Resilience: Cyber resilience—the ability to anticipate, withstand, recover from, and adapt to adverse cyber events—is now as critical as prevention, as it ensures survival over time, according to a 2023 study.
- Proactive Threat Management - A "not if, but when" mentality is necessary. Over half of security leaders (57%) faced a cyberattack in the past year, with cloud malware, credential theft, and API vulnerabilities being the most common methods.
- Focus on Core Security Pillars - Effective readiness is driven by continuous risk assessment, robust compliance (e.g., ISO 27001, NIST), and rapid, effective incident response, which, according to studies, positively impact an organization's innovation and performance.
- AI and Emerging Technologies - While AI is a key area for investment in security automation, it is also a major driver of new, sophisticated threats. 54% of security leaders cite AI-generated threats as a pressing concern, requiring AI-powered defense mechanisms.
- Addressing the Skills Gap - There is a significant gap between the sophistication of modern cyber defenses and the knowledge of individuals, with only 35% of leaders feeling they have enough resources to deal with current risks.

Strengthening cyber resilience is the utmost necessity to ensure an organization to not only prevent these attacks but also detect, respond to, and recover quickly if something goes wrong. So, while an organization is growing digitally and implementing ERP systems, one must simultaneously build strong, intelligent security systems to withstand increasingly sophisticated AI-driven cyber threats.

IN SHORT – GROW YOUR DIGITAL CAPABILITIES—BUT MAKE SURE YOUR CYBERSECURITY EVOLVES JUST AS FAST!

Strengthening cyber resilience with Threat intelligence

DR. MAKARAND SAWANT
DIRECTOR & CTO, SEAFB

"We have implemented AI enabled platform with Threat intelligence and automated response for all our mission critical applications to strengthen cyber resilience against all sophisticated attacks across all threat vectors. At the same time, we have implemented cloud based AI platform with Threat intelligence having cybersecurity capabilities like SOAR, Zero Trust and SASE.

As data protection gains prominence, our organization is gearing up for full compliance with the DPDP Act. For compliance with DPDPA, we are focusing on strong Identity and Access management systems with automated response, data classification and policies for data protection."

Shifting personal data governance from a compliance exercise to an operational function

PRINCE JOSEPH
GROUP CHIEF INFORMATION OFFICER - SFO TECHNOLOGIES PVT. LTD. (NEST GROUP)

"As digital transformation accelerates through ERP modernization and generative AI adoption, cyber resilience must scale at the same pace. In our organization, we treat security as a foundational design principle rather than a post implementation control. As we expand Microsoft Dynamics 365 and integrate manufacturing systems into a connected digital thread, every interface, API and identity layer is evaluated through a zero trust lens.

AI driven threats today are adaptive and automated. We are witnessing sophisticated phishing content, intelligent scanning for exposed services and rapid exploitation cycles. To counter this, we have converged network and security operations into a unified monitoring model that provides end to end visibility across endpoints, identities and ERP transactions. Role based access, segregation of duties and continuous log monitoring are embedded within ERP environments to reduce misuse risk.

Resilience also depends on recoverability. We have strengthened multi-layer backup strategies with periodic restore validation and conduct simulated cyber response drills to test readiness. For us, cyber resilience is not just about preventing breaches. It is about ensuring operational continuity even when disruption attempts occur.

COMPLYING WITH THE DPDP ACT

The Digital Personal Data Protection Act requires organizations to treat personal data governance as an operational discipline rather than a compliance exercise. Our approach begins with visibility. We are conducting structured data discovery and classification exercises across ERP, HRMS and collaboration platforms to understand where personal data resides and how it flows.

Data minimization is being enforced by reviewing forms, retention practices and redundant data fields. Consent capture and purpose documentation mechanisms are being strengthened so that processing activities are transparent and defensible. Incident reporting workflows are aligned with breach notification timelines to ensure regulatory readiness. Third party risk governance is also a critical focus. Vendors handling payroll, analytics or support functions are being assessed for contractual safeguards and operational alignment with data protection standards. Data protection metrics are now included in executive dashboards to ensure board level oversight. In regulated manufacturing and aerospace supply chains, trust is a competitive differentiator. Compliance with the DPDP Act is therefore not seen as an obligation alone. It is a reinforcement of our commitment to responsible data stewardship, operational integrity and sustained."

Countering AI threats with intelligence-driven strategy

DR. RAKHI R WADHWANI
CHIEF OPERATIONS AND COMPLIANCE OFFICER (ICT BUSINESS UNIT), ISOQAR (INDIA) PVT. LTD

"Cyber Resilience today has to be built into the foundation of every digital and ERP expansion; it cannot be an afterthought. AI driven threats are faster and more adaptive, so our defense strategy is equally intelligence-led. We are embedding zero-trust principles, AI-based anomaly detection, and continuous threat monitoring directly into platform architecture. Just as importantly, we run regular simulation exercises and recovery drills so that if an incident occurs, business operations can continue with minimal disruption. Our focus is not only on preventing breaches, but on ensuring rapid recovery and decision readiness.

Safety must be part of every new project from the start. AI Threats move very fast. Our defense uses smart technology to keep up. We use strict access rules and watch for odd behavior. We run drills to make sure we can get back to work quickly. We focus on stopping attacks and fixing problems fast.

INVESTING IN TOOLS, PROCESSES & SKILLING

We are investing across three layers: people, process, and technology. On the people side, we are upskilling teams in secure digital operations, AI risk awareness, and incident response. On the process side, we are embedding secure-by-design and privacy-by-design standards into every transformation program, along with tighter access governance and third-party risk controls. From a tool perspective, we are strengthening identity management, extended threat detection, data loss prevention, and ransomware-resilient backup capabilities. Trust is protected when security becomes part of everyday operations, not just a specialized function.

We are approaching data protection as a governance transformation that includes enterprise-wide data mapping, stricter data minimization, stronger consent and preference management, and clearly defined workflows for data subject rights. We are also strengthening vendor controls and audit trails so that compliance is demonstrable, not theoretical. Most importantly, we are building employee awareness and accountability around responsible data handling. Our goal is to move beyond compliance toward building long-term digital trust with customers and partners. We treat data safety as a way to run the whole company. We track where all our data lives. We only collect what we need. Users get clear ways to manage their info. We also check on our partners to keep things safe. Our goal is to build real trust with our customers. This goes beyond just following rules."

Cybersecurity is a business enabler that ensures secure, scalable digital transformation

YOGENDRA SINGH

HEAD-IT/SAP, BARISTA COFFEE COMPANY

"As a CXO at Barista Coffee Company, cyber resilience is embedded into our digital growth strategy. With the rise of AI- and ML-driven attacks, we have adopted a Zero Trust architecture, strengthened identity and access controls with MFA and role-based policies, and deployed advanced EDR and next-generation firewall solutions that use behavioral analytics to detect threats in real time.

As we expand our ERP and digital platforms, including SAP HANA, POS, and cloud integrations, we follow a secure-by-design approach—ensuring encryption, regular VAPT assessments, network segmentation, and continuous patch management. We also maintain immutable backups and conduct regular disaster recovery drills to safeguard against ransomware. Equally important, we invest in employee awareness and third-party risk governance to secure our entire ecosystem. For us, cybersecurity is not just protection—it is a business enabler that ensures secure, scalable digital transformation.

DPDP READINESS

At Barista Coffee Company, we recognize that the DPDP Act is not just a regulatory requirement but a trust mandate. We are aligning our data governance framework to ensure full compliance while strengthening customer confidence. First, we are conducting a comprehensive data mapping and classification exercise to identify what personal data we collect across POS systems, loyalty platforms, ERP, and digital channels. This helps us minimize data collection and define clear retention policies.

Second, we are reinforcing consent management mechanisms, ensuring transparent notices, purpose limitation, and easy opt-in/opt-out options across customer touchpoints. Third, we are strengthening access controls, encryption, and audit trails within our SAP HANA, cloud platforms, and third-party integrations to safeguard personal data. We are also formalizing data principal rights processes—including mechanisms for data access, correction, and erasure requests—along with a structured incident response and breach notification framework aligned with regulatory timelines.

Finally, employee awareness and vendor risk governance remain key pillars to ensure ecosystem-wide compliance. We also believe that for protecting trust and ensuring business continuity requires balanced investments across skills, processes, and technology. Together, these investments ensure that as we scale digitally, customer trust, operational stability, and data protection remain uncompromised."

CAN CYBER READINESS TRAINING MITIGATE THE IMPACT OF AN ATTACK?

It is true that cybersecurity readiness is currently failing to keep pace with the speed of technological evolution. While organizations are accelerating digital transformation (cloud, APIs, hybrid work), cyber risks are compounding faster than digital value creation. In 2026, the reliance on Generative AI has made it both a critical productivity catalyst and a significant risk amplifier, enabling more sophisticated, automated attacks

As cyber threats become more sophisticated, often powered by AI, cyber readiness training plays a crucial role in strengthening an organization's overall security posture. It ensures that employees are not just aware of risks but are also equipped to act quickly and responsibly when faced with potential threats. Cyber readiness training prepares people to recognize, prevent, and respond to cyberattacks effectively.

The 2025 Security Awareness and Training Global Research Report released by Fortinet shows security awareness training is rapidly evolving from a routine compliance exercise into a measurable control for reducing cyber risk. One of the strongest findings in the report is that training works. Sixty-seven percent of organizations report moderate or significant reductions in intrusions, incidents, and breaches after implementing security awareness and training.

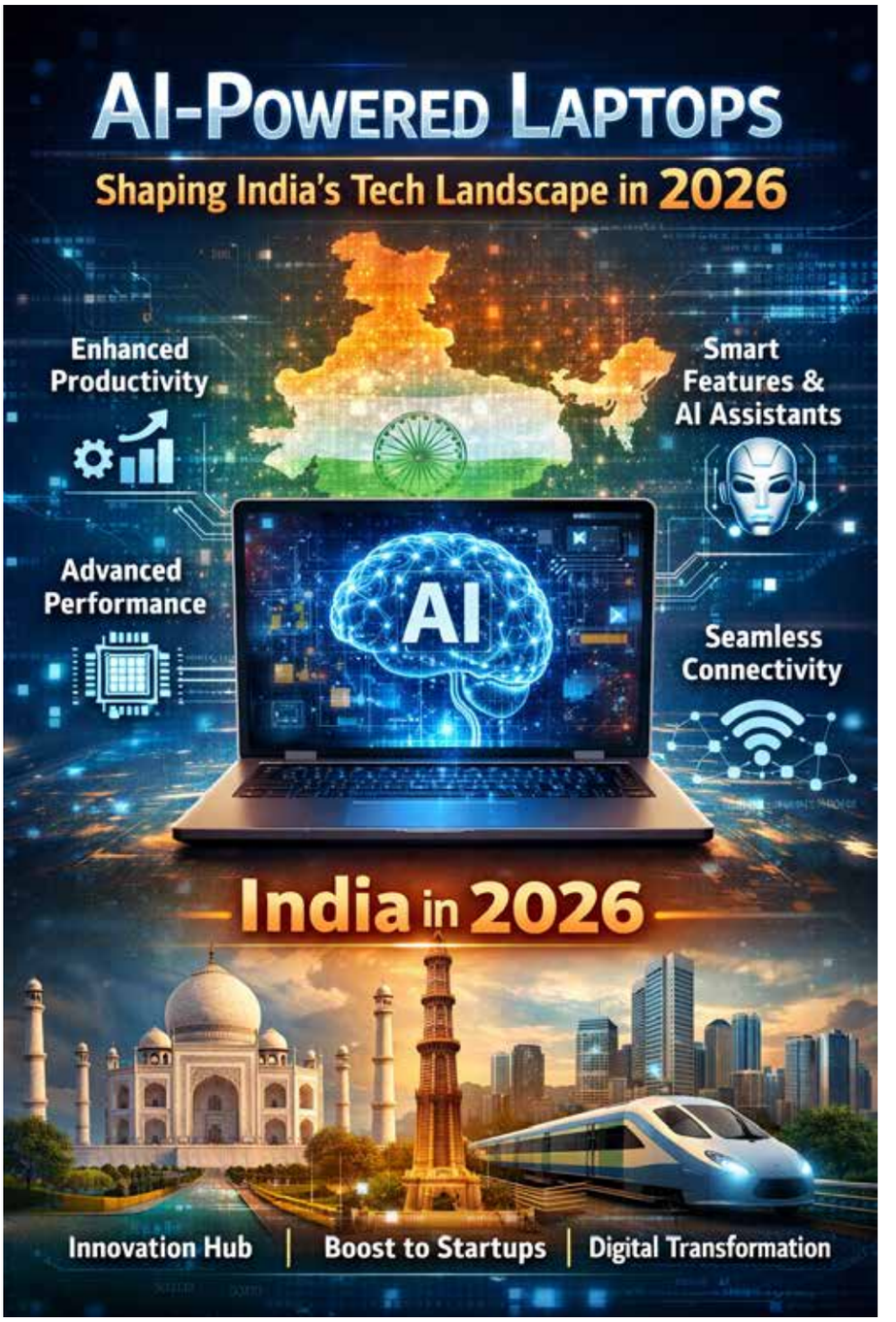
Security awareness training reduces incidents. And organizations that invest in it and measure it see real results. But AI is accelerating both attacker capabilities and business adoption. At the same time, insider risk is growing. And too many programs still lose impact because of low completion rates or outdated content. To be effective, training has to be continuous, relevant, and treated as a core risk management control, not a side project.

Most leaders now see security awareness as a shared responsibility across the organization, not just an IT or security function. Nearly all are also open to using policy to manage high-risk behavior, especially when it is paired with training that explains the rationale behind those policies.

This is an important shift. Effective security awareness training is not just about passing a test. It is about shaping daily decisions, reinforcing good behavior, and reducing risk where work actually happens.

AI Laptops set to redefine India's Tech Future in 2026

INDIA'S DIGITAL TRANSFORMATION IS ENTERING A NEW PHASE IN 2026—ONE WHERE COMPUTING IS NO LONGER JUST ABOUT SPEED OR STORAGE, BUT INTELLIGENCE. AT THE CENTER OF THIS SHIFT ARE AI-POWERED LAPTOPS, RAPIDLY REDEFINING HOW INDIVIDUALS AND ENTERPRISES INTERACT WITH TECHNOLOGY.



In 2026, the best laptop for driving productivity in India is no longer just about speed or specifications. CXOs now view their laptops as secure AI-enabled productivity partners embedded within enterprise workflows. These ideal devices are capable of securely running AI models, support global mobility, ensure long lifecycle value beyond standard refresh cycles, and minimize risk. In an AI-first environment, laptops are believed to deliver secure, resilient, worry-free performance.

Unlike traditional systems, these next-generation laptops are equipped with dedicated Neural Processing Units (NPUs), enabling on-device AI capabilities such as real-time language translation, intelligent automation, enhanced cybersecurity, and personalized user experiences. This shift from cloud-dependent AI to edge computing is not only improving performance but also addressing data privacy and latency concerns.

The momentum is significant. Industry estimates suggest that AI-enabled PCs are quickly moving toward mainstream adoption, with a substantial share of devices now designed to handle AI workloads natively. Moreover, enterprise adoption is accelerating, with forecasts indicating that AI PCs could dominate business purchases by 2026.

In India, the impact is particularly transformative. AI-powered laptops are enabling businesses to streamline operations, enhance decision-making, and drive innovation. From startups leveraging AI for analytics to large enterprises automating workflows, these devices are becoming critical tools for productivity and competitiveness.

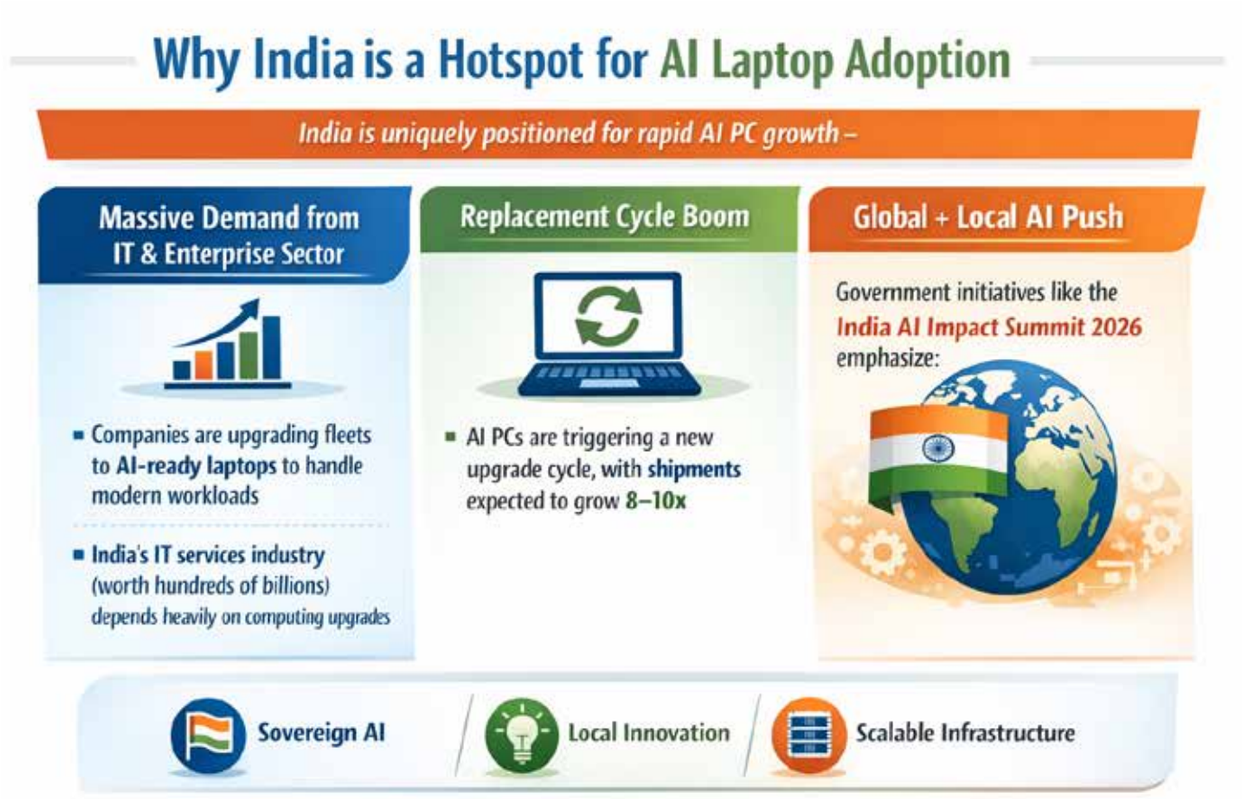
For professionals and creators, AI laptops are unlocking new possibilities. Tasks such as video editing, design, coding, and content creation are becoming faster and more intuitive. Features like AI-assisted writing, predictive analytics, and real-time collaboration are redefining everyday workflows. At the same time, global tech giants are aggressively investing in this space. From lightweight AI ultrabooks to high-performance machines designed for intensive workloads, manufacturers are embedding AI across product categories to deliver smarter and more adaptive computing experiences.

However, this transformation is not without challenges. The demand for AI-capable hardware is driving up component costs, with laptop prices expected to rise significantly due to increased demand for advanced processors and memory. Additionally, adoption in price-sensitive markets like India may take time as consumers weigh the cost against tangible benefits. Rising High-bandwidth memory (HBM) demand is causing DRAM shortages, with prices up 18–25% and possibly 50% by 2026, raising AI infrastructure costs.

So is increasing memory costs slowing down consumer demand and innovation in the PC market?

Currently the leading innovation driver in the PC market is the inclusion of on-device AI processing to build more use cases and applications of edge AI. However, this transition will now be delayed as a key component associated with on-device AI processing is memory, which is getting more expensive and less available. According to Gartner, while the memory crisis represents its own challenge, the integration of high-performance NPUs too is adding more expense to the BOM costs. Advanced 3nm and 2nm chip manufacturing costs have increased and forced vendors to abandon the sub-$750 price point for AI PCs – the price that would have drove greater adoption. Instead, AI PCs are likely to remain a premium niche through 2026.

There are other innovations underway in the PC market such as foldable/rollable



displays but creating relevant experiences on top of display hardware that maximizes their utilization requires applications will utilize memory and as such these displays will be restricted to premium devices that require more memory.

BUT NONETHELESS...

Despite these hurdles, the trajectory is clear. AI-powered laptops are evolving from niche innovations to essential digital tools, aligning with India's broader ambitions of becoming a global technology hub. As businesses, students, and creators embrace this new generation of computing, AI-powered laptops are not just enhancing productivity—they are reshaping India's entire technology landscape. India remains competitive, highlighting the need for innovation and contingency planning.

AI-powered laptops becoming the foundational infrastructure for India's AI-first enterprise future

INDRAJIT BELGUNDI
SENIOR DIRECTOR & GENERAL MANAGER, CLIENT SOLUTIONS GROUP, DELL TECHNOLOGIES INDIA

"India is experiencing a defining moment in its technology evolution, with AI-powered laptops emerging as the foundation of enterprise digital strategy. As per IDC, India's traditional PC market recorded its strongest year ever in 2025 indicating that the country's PC userbase went through an overhaul as Microsoft ended support for Windows 10. According to Gartner, IT spending in India is expected to reach $176.3 billion in 2026, an increase of 10.6% from 2025, and AI PCs are a critical hardware pillar driving this momentum. From a productivity standpoint, AI PCs can deliver up to 12%-time savings per day per employee, while certain workloads consume 42–49% less power than cloud equivalents. This contributes to both business efficiency and sustainability goals.

INFLUENCING CREATORS, BUSINESSES & STUDENTS

As a global leader in commercial PCs, we are driving the next wave of productivity by bringing AI capabilities directly to the end-user, supported by a growing ecosystem of over 100 ISVs building applications for on-device NPUs. AI PCs are changing the game on tech deployment and management. AI momentum accelerates when compute sits beside the people doing the work. For teams pushing the boundaries of what's possible with AI especially those building autonomous agents, fine-tuning LLMs, or working with sensitive data the Dell Pro Max with GB10 is changing the economics and control of AI development. Companies are leaning on AI PCs to keep AI use under IT's purview, keeping data secure and local. Businesses are also witnessing up to 58% power savings by offloading tasks for NPU to perform in the background, supporting both operational efficiency and attaining sustainability goals.

For creators, local AI acceleration is dramatically transforming workflows. Toolkits like Dell Pro AI Studio are compressing AI application development cycles from six months to as little as six weeks. This was previously possible only with expensive cloud platforms or high-end workstations, but thanks to AI PCs, it is now accessible directly on the device.

For students and mobile professionals, users have an option to choose a product that best meets their needs. AI PCs are delivering exceptional battery life alongside intelligent assistance tools like Copilot, making high-performance, AI-enabled computing accessible across diverse learning and professional environments. This is particularly significant for India, where digital access remains uneven across geographies.

Our scale, go-to-market model and long-standing supplier relationships differentiate us, and provides tangible advantages in periods of disruption. We are managing this environment in real time, applying lessons from prior cycles, and continuing to offer customers value."

Laptops evolving from being simple Productivity Tools into Intelligent Companions

SANJEEV MEHTANI
CHIEF SALES OFFICER, ACER INDIA

"AI-powered laptops are significantly reshaping India's technology landscape by bringing advanced AI capabilities directly to the device. We are seeing a shift from traditional computing to AI PCs that can process workloads locally, enabling faster performance, stronger data privacy, and reduced dependence on the cloud. At Acer India, we see AI laptops transforming how professionals, creators, and students work by enabling smarter productivity tools, real-time collaboration, and personalized computing experiences. Features such as on-device AI assistants, intelligent video conferencing, and automated workflows are making everyday computing far more efficient.

AI PCs are also helping enterprises accelerate digital transformation, allowing organizations to run AI applications securely on devices while improving operational efficiency. In a diverse and fast-growing digital economy like India, AI-powered laptops will play a critical role in democratizing access to AI, supporting innovation, and enabling a new generation of intelligent computing experiences for businesses and consumers alike.

TRANSFORMING BUSINESS, STUDENTS, AND CREATOR LANDSCAPE

AI-powered laptops are set to significantly transform how businesses, students, and creators work. With dedicated AI processors and on-device capabilities, these systems can run complex AI workloads locally, enabling faster performance, improved privacy, and reduced reliance on cloud connectivity.

For businesses, AI laptops enable smarter productivity tools from real-time meeting enhancements and automated workflows to advanced security features, helping teams collaborate and make decisions more efficiently. For students, these devices unlock new learning possibilities through AI-assisted research, coding support, real-time transcription, and personalized learning tools. Creators, meanwhile, benefit from accelerated content workflows, including faster video editing, image processing, and AI-driven design assistance that dramatically reduces production time.

As AI capabilities continue to move closer to the device, laptops will evolve from being simple productivity tools into intelligent companions that can adapt to user behaviour, optimize performance, and empower users to work more creatively and efficiently. In a fast-digitizing market like India, this shift will play a crucial role in enabling individuals and organizations to innovate, scale, and compete in the AI-driven economy."

MSI's approach is centered on making AI performance both powerful and accessible

JAMES SUNG
NB SALES DIRECTOR OF INDIA, MSI

"At MSI, we see a clear transition towards on device AI, where NPUs handle everyday workloads locally, enabling faster performance, better battery efficiency and reduced reliance on constant connectivity. At the same time, India's 'slash generation' is driving demand for devices that can seamlessly support gaming, content creation and productivity on a single machine, without compromising on performance. This is also accelerating the move towards portable high performance laptops that combine desktop level capability with mobility and intelligent optimization.

AI-POWERED LAPTOPS - THE WAY FORWARD IN 2026

AI powered laptops are set to fundamentally transform how India works, learns and creates in 2026 by embedding intelligence directly into everyday computing. For businesses, this will translate into sharper productivity and faster decision making, with AI automating routine workflows and enabling real time insights. For students, these devices have started evolving into personalized learning companions that simplify research, content creation and knowledge access in a more intuitive way.

For creators, the shift is even more significant. With on device AI and advanced GPUs, tasks like video editing, design and 3D workflows become faster, more efficient and less dependent on the cloud, enabling greater flexibility and control. What ties all of this together is the move towards a single, high performance device that can intelligently adapt to different needs. AI powered laptops are not just enhancing productivity, they are redefining how seamlessly users across India can switch between work, learning and creation.

At MSI, our approach is centered on making AI performance both powerful and accessible. We are actively collaborating with our component partners to ensure a more stable supply chain, while expanding our portfolio with diverse configurations that cater to different user needs and price points. At the same time, advancements in NPUs and overall system optimization are enabling us to deliver robust AI capabilities without an overdependence on high memory capacities.

Beyond hardware, we also believe in giving back to the community and nurturing young talent. We actively collaborate with the Google Developer Community to host both physical and online workshops, empowering individuals with the latest AI skills, from building personal language models to optimizing performance with newer models like Llama 3. Ultimately, our goal is to deliver the right balance of performance, longevity, and value, while fostering a strong developer ecosystem that encourages innovation and makes AI computing more accessible for all."

Should PC makers rethink pricing strategies as supply constraints persist?

RISHI PADHI
PRINCIPAL ANALYST, GARTNER

"Escalating memory costs are driving PC bills of materials (BOMs) to record highs. Given that vendors (OEMs) typically operate within fixed margin structures, they have limited capacity to absorb these cost increases. As a result, the additional expense is being passed on to end-users, and this this will erode device affordability and triggering a contraction in shipment volumes. We anticipate that PC shipments will decline by a significant double-digit percentage this year, primarily due to these price pressures.

The consumer segment is expected to bear the brunt of this impact, not because of a lack of demand, but because higher prices are likely to make consumers more cautious with their discretionary spending. In contrast, business and enterprise buyers are likely to adopt a more strategic approach. With budgets already set, many organizations will prioritize pre-emptive purchasing and collaborate closely with channels to mitigate the full impact of anticipated price increases, particularly as these hikes are expected to intensify in the second half of the year.

MANAGING SURGING MEMORY PRICES IN 2026

The first half of 2026 has emerged as a critical window for vendors and channels to optimize pricing and protect margins before component inflation further compresses profitability in the latter half of the year. One of the most visible strategies is the shift toward premium devices. Manufacturers are concentrating their limited memory supplies on high-end laptops and workstations where higher margins can better absorb the increased costs. For major vendors like HP, Dell, and Lenovo, this has meant prioritizing AI PCs and enterprise grade workstations, which recorded a standout performance in India during 2025. These larger vendors are better positioned to navigate supply constraints than mid-range vendors, as they possess greater leverage with suppliers and larger inventory reserves.

At the lower end of the price spectrum, vendors are striving to maintain market presence without incurring significant disruptions. Some are exploring limited product redesigns to reduce overall memory requirements. This is why Apple's MacBook Neo has created so much attention by introducing a product with aggressive pricing while being restricted to 8GB of memory and keeping adequate performance. While Apple has successfully identified a pricing sweet spot, this does not necessarily translate into improved supply for this segment. Availability remains a concern, as memory manufacturers are prioritizing high-bandwidth memory (HBM) production for AI datacenters, diverting resources away from consumer-grade devices. As the year progresses, particularly in the second half, PC vendors are expected to carefully recalibrate pricing strategies while navigating ongoing supply challenges to maintain profitability amid volatile component costs."

Gartner analysts forecast AI PC shipments will total 143 million units and are projected to represent 55% of total PC market in 2026, while it was 31% of the total PC market globally by the end of 2025. By 2029, AI PCs will become the norm. Worldwide shipments of AI PCs was projected to total 77.8 million units in 2025.

Gartner expects that by end of 2026, 40% of software vendors will prioritize investments in AI capabilities directly on PCs, up from 2% in 2024. In the same year, multiple small language models (SLMs) will run locally on PCs, up from zero in 2023.

DATA PRIVACY:
A Shared Responsibility

FOR EVERY RUPEE SPENT RESPONDING TO A DATA BREACH, THE REAL COST IS MEASURED IN SOMETHING FAR HARDER TO REBUILD — TRUST.

India's digital economy is generating data at a pace that its regulatory architecture is still scrambling to match. With over 900 million internet users and enterprise cloud adoption accelerating across every industry vertical, the country sits atop one of the world's largest, and most exposed, pools of personal data. The numbers tell an uncomfortable story. Cybersecurity incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024, according to government data. Cybercrime losses are projected to reach ₹20,000 crore across sectors in 2025, with banking and financial services alone accounting for ₹8,200 crore. And the average cost of a single data breach in India has reached an all-time high of ₹19.5 crore in 2024, up 39% since 2020, according to IBM's annual Cost of a Data Breach Report.

The question is no longer whether data privacy matters. It is who, exactly, is responsible for it, and whether that responsibility is being shared equitably across the ecosystem. The honest answer, for most organisations, is no.

INDIA'S REGULATORY MOMENT — NOW WITH A DEADLINE

For years, enterprises deferred DPDP compliance decisions, citing the absence of notified rules. That window has closed. MeitY formally notified the Digital Personal Data Protection Rules, 2025 on November 13, 2025, operationalising the DPDP Act, 2023 after more than two years of legislative and consultative process. The Data Protection Board of India (DPBI) has been established and the compliance clock is now running.

The rollout is phased: procedural provisions and the DPBI framework became effective immediately from November 14, 2025; consent manager registration obligations kick in by November 2026; and all substantive compliance obligations including privacy notices, consent systems, security safeguards, breach protocols, and data principal rights infrastructure, must be fully operational by May 13, 2027. Violations can attract penalties of up to ₹250 crore per breach of obligation. That is not an 18-month grace period, it is an 18-month implementation runway, and organisations that treat it as the former will find themselves structurally exposed on Day 1 of full enforcement.

The DPDP Rules introduce specific, operational obligations. Data Fiduciaries must issue clear, standalone privacy notices before collecting data; implement technical controls including encryption, masking, access controls, and visibility logs; maintain audit logs for at least one year; and report data breaches to the DPBI within 72 hours. Significant Data Fiduciaries face additional constraints, including restrictions on cross-border transfer of traffic data. The framework draws from established global privacy principles, GDPR in the EU, PDPA in Singapore, CCPA in California, while reflecting India's own digital scale and policy priorities.

For the VAR and system integrator community, this transition window is not a compliance challenge to be observed from the sidelines. It is a commercial and advisory opportunity of the first order.

THE MYTH OF THE SINGLE ACCOUNTABLE PARTY

Ask most organisations who owns data privacy, and the answer will lead you to the CISO's office, or perhaps legal and compliance. That framing is dangerously outdated.

Under the DPDP Act, the primary accountable entity is the Data Fiduciary — the organisation that determines the purpose and means of data processing. But accountability within that organisation cannot, and should not, sit with a single function. The CISO manages security controls. The Chief Data Officer, where one exists, governs data architecture and quality. Legal interprets regulatory obligations. HR manages employee data and consent. Marketing runs customer consent workflows. Every business unit that touches personal data is, in effect, a node in the privacy accountability chain.

The breakdown typically occurs at the seams between these functions. A marketing team launches a new data collection workflow without looping in legal. A business unit onboards a SaaS application without informing IT, creating an unsanctioned data flow. A vendor receives a data extract for analytics without a proper data processing agreement in place.

None of these failures are malicious. Most are structural, the result of organisations that have built data practices around operational convenience rather than privacy architecture.

Cloud complexity compounds the challenge considerably. According to IBM's 2024 Cost of a Data Breach Report, 34% of data breaches in India involved data stored on public clouds, with breaches in public cloud environments costing the most — an average of ₹22.7 crore per incident. Incidents spanning multiple cloud environments took the longest to identify and contain, 327 days on average. The same report found that 35% of breaches globally involved shadow data, with those breaches costing 16% more on average and taking significantly longer to detect. Data sprawl is not a metaphor — it is a measurable operational liability.

India's breach record in recent years illustrates the stakes concretely. In 2024 alone, Hathway's data breach exposed the personal information of over 41.5 million customers; BSNL suffered an intrusion that put sensitive subscriber data — including IMSI numbers and SIM card details — up for sale on dark web marketplaces; and boAt saw the personal records of 7.5 million customers compromised. Each breach followed a familiar pattern: governance gaps, inadequate access controls, and delayed detection.

THE CHANNEL OPPORTUNITY: FROM RESELLER TO TRUSTED ADVISOR

For VARs, MSPs, and system integrators, the DPDP Rules create a regulatory inflection point that demands a strategic response. Any entity that processes personal data on behalf of a Data Fiduciary — which describes the function of virtually every MSP and SI with a managed services contract — qualifies as a Data Processor under the framework. This carries real legal obligations: adherence to contractual data processing terms, implementation of security standards prescribed under the Rules, and breach notification requirements.

Channel partners that have not reviewed their customer contracts and data handling practices through a DPDP lens are carrying unquantified legal exposure. The first step is internal housekeeping: understanding what personal data flows through service delivery infrastructure, and on whose behalf it is being processed.

The broader opportunity lies in what the channel can offer customers who are themselves underprepared. India's cybersecurity domestic market was valued at approximately USD 4 billion in 2024 and is on a growth trajectory, according to DSCI. The cybersecurity products segment alone generated revenue of USD 4.46 billion in 2025 and is projected to reach USD 5.98 billion in 2026, growing 25% year-on-year, according to DSCI CEO Vinayak Godse at the Annual Information Security Summit 2025. Privacy-driven spending on data classification, consent management, DLP, and DSPM is a rising share of that market.

Data Security Posture Management platforms, which provide continuous visibility into where sensitive data lives, who has access to it, and whether it is appropriately protected, are moving from early adopter to mainstream procurement conversations in Indian enterprise accounts. The channel partner that can walk into a boardroom and connect these technology investments to regulatory risk mitigation, reputational protection, and customer trust, rather than simply presenting a product stack, earns a strategic advisory relationship, not a transactional one.

THE HUMAN FACTOR: CULTURE EATS POLICY

Technology and regulation can establish the conditions for good data privacy practice. They cannot, by themselves, produce it. According to IBM's India data, phishing and stolen or compromised credentials were the most common initial attack vectors, each accounting for 18% of incidents, with business email compromise the costliest root cause at ₹21.5 crore per breach on average. These are not purely technical failures. They are human ones.

Privacy fatigue is a real phenomenon. Employees who are subjected to annual compliance training, typically a checkbox exercise — retain little actionable knowledge and develop no meaningful instinct for privacy risk. The emergence of generative AI tools has introduced an entirely new category of shadow data risk. Employees across functions are routinely feeding customer records, internal analyses, and personally identifiable information into AI assistants and productivity tools that sit entirely outside the organisation's data governance perimeter.

IBM's 2025 Cost of a Data Breach Report found that 61% of organisations lack AI governance technologies, even among those that have governance policies in place. Only a minority perform regular audits for unsanctioned AI. The gap between what employees are doing with AI tools and what IT and security teams know about is, in most Indian enterprises, substantial, and growing.

Building a genuine privacy culture requires visible leadership commitment, the appointment of Data Protection Officers or privacy leads with real authority, and the kind of ongoing contextual communication that connects privacy principles to specific workflows. The IBM data shows that organisations in India which deployed security AI and automation extensively shortened their breach lifecycle by 112 days and spent ₹13 crore less per breach on average — yet 72% of studied Indian organisations have limited or no use of these technologies. The preparedness gap is real, and it is measurable.

TECHNOLOGY AS ENABLER AND MULTIPLIER OF RISK

The same technologies transforming Indian enterprises are also expanding the surface area of data privacy risk. India's cyberspace is the second most targeted in the world, facing increasing ransomware, phishing, and supply chain attacks, according to the Carnegie Endowment for International Peace. Between 2019 and 2023, cyber attacks on the Indian government increased by 138%.

Zero-trust architecture, which assumes no implicit trust for any user, device, or workload, has become foundational to modern security design, and it serves privacy objectives as well. By enforcing granular access controls and eliminating broad ambient access to data, zero-trust reduces the blast radius of both external breaches and insider incidents. Privacy-enhancing technologies such as differential privacy, federated learning, and data tokenisation are moving from research into enterprise product roadmaps, driven by both regulatory pressure and the commercial imperative to extract value from data without compromising individual privacy.

DSPM and consent management platforms are gaining traction particularly in BFSI and healthcare, India's two most regulated sectors and, not coincidentally, its two most breach-exposed. The DPDP Rules' specific requirements around encryption, masking, and access visibility are accelerating procurement conversations that had previously stalled at the evaluation stage.

TOWARD A SHARED ACCOUNTABILITY MODEL

Data privacy cannot be owned by a single team, solved by a single technology, or legislated into existence by a single law. It is, by its nature, a distributed responsibility, one that requires aligned action from regulators, enterprises, channel partners, technology vendors, and individuals simultaneously.

The DPDP framework has permanently changed the calculus. With the Data Protection Board now established, a three-phase enforcement timeline running to May 2027, and penalties of up to ₹250 crore per violation waiting at the end of that runway, compliance is no longer a future-state aspiration. It is a time-bound operational imperative.

Organisations that treat the current phased rollout as an extension of the old ambiguity will find themselves structurally exposed when full enforcement begins. Those that use this window to build genuine privacy accountability — across people, processes, and technology, will find that it pays dividends well beyond regulatory compliance. And the channel partners that help them get there will have earned something more durable than a product sale.

In a digital economy built on data, trust is infrastructure. And infrastructure, once neglected, is expensive to rebuild.

OpenAI Appoints Former JioStar CEO Kiran Mani to Lead APAC Operations

OpenAI has appointed former JioStar digital CEO Kiran Mani as Managing Director for Asia-Pacific. He will join in June, relocate to Singapore, and report to Chief Strategy Officer Jason Kwon, as the company strengthens its regional expansion strategy.

Mani brings over two decades of experience across digital media, technology and consumer internet sectors. At JioStar, he led product, growth and digital strategy, helping scale one of India's fastest-growing streaming platforms. His expertise in building large-scale digital ecosystems is expected to support OpenAI's efforts to deepen partnerships across the region.

In his new role, Mani will oversee business strategy, partnerships and market expansion across APAC, including India and key Asian markets. The move aligns with OpenAI's growing focus on India as a major AI market, amid rising competition from global and regional players.

Saviynt Ropes in Alex Lei as SVP of Sales for APJ to Drive Regional Growth

Saviynt has appointed Alex Lei as Senior Vice President of Sales for Asia Pacific and Japan (APJ). Based in Singapore, he will lead the regional sales organisation as enterprises accelerate investments in identity security to support cloud adoption, AI initiatives and evolving digital environments.

In this role, Lei will oversee customer acquisition, partner strategy and go-to-market execution across APJ. Todd Rotger, Chief Revenue Officer at Saviynt, said the region is witnessing strong demand for identity security, and Lei's leadership will help expand the company's footprint and support customers managing complex identity challenges.

Lei joins from Ivanti and has held senior roles at Proofpoint and Dell EMC. He brings extensive experience in enterprise sales and will focus on strengthening engagement and advancing identity security strategies across the APJ market.

Motorola Names Ipshita Chowdhury as India Marketing Head

Motorola has appointed Ipshita Chowdhury as Marketing Head, India, to lead brand strategy and integrated campaigns. She succeeds Gagandeep Bedi, who has been elevated to Asia Pacific Marketing Strategy and Operations Lead. Both will report to Shivam Ranjan, Marketing Head, Asia Pacific, Motorola.

The transition highlights Motorola's focus on strengthening India growth while enhancing regional alignment. Ranjan said India remains a key market and Chowdhury's cross-sector experience will help deepen consumer engagement and scale the brand. Chowdhury said she aims to build stronger consumer connections and accelerate growth momentum.

Chowdhury brings over two decades of experience, with leadership roles at Nokia, Microsoft and Philips Lighting. Meanwhile, Bedi will drive regional strategy across APAC. Motorola India continues to see strong growth, supported by an expanding portfolio and increasing consumer preference.

Former Tata Electronics, Adani CISO Dharmesh Rathod Joins Alterego as Group CISO

Alterego Technology has appointed Dharmesh Rathod as Group Chief Information Security Officer and Member of the Board. A former CISO at Tata Electronics and Adani Group, Rathod will strengthen cybersecurity governance as the company expands its consulting and managed security services portfolio.

The appointment reflects Alterego's focus on embedding cybersecurity at the board level. Nikunjsinh Matieda, Managing Director of Alterego Technology, said Rathod's experience in building enterprise-scale security programmes will support the company's growth and reinforce governance-led resilience across enterprise and industrial environments. Rathod brings nearly three decades of experience across sectors including semiconductors, energy and logistics. He has also held leadership roles at Essar Group and Welspun Group. In his new role, he will oversee cybersecurity strategy and contribute to strengthening critical infrastructure and governance-driven security frameworks globally.

Adobe Appoints Shamik Basu as VP for Creative Products Group in India

Adobe has appointed Shamik Basu as Vice President, Creative Products Group in India. Based in Noida, he will lead engineering and product management teams, reporting to Ely Greenfield, Chief Technology Officer, Creative Products Group., and join the India leadership team to drive innovation and growth.

Highlighting India's strategic importance, Greenfield said the country plays a key role in advancing creator-first, AI-driven experiences at scale. He noted that Basu's expertise in building large-scale intelligent platforms will strengthen local leadership and improve global alignment. Basu said he looks forward to collaborating with teams to shape next-generation creative technologies.

Basu joins from Microsoft with over three decades of experience. He will work on products including Firefly, Photoshop and Premiere, while strengthening India's role in Adobe's global innovation ecosystem and expanding its influence in AI-led creativity.

Amit Luthra Appointed One Lenovo Commercial Leader for India

Lenovo India has expanded the mandate of Amit Luthra, appointing him as One Lenovo Commercial Leader to drive a unified commercial vision and strengthen go-to-market execution across the country. The move is designed to deliver a more seamless, integrated experience while addressing the evolving needs of enterprise customers across industries.

Luthra will continue as Managing Director of the Infrastructure Solutions Group (ISG), leading growth across servers, storage, and hyperconverged solutions. The "One Lenovo" initiative aligns regional and global priorities, strengthens enterprise partnerships, and accelerates adoption as organisations invest in scalable, future-ready digital ecosystems and infrastructure modernisation.

With nearly 12 years at Dell Technologies and leadership roles at Sun Microsystems and HCL Infosystems Ltd., Luthra brings deep domain expertise. His experience will support Lenovo's customer-centric strategy and strengthen its position in India's rapidly evolving enterprise technology landscape.

Transforming Modern Cybersecurity

Why Risk Operations Center (ROC) Is Essential to Unify Risk Management

In today's digital landscape, cybersecurity is not just technology; it's about managing risks within the broader business context. The modern CISO faces an expanded attack surface, fueled by cloud environments, IoT devices, and remote work setups. With over 31,000 new vulnerabilities disclosed globally in 2023 alone, traditional, siloed methods, that are often checklist-driven and without business context, fall short.

The disconnected tools lead to inefficiencies, inflated budgets, and fragmented risk management efforts. CISOs must redefine the concept of a "risk surface" and align security strategies with business priorities. A **Risk Operations Center (ROC)** becomes essential, enabling CISOs to unify and coordinate responses to evolving risks in real time across the enterprise with an integrated approach for effective risk management.

Risk Operations Center (ROC)

Qualys Enterprise TruRisk™ Management (ETM), the world's first cloud-based Risk Operation Center, provides a centralized platform to enable a ROC, allowing security teams to elevate risk management to a strategic level while ensuring continuous oversight and data-driven decision-making. Qualys ETM provides a centralized platform to enable a ROC, allowing security teams to elevate risk management to a strategic level while ensuring continuous oversight and data-driven decision-making.

Qualys Enterprise TruRisk Management (ETM)

Scan Now

Visit us at qualys.com/roc or call us on +1 800 745 4355

v250131

shivaami

6 TIME GOOGLE CLOUD PARTNER OF THE YEAR

SIMPLIFY | SECURE | SCALE

Transform Today!

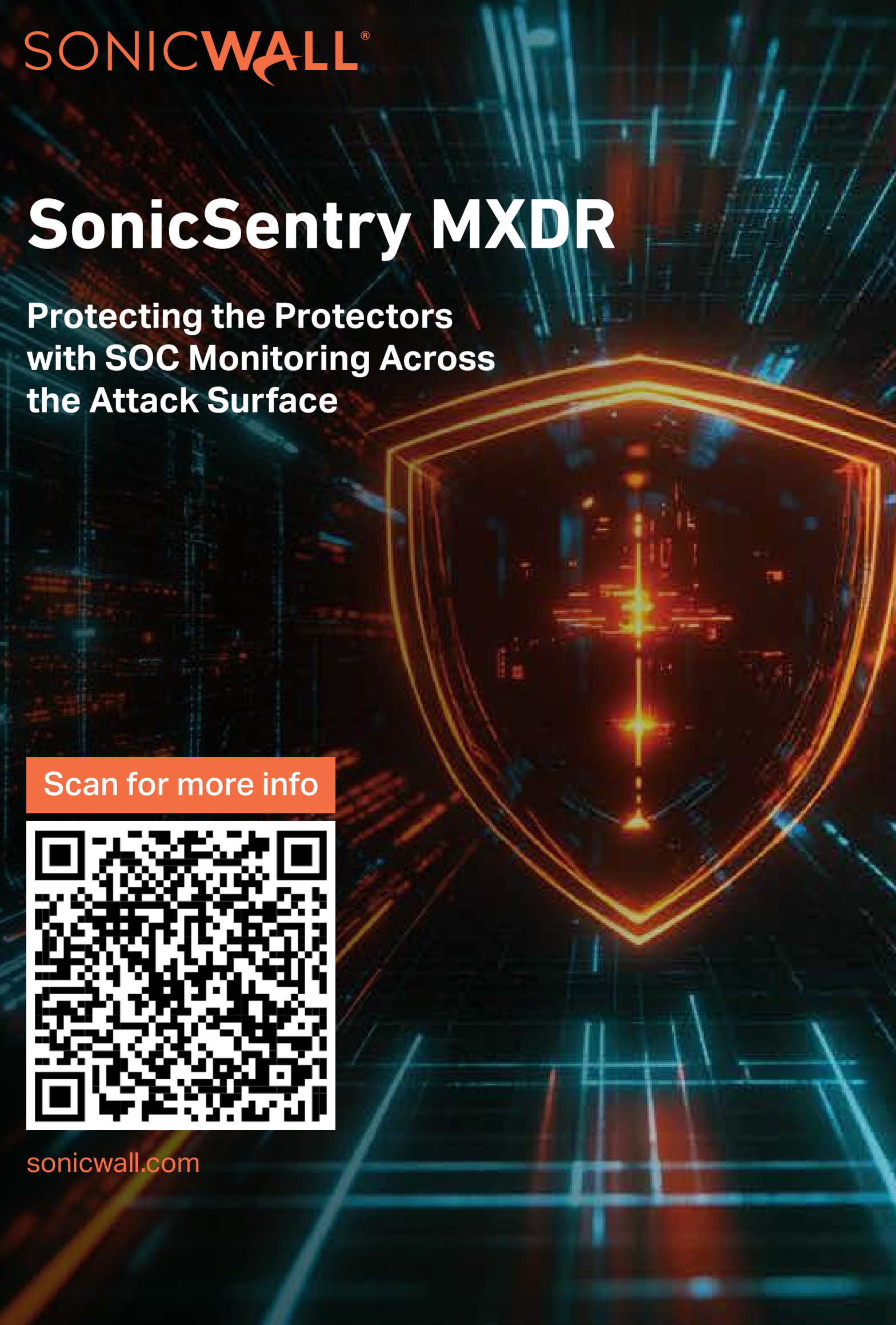
Scan to Explore

www.shivaami.com

SONICWALL®

SonicSentry MXDR

Protecting the Protectors with SOC Monitoring Across the Attack Surface



Scan for more info

sonicwall.com

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