

SME CHANNELS

India's leading IT magazine for channel business

VOLUME 16 | ISSUE 10 | PAGES 44 | DECEMBER 2025 | RS. 250/-



SMART IT / 16
Orienting with a New Turb
Service Delivery Centre with
Next-Gen NOC & SOC



AI / 17
Stark geographical and
generational divides in AI
uptake and digital wellbeing



GUEST ARTICLE / 28
The Rise of Antifragile
Workforces: How HR Can Help
Organizations Thrive Amid
Disruption



CHANNEL ACCELERATOR AWARDS 2025 A CELEBRATION OF EXCELLENCE, INNOVATION, AND INDUSTRY LEADERSHIP

Attracting robust participation from over 200 key partners from areas as diverse as digital transformation, cloud, cyber security, automation,...**Page..18**

Introducing Dell Pro Essential.

Explore the newest entries to the Dell Pro lineup — business-ready laptops with essential security and manageability features.



Options to fit your business needs.

Dell Pro Essential laptops available in two sizes and with a range of Intel® Core™¹ or AMD Ryzen™² processors.



Dell Pro 15 Essential

Featuring smooth performance and a numeric keypad, this 15" laptop blends portability and productivity. Ideal for everyday workflows and seamless multitasking.

Plastic (PC+ABS): Starting at 3.59 lbs (1.63 kg)
Aluminum: Starting at 3.64 lbs (1.65 kg)

Dell Pro 14 Essential

Portable 14" laptop with smooth performance and a roomy 16:10 aspect ratio for mobile productivity. Designed for everyday workflows and seamless multitasking wherever you work.

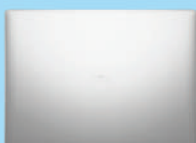
Plastic (PC+ABS): Starting at 3.40 lbs (1.54 kg) Aluminum: Starting at 3.44 lbs (1.56 kg)

Professional designs with commercial-grade durability.

Dell Pro Essential laptops are available with optional chassis materials and colors³; crafted to meet military-grade standards (MIL-STD) for proven reliability.



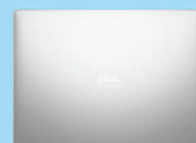
Carbon Black
(Plastic: PC+ABS)



Platinum Silver
(Plastic: PC+ABS)



Midnight Blue
(Aluminum)



Platinum Silver
(Aluminum)

Please Contact

Iris Global Services Pvt Ltd

1, Bypass Road, Mahipalpur, New Delhi- 110037

Shivani Saini: +91 98998 77471

shivani.saini@irisglobal.in



IRIS GLOBAL

SME CHANNELS

India's leading IT magazine for channel business



AI / 29
AI Adoption in Cybersecurity
Surging Ahead



CYBERSECURITY / 30
AWS re:Invent 2025:
Advancing Next-Gen SIEM
and Cloud Security Access
on AWS



CYBERSECURITY / 31
eScan enhances Enterprise
DLP with ChatGPT Tenant
Control, Addressing Critical
Data Sovereignty Gap

EDITORIAL

INDO-RUSSIA GROWING BONHOMIE: IMPLICATIONS FOR THE INDIAN IT INDUSTRY

MANASH RANJAN DEBATA
manash@accentinfomedia.com



India and Russia have shared a time-tested strategic partnership rooted in defence, energy, space cooperation, and diplomacy. In recent years, this relationship has gained renewed momentum as both nations seek to navigate a rapidly shifting geopolitical and economic order. Beyond traditional sectors, the strengthening Indo-Russian bonhomie is now opening new frontiers for collaboration in the technology and IT ecosystem—an area increasingly central to global power and economic growth.

One of the most direct impacts of closer India–Russia ties is the expansion of technology exchange and joint innovation. Russia possesses advanced capabilities in areas such as cybersecurity, artificial intelligence (AI), semiconductors, quantum computing, and space technologies. Indian IT firms, known globally for software services, cloud computing, and digital transformation, are well-positioned to complement Russian strengths in deep-tech research. Joint R&D centers, technology parks, and startup collaborations could accelerate innovation while reducing overdependence on Western technology ecosystems.

Another major implication lies in the growing demand for secure and sovereign digital infrastructure. As global technology becomes increasingly politicised, both India and Russia are focusing on digital sovereignty. This creates opportunities for Indian IT companies to provide software solutions in cybersecurity, fintech, e-governance, telecom infrastructure, and data centers for Russian enterprises and public-sector projects. With global sanctions limiting Russia's access to Western IT vendors, Indian firms can emerge as trusted alternative partners for software services, enterprise solutions, and digital modernization.

The expanding cooperation in defence technology is also spilling over into the civilian IT sector. Defence digitalisation, AI-driven surveillance systems, supply-chain digitisation, and logistics software are becoming key areas of collaboration. Indian IT companies with experience in defence digitization and secure systems may find new, high-value projects in Russia's military-industrial ecosystem, further pushing India up the global value chain from services to strategic technology solutions.

For Indian startups and SaaS companies, the Indo-Russia partnership opens access to a relatively underexplored but high-potential market. Russia's strong engineering talent, combined with India's scale and software expertise, can fuel cross-border innovation in edtech, health tech, blockchain, and AI platforms. At the same time, payment systems, cross-border data regulations, and digital trade frameworks will need alignment for smoother collaboration. **SME**

MY EXPERIENCE

Huawei MateBook Fold Ultimate

Huawei MateBook Fold Ultimate is a futuristic premium laptop designed for users who seek performance, portability, and innovation in one device. Its foldable display allows it to transform effortlessly between laptop, tablet, and presentation modes, making it highly versatile for work and creativity. It runs on a powerful operating system optimized for multitasking and smooth performance. The stunning high-res foldable screen delivers immersive visuals with fluid touch response.

SPECIAL FEATURE : FOLDABLE OLED DISPLAY, PREMIUM ULTRA-SLIM DESIGN, HIGH-PERFORMANCE PROCESSOR, TOUCH AND STYLUS SUPPORT, ADVANCED COOLING SYSTEM, FAST CHARGING, LONG BATTERY LIFE, AI-POWERED FEATURES



FINAL WORD:

The Huawei MateBook Fold Ultimate stands out for its innovative foldable design and premium build quality. It offers fast charging, smooth performance, and an exceptional viewing experience. Whether used for professional work, creative tasks, or media consumption, this device delivers a truly next-generation computing experience.

contents

VOLUME 16
ISSUE 10

2025

DEC

SME CHANNELS
Trusted Advisor of Channel Business

Publisher: Sanjib Mohapatra
Group Editor: Sanjay Mohapatra
Editor: Manash Ranjan Debata
Designer: Deepak kumar
Web Designer: Sangeet Kumar
Technical Writer: Manas Ranjan
Lead Visualizer: DPR Choudhary

MARKETING

Marketing Manager: Annie Garg
Events Marketing: Vipin Negi
Circulation and Printing: Rajkumar Hansa

SALES CONTACTS

Delhi 6/102, Kaushalya Park, Hauz Khas
New Delhi-110016
Phone: 91-11-41055458 / 8587835685
sanjeev@smechannels.com

Bangalore

#28/1, 3rd Floor, Sri Lakshmi Krupa, Near
Shamanna Park, Model House Street,
Basavanagudi, Bangalore - 560004
Ph. No. +91 88618 21044
Mumbai Tahmeed Ansari
2, Ground Floor, Park Paradise, Kay-Bees CHS.
Ltd., Opp. Green Park, Oshiwara, Andheri (west),
Mumbai - 400 053.
Ph. +91 22 26338546, Fax +91 22 26395581
Mobile: +91 9967 232424
E-mail: Info@smechannels.com

Kolkata

S Subhendu
BC-286, Laxmi Apartment, Kestopur
Kolkata-700101
Phone: 9674804389

EDITORIAL OFFICE

Delhi: 6/103, (GF) Kaushalya Park, New Delhi-
110016, Phone: 91-11-40587445
info@smechannels.com

Bangalore

#28/1, 3rd Floor, Sri Lakshmi Krupa, Near
Shamanna Park, Model House Street,
Basavanagudi, Bangalore - 560004
Ph. No. +91 88618 21044 E-Mail info@
accentinfomedia.com



CHANNEL ACCELERATOR AWARDS 2025: A CELEBRATION OF EXCELLENCE, INNOVATION, AND INDUSTRY LEADERSHIP /18

Attracting robust participation from over 200 key partners from areas as diverse as digital transformation, cloud, cyber security, automation, AI, etc, representing top Partners, Vendors. ISVs, SIs and VADs, India's largest channel fiesta came up as a spectacular success

AI



COMMVault / 32
"Commvault's Data Rooms: Safely
Connecting Enterprise Data with
AI Platforms"

CYBERSECURITY



RISK PROFILER / 33
"RiskProfiler Makes it to
Onstage's Top 100 Startups
List"

GUEST ARTICLE



CHECKPOINT / 36
"Strengthening Security in the
AI and Post-Quantum Era"

more inside

Editorial	03
Snippets	05
Product	38

Printed, Published and Owned by

Sanjib Mohapatra
Place of Publication: 6/101-102, Kaushalya
Park, Hauz Khas
New Delhi-110016
Phone: 91-11-46151993 / 41055458
Printed at Karan Printers, F-29/2, 1st floor,
Okhla Industrial Area, Phase-2, New Delhi
110020, India.

All rights reserved. No part of this publication
can be reproduced without the prior written
permission from the publisher.

Subscription: Rs.200 (12 issues)

All payments favouring: Accent Info Media
Pvt. Ltd.

NETWORK BLIND SPOTS IN FOCUS AS NETPOLEON INDIA ONBOARDS GARLAND TECHNOLOGY FOR INDIAN MARKET



Netpoleon India, a leader in enterprise cybersecurity solutions and part of the global Netpoleon Group, today announced the onboarding of Garland Technology, a pioneer in network visibility solutions, into its India portfolio. This strategic alliance aims to enhance India's cybersecurity infrastructure amid rising digital transformation demands.

Bridging Network Visibility Gaps

The collaboration brings Garland Technology's industry-leading network packet brokers, network TAPs, hardware data diodes, and bypass switches to Indian enterprises. These tools are designed to enhance threat detection, optimize traffic monitoring, and ensure compliance with India's evolving data sovereignty regulations.

"As India's industries accelerate their digital journeys, invisible network vulnerabilities pose critical risks," said Mohan Kumar TL, Director of Netpoleon India. "Garland Technology's solutions empower organizations to eliminate blind spots, enabling real-time insights into encrypted and lateral traffic – a game-changer for sectors like fintech and smart manufacturing."

Garland Technology's entry into the Indian market via Netpoleon India underscores its commitment to the region's cybersecurity growth potential. "India's network complexity requires adaptive solutions," said Michael Fisher, AVP - APJ, Garland Technology. "With Netpoleon's regional expertise, we're delivering battle-tested visibility tools that scale with India's 5G and edge computing boom."

NTT DATA Announces Six New AI-Powered Cyber Defense Centers

NTT DATA officially launched four next-gen autonomous Cyber Defense Centers powered by AI technologies in Bengaluru, Hyderabad, Noida and Mumbai, with two additional centers set to open in Birmingham (UK) in Dec 2025 and Dallas (USA) by Jan 2026.

These purpose-built Cyber Defense Centers reinforce NTT DATA's strategic focus on modernizing cybersecurity for

the AI era. They represent a shift from traditional centralized security operations to a distributed, AI-driven, hyper-automated model that learns from past incidents and human expertise to automate, triage and prioritize alerts, accelerate investigations and incident response, contain threats faster and support regional data privacy and cybersecurity regulations. According to Omdia,

autonomous Security Operations Centers (SOCs) will become the industry standard within two years, positioning NTT DATA as a leading example of how the industry is evolving toward autonomous cyber resilience.

The next-generation Cyber DefenseCenters combine human security experts and AI agents to defend against evolving cyber threats. AI agents autonomously

triage, analyze and hunt potential incidents, reducing investigation time by up to 60%, enabling teams to contain threats earlier in the kill chain. By

automating high-volume, repetitive tasks, these capabilities free security analysts to focus on higher-value work such as digital forensics, containment and recovery.

Securonix Enters Strategic Partnership with Orient Technologies to Deliver Advanced AI-powered SIEM Capabilities Across India

Securonix, Inc. announced a strategic partnership with Orient Technologies, a prominent player in the transformative IT solutions domain. In the MSSP space, Orient offers a full spectrum of cybersecurity solutions, with a focus on proactive security measures. The partnership aims to address the rapidly evolving digital threat landscape by driving impactful innovation in cybersecurity with Unified Defense SIEM powered by Agentic AI for the modern Security Operations Centre (SOC) experiences to customers across India.

This critical alliance further supports Securonix's growth strategy in India, leveraging Orient Technologies' extensive knowledge of the regional cybersecurity landscape. By integrating Securonix's cutting-edge, Agentic AI, advanced analytics, and ML capabilities with Orient Technologies' technical expertise and strong local presence, the partnership seeks to equip businesses and PSUs with robust, proactive security measures.

"Growing digital transformation, surge in cyberattacks, evolving regulatory compliance and shortage of cybersecurity talent drive strategic collaborations that deliver meaningful impact. Orient's local expertise and established network across India make it an ideal partner for Securonix," said Dipesh Kaura, Country Director, India & SAARC, Securonix.

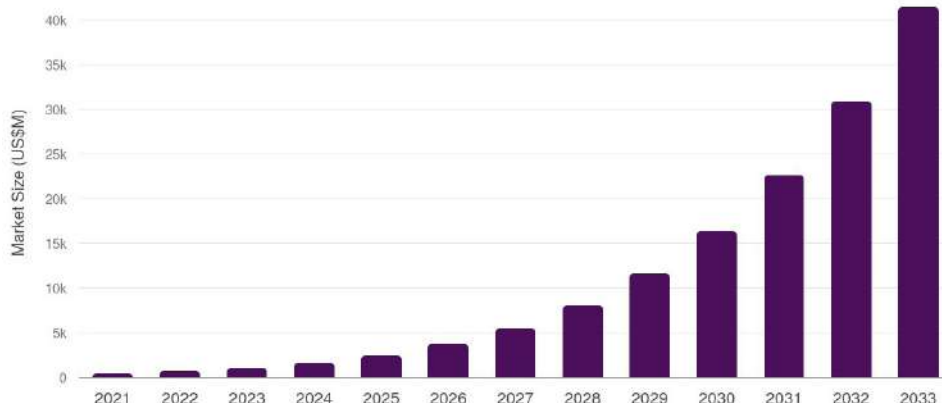
Observability Delivers Up to 10x ROI for Telcos: New Relic Study

Honeywell launched their all-India Building Automation Xpress Roadshow, a mobile experience campaign designed to showcase Honeywell's latest innovations in Fire Detection and Alarm System, STQC Certified Video Surveillance, Access Solutions, Building Management System and Electrical Products. The initiative, aligned with the automation megatrend, commenced at the Honeywell Growth Symposium, held on October 31 in Bangalore.

Honeywell Growth Symposium brings together business leaders and technology experts, and Honeywell's senior leadership to explore the future of innovation and growth in India. The two-day event will feature strategic discussions on digital transformation, sustainability, and automation, alongside collaborative sessions on co-innovation and an evening celebrating achievements in technology and growth.

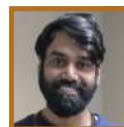
The Honeywell Building Automation Xpress Roadshow was officially flagged off today by Ashish Modi, President, Honeywell India, Bilal Hammoud, President and CEO, Honeywell Building Automation, Shailen Chauhan, Chief Commercial Officer, Honeywell Building Automation, and Atul Pai, Vice President and General Manager for India, ASEAN & East Asia, Building Automation, Honeywell India.

India Edge Computing Market, 2021-2033



(Source: Grand View Research)

EXECUTIVE MOVEMENT



RAPOO APPOINTS GAURAV RAWOOL AS MARKETING HEAD - INDIA, MEA & SAARC



KEEPER SECURITY APPOINTS TIM STRICKLAND AS CHIEF REVENUE OFFICER



ZETWERK APPOINTS JAI SHANKAR KRISHNAN AS INDEPENDENT DIRECTOR



INSPIRA ENTERPRISE APPOINTS SWETHA SRIVASTAVA AS PRACTICE HEAD - DATA ANALYTICS AND AI

TRANSFORMING SMART HOME NETWORKS

Seamless connectivity, intelligent design & performance you can rely on - all from D-Link.

Whole Home Mesh Router



AQUILA PRO AI



EAGLE PRO AI



Whole Home Mesh Router

Home Wi-Fi



5G/4G Router



PDQC Chargers, Power Strip & Cable



ADDON

Wireless Adapters



*All D-Link wireless routers are MTCTE certified

NETGEAR and Riedel Communications Strike Global Technology Partnership

NETGEAR, a leading provider of intelligent networking solutions designed to power extraordinary experiences, has announced a global technology partnership with Riedel Communications, known for its innovative tools that power live production across media, sports, and entertainment. As a first step, the collaboration brings together NETGEAR AV's managed switches in the M4350 series with Riedel's cutting-edge MediorNet MuoN A processing SFPs to deliver ST 2110 Gateway functionality for decentralized signal distribution over standard IP networks.

Now underway and spanning global markets, the partnership begins with Riedel carrying NETGEAR's M4350-16V4C Fully Managed Switch (VSM4320C) — a high-performance 25G/100G switch featuring 25G SFP28 ports, 100G uplinks, and SMPTE ST 2110 Grandmaster and Boundary Clock functions. NETGEAR's switches provide seamless connectivity and reliable, stable performance, enabling robust AV-over-IP systems for broadcast, live events, and commercial AV installations.

"At Riedel, we are always looking for ways to streamline workflows and enhance reliability for our customers," said Louis Caron, Senior Product Manager Video at Riedel Communications. "Partnering with NETGEAR allows us to offer a proven networking backbone."

Keeper Security Appoints Tim Strickland as Chief Revenue Officer

Keeper Security, the leading provider of zero-trust and zero-knowledge cybersecurity software protecting passwords and passkeys, infrastructure secrets, remote connections and endpoints, today announces the appointment of Tim Strickland as Chief Revenue Officer (CRO). Strickland will lead Keeper's global revenue organisation, driving go-to-market strategy, customer growth and channel expansion as demand accelerates globally for modern Privileged Access Management (PAM) and identity security solutions.

Strickland brings more than two decades of executive leadership experience scaling high-performance revenue teams at category-defining SaaS companies. Most recently, he served as Chief Revenue Officer at ZoomInfo, where he guided the company through a successful IPO, built its customer growth and strategic sales functions and oversaw the go-to-market integration of eight acquisitions.

Prior to ZoomInfo, Strickland held senior revenue leadership roles at Marketo, where he played an integral role in the company's growth, its take-private acquisition by Vista Equity Partners and subsequent sale to Adobe.

Manufacturing Industry Blocks More Ransomware Attempts: Sophos Study

Sophos, a global leader of innovative security solutions for defeating cyberattacks, today announced new findings from the Sophos State of Ransomware in Manufacturing and Production 2025 report. The study reveals that manufacturers are stopping more ransomware attacks before data can be encrypted; however, adversaries are increasingly stealing data and using extortion-only tactics to maintain pressure. As a result, more than half of manufacturing organizations impacted by encryption paid the ransom despite progress in defensive measures. The report is based on an independent survey of 332 manufacturing organizations that were hit by ransomware in the last year.

"Manufacturing depends on interconnected systems where even brief downtime can stop production and ripple across supply chains," said Alexandra Rose, Director of Threat Research, Sophos Counter Threat Unit. "Attackers exploit this pressure: despite encryption rates falling to 40%, the median ransom paid still reached \$1 million."

DE-CIX and Epsilon Telecom Expand Partnership to Power AI Adoption

DE-CIX, a leading Internet Exchange (IX) operator, has upgraded global interconnectivity provider, Epsilon Telecommunications, to Premium Reseller Partner status within the DE-CIX R³ (Resell, Refer, Reach) Partner Program. The expanded partnership strengthens DE-CIX's reach across the Asia-Pacific region to support surging enterprise demand for robust, low-latency connectivity, while expanding Epsilon's service offerings for customers.

Enterprise connectivity demands in the APAC region are changing, driven by growing AI workloads, cloud services, and global digital operations. The region has emerged as the global leader in AI adoption, with 70% of businesses using generative AI compared to the global average of 51% according to Boston Consulting Group. Epsilon's role as a Premium Reseller Partner enables it to meet evolving customer requirements and offer DE-CIX's full portfolio of interconnection services globally, including peering, cloud connectivity and enterprise solutions.

"Epsilon and DE-CIX have built a strong, mutually beneficial relationship over the past 13 years, growing together to better serve our customers on a global scale," said Ivo Ivanov, CEO at DE-CIX.

Hexaware Expands Global Footprint with a New Delivery Center in Cair

Hexaware Technologies has strengthened its global delivery network with a new center in Cairo. Launching with 100 professionals, it will serve customers in Egypt, the Middle East, and key European markets.

Located in one of Cairo's leading technology parks, it will provide multilingual CX services in Arabic, English, and major European languages. Egypt's strong education system, high availability of international language skills, and favorable time zone make Cairo a growing hub for digital operations and customer experience services. Hexaware is also engaging with local universities to build a steady pipeline of talent for future growth.

"This delivery center marks Hexaware's entry into a new geography and is a significant expansion of our presence in Egypt," said Amrinder Singh, President & Head of EMEA & APAC, Hexaware. "Cairo gives us access to rich talent and modern infrastructure, allowing us to support our clients more closely as they scale their operations in the region."

Hikvision's Intelligent X-Ray Baggage Scanners Revolutionize Security Screening

Hikvision India has recently introduced the latest next generation intelligent X-Ray baggage scanners. The next-generation X-ray Baggage Inspection Systems include ISD-SC6040S-H4CVL and ISD-SC100100S-H4CVL. These generation X-ray Baggage Inspection Systems are highly effective for security inspections in various application scenarios across the vertical.

Both models are equipped with Raytina 2.0 HD Image Processing, delivering ultra-high-resolution X-ray images that enhance object visibility and operator accuracy. The 120 Hz display ensures smooth operation, reducing eye strain and improving inspection efficiency.

What sets these scanners apart is their Intelligent Recognition Algorithm, capable of automatically detecting over 35 major types of prohibited items across 64 categories, including weapons, explosives, and contraband.

Hikvision's X-Ray Baggage Inspection System utilize multi-color material discrimination technology, identifying organic, and inorganic materials with 3 or 6 color coding.

Sophos Recognized with Microsoft Verified SMB Solution Status

Sophos has announced its integration with Microsoft Defender for Business, Microsoft Defender for Endpoint, and that its Sophos MDR for Microsoft environments solution has achieved Microsoft verified Small & Medium Business (SMB) solution status through the Microsoft Intelligent Security Association (MISA). Microsoft's verified SMB Solution status highlights the crucial role of partner collaboration in protecting small and medium businesses against increasing cyberattacks. By achieving this status, Sophos has demonstrated that its solution is purpose-built for the needs of managed service providers (MSPs) and their SMB customers and is tightly integrated with Microsoft security technology, including Microsoft Defender for Business and Microsoft Defender for Endpoint. Sophos MDR for Microsoft environments detects, contains, and neutralizes attacks within Microsoft 365 environments. It harnesses telemetry from a broad range of Microsoft solutions, including Microsoft 365, Defender for Office 365, Defender for Endpoint, Defender for Cloud Apps, Defender for Identity,

Entra ID Protection, Purview DLP, and more. Combined with telemetry from Sophos and dozens of other vendors,

AI Will Be Key Driver for Margin Gains in 2026: TCS Study

Tata Consultancy Services, in collaboration with Amazon Web Services, today announced the findings of the Future-Ready Manufacturing Study 2025, revealing that global manufacturers are rapidly advancing toward intelligence-driven operations and higher levels of autonomy in manufacturing processes.

The study provides a data-backed view of how manufacturers are strengthening digital and data foundations to support autonomy, decision intelligence, and future-ready operations. While 75% expect AI to become one of the top three contributors to operating margins by 2026, only 21% say they are fully AI-ready, highlighting foundational gaps in data, integration, and system readiness across plants and supply chains.

The study surveyed 216 senior leaders across North America and Europe, representing automotive, industrial machinery, aerospace and defense, process industries, chemicals, and heavy equipment. It examines how enterprises are reshaping their data estates, workforce capabilities, supply-chain transparency, and operational frameworks to prepare for the next era of manufacturing performance powered by AI, cloud, and real-time intelligence.

Armada and LTIMindtree Team Up to Accelerate Edge AI Adoption Across Global Industries

Armada, a hyperscaler for the edge, announced a collaboration with LTIMindtree to expand the reach and deployment of Edge AI, Sovereign AI, and Federated Learning across industries worldwide.

Through this collaboration, Armada will integrate its Galleon modular data centers and Armada Edge Platform (AEP) with LTIMindtree's global delivery and digital transformation capabilities. LTIMindtree will help bring Armada's products to its established enterprise customers and support expansion into emerging markets where Armada does not yet have a presence.

AEP unifies compute, connectivity, and real-world AI into a single, scalable system designed for rugged and distributed environments. Together, Armada and LTIMindtree will enable enterprises in manufacturing, health-care, energy, and other regulated sectors to deploy and manage advanced AI workloads at the edge while maintaining data sovereignty, privacy, and operational continuity.

Check Point Software Unveils Quantum Firewall Software R82.10 to Secure the AI-Driven Enterprise

Check Point Software Technologies Ltd., a pioneering global cyber security solutions provider has announced its new Check Point Quantum Firewall Software, R82.10, introducing 20 new capabilities designed to help enterprises safely adopt AI, protect distributed environments and simplify Zero Trust across hybrid networks.

"As organizations embrace AI, security teams are under growing pressure to protect more data, more applications and more distributed environments," said Nataly Kremer, Chief Product Officer at Check Point Software Technologies. "R82.10 helps enterprises shift to a prevention-first model by unifying management, strengthening Zero Trust and adding protections that support safe, responsible AI adoption and development."

Enterprises are rapidly increasing their use of AI tools and LLM development, expanding connectivity across users, branches and cloud environments. This creates new risks, including AI-generated threats, identity abuse and configuration drift. R82.10 addresses these challenges.

Cloudera Advances Unified Data Access and Governance

Cloudera, has announced a major platform update that integrates Trino, Cloudera Shared Data Experience (SDX), and Cloudera Octopai Data Lineage to deliver unified data access, control, smarter governance, and lineage across the entire data estate. With the power of AI-driven automation and intelligence, enterprises can now seamlessly discover, govern, and access all their data, wherever it resides.

As enterprises accelerate their AI initiatives, data accessibility remains a key barrier to success. According to a recent survey, only 9% of IT leaders report that all of their organization's data is accessible, with just 38% saying that most of their data is usable for AI. For most organizations, data is often trapped in disparate systems with fragmented governance and security policies. This update empowers organizations to unite data silos, securely enable self-service access, and automate governance workflows for improved efficiency and trust in their data without ever moving their data.

COREEL ACQUIRES AEROSPACE & DEFENCE DIVISION OF LEKHA WIRELESS

CoreEL Technologies India Private Limited (CoreEL), a leading provider of advanced electronic system-level products and solutions for the Aerospace and Defence as well as the commercial sectors, has announced the acquisition of Aerospace and Defence System (ADS) division of Lekha Wireless, a Bangalore based wireless communications company. The acquisition brings proven wireless communication technologies, indigenous IP, and a specialised engineering team, strengthening CoreEL's position in Military Communication domain.

The acquisition comes at a time when India's market demand for secure communication solutions specifically in the Aerospace and Defence sector is undergoing significant transition. Customers are increasingly seeking indigenous and product-ready communication systems. The addition of Lekha ADS's capabilities enhances CoreEL's ability to serve these requirements with an advanced set of scalable portfolio of products.

Datadog Launches Bits AI SRE Agent to Resolve Incidents Faster

Datadog, Inc., a monitoring and security platform for cloud applications, has launched Bits AI SRE, an AI agent aware of telemetry, architecture, and organizational context that investigates alerts and surfaces actionable root cause in minutes, giving engineers the information they need to confidently resolve incidents faster, save engineering hours, and reduce end-user and business impact. Unveiled at DASH in Limited Availability, Bits AI SRE is part of Datadog's Bits AI, a suite of AI capabilities that works autonomously across critical monitoring, development, and security workflows to help teams resolve application issues in real time.

Incident response is a high-stakes process for every digital business. When production issues occur, every second of downtime increases the risk of losing customer trust. The challenge is exacerbated as root causes become harder to find amid increasing fragmentation across systems and organizations. Although many teams are eager to adopt AI-powered agents to overcome this burden, point solutions struggle to access and understand the scale and complexity of real production systems.

AI Supercharging Old-School Tactics with New Scal

AI isn't just transforming how we work. It's reshaping how cybercriminals attack, with threat actors exploiting AI to mass produce malicious code loaders, steal browser credentials and accelerate cloud attacks, according to a new report from leading Search AI Company Elastic.

The 2025 Global Threat Report, based on more than 1 billion data points derived from real production environments, finds that generic threats — typically loaders built using AI — jumped 15.5% in the past year, while malicious code execution on Windows nearly doubled to 32.5%.

AI-created malware and easy access to stolen browser credentials are fueling a new class of bad actors who are less reliant on stealth attacks and are leaning into continuous, steady probes for entry into corporate networks.

DIGEST

ESCAN ENHANCES ENTERPRISE DLP WITH CHATGPT TENANT CONTROL

ESCAN, A LEADING CYBERSECURITY SOLUTIONS PROVIDER, HAS INTRODUCED AN ADVANCED TENANT CONTROL FEATURE FOR CHATGPT WITHIN ITS ENTERPRISE DLP PLATFORM. THE NEW CAPABILITY DIRECTLY ADDRESSES ONE OF THE BIGGEST BARRIERS TO ENTERPRISE AI ADOPTION: THE RISK OF SENSITIVE DATA LEAKING THROUGH UNMANAGED PERSONAL AI ACCOUNTS. AS ENTERPRISES INCREASINGLY ADOPT CHATGPT, A CRITICAL GAP HAS EMERGED. EVEN WHEN ORGANIZATIONS PROCURE CHATGPT ENTERPRISE LICENSES FOR THEIR WORKFORCE, EMPLOYEES CAN STILL ACCESS CHATGPT USING PERSONAL ACCOUNTS VIA GOOGLE, APPLE, OR MICROSOFT AUTHENTICATION PROVIDERS, COMPLETELY BYPASSING CORPORATE OVERSIGHT AND CREATING UNGOVERNABLE DATA RISKS.

HITACHI VANTARA UNVEILS HITACHI IQ STUDIO

HITACHI VANTARA, THE DATA STORAGE, INFRASTRUCTURE AND HYBRID CLOUD MANAGEMENT SUBSIDIARY OF HITACHI LTD., HAS ROLLED OUT HITACHI IQ STUDIO, THE LATEST ADDITION TO THE HITACHI IQ PORTFOLIO OF AI SOLUTIONS. HITACHI IQ STUDIO IS DESIGNED TO HELP ENTERPRISES BUILD, DEPLOY AND MANAGE AI AGENTS AND APPLICATIONS AT SCALE, ACTING AS A TURNKEY INTEGRATION HUB WITH A NO-CODE AND LOW-CODE AGENT BUILDER AND A LIBRARY OF INDUSTRIAL AI SOLUTION TEMPLATES THAT ENABLE RAPID PROTOTYPING AND PRODUCTION ACROSS DIVERSE DATA ENVIRONMENTS. THIS HELPS ENTERPRISES OPERATIONALIZE THEIR AI SOLUTIONS FASTER WHILE MAINTAINING FULL CONTROL OVER THEIR DATA AND MODELS.

IIT KANPUR AND NMDC SIGN MOU TO ENHANCE CYBER-SECURITY AND DRIVE AI/ML ADOPTION

THE INDIAN INSTITUTE OF TECHNOLOGY KANPUR (IIT KANPUR) AND NMDC LIMITED, A NAVRATNA PUBLIC SECTOR ENTERPRISE UNDER THE MINISTRY OF STEEL, GOVERNMENT OF INDIA, SIGNED A LANDMARK MEMORANDUM OF UNDERSTANDING (MOU) TO DEEPEN COLLABORATION IN CYBERSECURITY, INFORMATION SECURITY, ARTIFICIAL INTELLIGENCE (AI), MACHINE LEARNING (ML), DIGITAL TRANSFORMATION, AND NEXT-GENERATION TECHNOLOGICAL APPLICATIONS ACROSS NMDC'S IT AND OT ECOSYSTEMS. THE MOU WAS SIGNED BY SATYENDRA RAI, EXECUTIVE DIRECTOR (DIGITAL TRANSFORMATION), NMDC LIMITED, AND DEAN OF RESEARCH & DEVELOPMENT, IIT KANPUR, IN THE PRESENCE OF PROF. MANINDRA AGRAWAL, DIRECTOR, IIT KANPUR, PROJECT DIRECTOR, PROJECT LEADS, AND OFFICIALS FROM NMDC AND I-HUB NTIHAC FOUNDATION (C3IHUB). IIT KANPUR'S C3IHUB WILL SUPPORT NMDC IN CYBER RISK ASSESSMENTS, VULNERABILITY ANALYSIS, SECURITY GOVERNANCE, AND INCIDENT RESPONSE PLANNING.



Win the data race.

Micron® 7600 NVMe™
Enterprise SSD



Best for



Artificial
intelligence



Server
memory
extension



Massive
high-speed
OLTP



High-performance
computing

Speed

12,000MB/s

Capacity

Up to 15.36TB

Warranty

5-year limited

Key Features

- Power loss protection
- Enterprise data path protection
- NVMe® 2.0d, TCG Opal v2.02, OCP 2.6
- NVMe Management Interface (NVMe-MI™) over SMBus
- NVMe® power states
- Firmware activated without reset
- Secure firmware download
- Hardware root of trust, secure signed firmware
- Self-encrypting drive (SED) with AES-256 encryption
- Micron's Secure Encrypted Environment (SEE)
- Self-monitoring and reporting technology (SMART)

Contact us – expert talk

Mr. Sanjeeo Singh
Lead – Enterprise Business
Contact: +91 8800507776

Iris Waves secures Bank of Baroda

Iris Waves, a leading System Integration and Cloud Solution Provider under the Iris Group, has successfully deployed a robust Cloud Security and Endpoint Patch Management Solution for Bank of Baroda (BoB), one of India's largest public sector bank using Persistent' Sentient End Point Manager.

The deployment marks a significant milestone in strengthening BoB's cyber defense and operational resilience. With growing regulatory mandates and increasing sophistication of cyber threats, timely patching and security compliance have become critical for financial institutions. Iris Waves' solution delivers a unified, AI-driven approach to real-time patch management and secure cloud integration - both essential for safeguarding large-scale banking environments.

Under this engagement, Bank of Baroda will now be able to centrally manage and update 75,000 endpoint systems across its nationwide network of branches through a single, unified agent.

The solution not only enhances IT hygiene but also ensures business continuity by minimizing system vulnerabilities and downtime. The project was awarded to Iris Waves with a three-year support contract valued at INR 5 Crore

LogRhythm | Exabeam Expands Saudi Presence with Al Moammar Information Systems Co

LogRhythm | Exabeam, a leading player in intelligence and automation that powers security operations, has expanded its presence in Saudi Arabia by partnering with Al Moammar Information Systems Co., one of the Kingdom's leading IT solution providers, and launching its Customer Innovation Center in Riyadh. These commitments reinforce the Kingdom's cybersecurity foundation and advance the strategic objectives of Saudi Vision 2030.

Under the expanded agreement, MIS and LogRhythm | Exabeam will jointly offer LogRhythm SIEM and the Exabeam New-Scale Security Operations Platform to Saudi-based organizations. The partnership will harden local defenses against digital risk through AI-driven threat detection, improved incident response automation, and proactive threat mitigation. This comes as LogRhythm | Exabeam witnesses strong business growth in the Kingdom, achieving 21% revenue growth from 2024 to 2025, with the goal to maintain high double-digit growth in 2026.

Vertiv and IIT Bombay Join Hands to advance cooling strategies for AI powered Data centers

Vertiv has entered into a strategic collaboration with IIT Bombay. The collaboration is aimed at advancing cooling solutions for AI-driven computing workloads in data centers, an increasingly critical area as India accelerates its digital and technological progress. This collaboration builds on Vertiv's existing partnerships across various educational institutes and IITs across the country where we are developing the skilled workforce required for the operation and maintenance of data centers and helping the industry bridge its talent gap. As AI reshapes industries ranging from healthcare and manufacturing to financial services and urban development, the demand for dependable, high-performance computing infrastructure has increased significantly. Managing this surge requires fresh thinking, strong engineering foundations, and collaborative innovation between industry and academia.

AI Chips to Triple in Value and Become a \$330 Billion Industry by 20

In just five years, the AI chip market has skyrocketed in value, surging over 400% to \$92 billion as of this year. And while this triple-digit growth beats even the broader AI industry by nearly threefold, the momentum shows no signs of slowing any time soon, with the following years bringing just as impressive growth rates. According to data presented by Jemlit.com, AI chips are projected to triple in value and become a \$330 billion industry by the end of the decade.

For the past three years, artificial intelligence has been the top technology, driving innovation, setting new standards, and fueling the tech industry's growth, and AI chips have been at the heart of this change. Giant leaps in machine learning, the rise of cloud computing, and the AI startup boom have driven tech giants like NVIDIA, AMD, and Google to keep improving chip performance, pushing the market to record highs.

The AI chip volume will also skyrocket in this period, surging by 283% from 66.2 billion units in 2025 to a massive 254 billion in 2030.

NETGEAR and Riedel Communications Strike Global Technology Partnership

NETGEAR, a leading provider of intelligent networking solutions designed to power extraordinary experiences, has announced a global technology partnership with Riedel Communications, known for its innovative tools that power live production across media, sports, and entertainment. As a first step, the collaboration brings together NETGEAR AV's managed switches in the M4350 series with Riedel's cutting-edge MediorNet MuoN A processing SFPs to deliver ST 2110 Gateway functionality for decentralized signal distribution over standard IP networks.

Now underway and spanning global markets, the partnership begins with Riedel carrying NETGEAR's M4350-16V4C Fully Managed Switch (VSM4320C) — a high-performance 25G/100G switch featuring 25G SFP28 ports, 100G uplinks, and SMPTE ST 2110 Grandmaster and Boundary Clock functions. NETGEAR's switches provide seamless connectivity and reliable, stable performance, enabling robust AV-over-IP systems for broadcast, live events, and commercial AV installations.

"We always look for ways to streamline workflows and enhance reliability," said Louis Caron, Sr. Product Manager Video at Riedel.

**INK TANK
PRINTERS**

brother
at your side

Newly Launched

PRINTS BEYOND IMAGINATION



DCP-T230
Print • Scan • Copy
MRP ₹ 13,990/-*
(Incl. of all taxes)



DCP-T430W
Print • Scan • Copy
MRP ₹ 15,590/-*
(Incl. of all taxes)



DCP-T530DW
Print • Scan • Copy
MRP ₹ 17,990/-*
(Incl. of all taxes)



***Conditions Apply | *T&C Apply



DCP-T730DW
Print • Scan • Copy
MRP ₹ 22,990/-*
(Incl. of all taxes)

Works with
Apple AirPrint

*Not applicable
for DCP-T230



DCP-T830DW
Print • Scan • Copy
MRP ₹ 25,590/-*
(Incl. of all taxes)



MFC-T930DW
Print • Scan • Copy • Fax
MRP ₹ 35,590/-*
(Incl. of all taxes)



***Free Installation**

on Wi-Fi and Network Models

with standard warranty of 1 year***

FOR SALES ENQUIRIES : Mumbai : Rajesh Phatangare - 9619655576 | Pune, Chattisgarh, Goa, Rest of Maharashtra : Shishir Singh - 9860728548
I Gujrat, MP : Pulin Shah - 9924253604 | Bihar, Jharkhand, Orissa : Deepak Singh - 9771403031 | Telangana, Andhra Pradesh, Karnataka :
Saggive Kumar - 9962000969 | Chennai & Kerala : Govindrajan S - 9176681639 | Delhi, Rajasthan, Haryana : Ashish Kalra - 9899306959 |
Uttar Pradesh, Punjab, Jammu & Kashmir, Uttarakhand : Ajay Saxena - 9919666636 | Kolkata & Northeast : Preetam Panday - 9830472986

MRP mentioned above is for 1 unit and subject to change without prior notice | Yield in accordance with ISO/IEC 24712 (Ink Tank)
| IPM speed is in accordance with ISO/IEC 24734
India EPR Compliance | Entity Name: Brother International (India) Private Limited Plastic Waste EPR No.: BO-13-000-08-AADCBO263E-22
| Battery Waste EPR No.: 6821475 | Thickness for PE bag: 50 microns or above

Now get 24x7 support on WhatsApp **7045 450 450**

www.brother.in

Observability Delivers Up to 10x ROI for Telcos

New Relic, an Intelligent Observability company, has released its State of Observability for Telecommunications and Technology report, which reveals the dramatically different approaches to observability adoption being taken by these two industries. Surveying over 500 engineering leaders and IT team members at telecommunications and technology companies, the report is based on data from the New Relic 2025 Observability Forecast. The report reveals a link between companies using AI and realizing a strong return on investment (ROI) by adopting observability to monitor AI systems. The data also suggests that telcos are betting big on AI-powered observability, while technology companies lead the way in traditional monitoring capabilities.

The research reveals that 57% of telcos and 27% of technology respondents experience high-business-impact outages weekly or more. The cost of this downtime is staggering and a shared concern for both industries. High-impact outages cost telcos an average of \$2 million per hour, compared to \$1.6 million per hour for technology companies. For technology companies, outages can be linked to revenue loss and operational problems, but for telcos, the stakes are higher. An outage can represent a public safety crisis with implications for regulatory action.

eScan enhances Enterprise DLP with ChatGPT Tenant Control

eScan has introduced an advanced tenant control feature for ChatGPT within its Enterprise DLP platform. The new capability directly addresses one of the biggest barriers to enterprise AI adoption: the risk of sensitive data leaking through unmanaged personal AI accounts.

As enterprises increasingly adopt ChatGPT, a critical gap has emerged. Even when organizations procure ChatGPT Enterprise licenses for their workforce, employees can still access ChatGPT using personal accounts via Google, Apple, or Microsoft authentication providers, completely bypassing corporate oversight and creating ungovernable data risks.

When employees use personal ChatGPT accounts for work-related queries, organizations lose all visibility and control over what information gets shared. Unlike corporate accounts where IT teams can access conversation logs through compliance tools, personal account usage creates blind spots that compliance and security teams cannot monitor or remediate. This isn't theoretical risk. Consider recent incidents where confidential information found its way into AI systems. Samsung discovered employees had accidentally leaked proprietary semiconductor designs and meeting notes into ChatGPT.

Honeywell and TotalEnergies pilot AI-assisted control room to accelerate shift to industrial autonomy

Honeywell today announced a collaboration with TotalEnergies for the ongoing pilot of its AI-assisted Experion Operations Assistant at TotalEnergies' Port Arthur Refinery in Texas. The initiative aims to support and empower operators to make timely and informed decisions while also providing the opportunity to enhance operational autonomy.

Built on Honeywell's flagship distributed control system, Experion Operations Assistant is an advanced AI-powered solution designed to transform the way operators monitor plant operations from the control room. By merging operational analytics with real-time predictive insights, the solution facilitates a more efficient workflow within critical refinery operations. With the integration of this new solution, operators in the control room can forecast potential maintenance events before they happen and minimize risks associated with unsafe operations and production losses.

Rapoo Appoints Gaurav Rawool as Marketing Head - India, MEA & SAARC

Wireless peripherals brand Rapoo has appointed Gaurav Rawool as Marketing Head - India, MEA & SAARC.

With over 14 years of experience across leading global technology brands such as ASUS, TP-Link, Tenda, and ALOGIC, Mr. Rawool brings extensive expertise in channel marketing, digital transformation, brand repositioning, product launches, and gaming community engagement.

In his new role, Gaurav will lead Rapoo's marketing and brand growth initiatives across India, the Middle East, Africa, and SAARC regions. His appointment comes at a strategic time when Rapoo is expanding its footprint across emerging markets and aiming to establish itself as a household name in the peripherals category.

"I joined Rapoo seeing the immense potential in the brand and the growth we can achieve together. Rapoo's product design and quality have always stood out in the market, and I look forward to positioning it as the go-to peripheral brand that delivers seamless, reliable experiences for users. Having admired Rapoo's retail presence in my previous roles, I'm excited to take it to the next level.

Satcom Infotech Appoints Mrinal Srivastava as Chief Technology Officer

Satcom Infotech Pvt. Ltd., a leading value-added distributor in the cybersecurity domain, has announced the appointment of Mrinal Srivastava as its Chief Technology Officer (CTO). In this role, Mrinal will lead Satcom's technology strategy and solution innovation, driving the company's vision to deliver best-in-class security solutions for enterprises in India and across global markets.

With this strategic appointment, Satcom aims to extend its deep expertise in product distribution into solution-oriented cybersecurity offerings, helping organizations strengthen their digital resilience in the era of AI, Zero Trust, and intelligent automation.

Mrinal brings over 18 years of experience across cybersecurity, identity, and AI-driven innovation. A technologist at heart, he began his career building and engineering security products before evolving into a technology and business leader - leading global engagements, forming Centers of Excellence (CoEs), and building high-performing teams from the ground up.

He has worked extensively with global enterprises and ISVs, leading initiatives.

Trend Micro Rolls out Comprehensive Offering for Enterprise AI Risk Management

Trend Micro Incorporated is set to launch Trend Vision One AI Security Package—the first solution package delivering proactive, centralized exposure management with unparalleled analytics for AI-driven environments—at AWS re:Invent in December. This new package protects the full AI application stack from model development to runtime, extending proactive security across every stage of AI deployment, and will launch alongside a suite of other leading AI security capabilities to be introduced at the event.

Sharda Tickoo, Country Manager for India & SAARC at Trend Micro, said, “Innovation without oversight is a risk businesses cannot afford. Our goal is to provide the foundation for AI safety and guardrails to align AI transformation with security and trust. By building with these principles from the start, organizations can move forward with confidence as AI becomes central to their growth.”

Organizations are building AI systems at speed, but most lack visibility into how those systems process data, make decisions, or could be exploited by threat actors. Traditional security tools serving endpoints, network, and cloud were not built to understand model behaviors or AI-specific risks like prompt injection, data poisoning, or output manipulation.

eScan Wins Top Channel Favourite Cybersecurity Solution at Channel Accelerator Awards 2025

eScan has been honoured with the Top Channel Favourite Cybersecurity Solution at the prestigious SME Channels Accelerator Awards 2025, attended by more than 500 channel chiefs and enterprise CIOs. The award highlights the industry's growing trust in eScan's innovative and dependable security offerings.

The honour comes at a critical moment for India's cybersecurity landscape. In 2025, the country witnessed several high-profile breaches that underscored the inadequacy of traditional security approaches. When major IT services firms faced scrutiny over incidents like the Marks & Spencer breach and the Jaguar Land Rover attack, enterprises began prioritising not just technology features but their security partners, trust, and proven performance.

“It is a proud moment for our entire team,” said Govind Ram-murthy, CEO of eScan. “This award motivates us to do better and strengthen India's security ecosystem. But what makes it particularly meaningful is that it comes from the channel partners and CIOs.”

Milestone Systems teams up with DCAI to advance responsible AI model development

The work will focus on the deployment and fine-tuning of the world's most advanced AI Vision Language Model (VLM) for traffic and smart city applications, developed by Milestone in collaboration with NVIDIA.

Today, millions of video cameras capture valuable footage that could improve everyday life. Yet much of this potential remains untapped due to the time-consuming task of reviewing and analyzing countless hours of video to uncover meaningful insights. Milestone has developed a cutting-edge VLM using NVIDIA CosmosReason, designed to deliver advanced video intelligence by automatically converting video footage into detailed written reports, summaries, and real-time alerts. Milestone's VLMs can be used to build video analytics AI agents and applications across a variety of use cases such as traffic management across cities, ports, airports, and other urban areas.

The VLM will now also run on DCAI's EU-based Gefion cloud, ensuring full compliance with European data sovereignty and regulatory frameworks, including the AI Act and GDPR.

Fortinet Launches Secure AI Data Center Solution

Fortinet, a leading cybersecurity company driving the convergence of networking and security, has announced the Secure AI Data Center solution, the industry's first end-to-end framework purpose-built to protect AI infrastructures. Designed to secure the full AI stack—from data center infrastructure to applications and large language models (LLMs)—the solution delivers advanced AI threat defense with ultra-low latency and reduces power consumption on average by 69% compared to traditional approaches.

As part of this announcement, Fortinet introduced the FortiGate 3800G, a high-performance data center firewall that delivers the power efficiency, throughput, and scalability required for AI workloads. Powered by NP7 and SP5 ASICs and 400 GbE connectivity, the 3800G is the latest addition to the Fortinet data center firewall portfolio to deliver the hyperscale throughput, energy efficiency, and real-time GPU-cluster protection as part of the Secure AI Data Center framework.

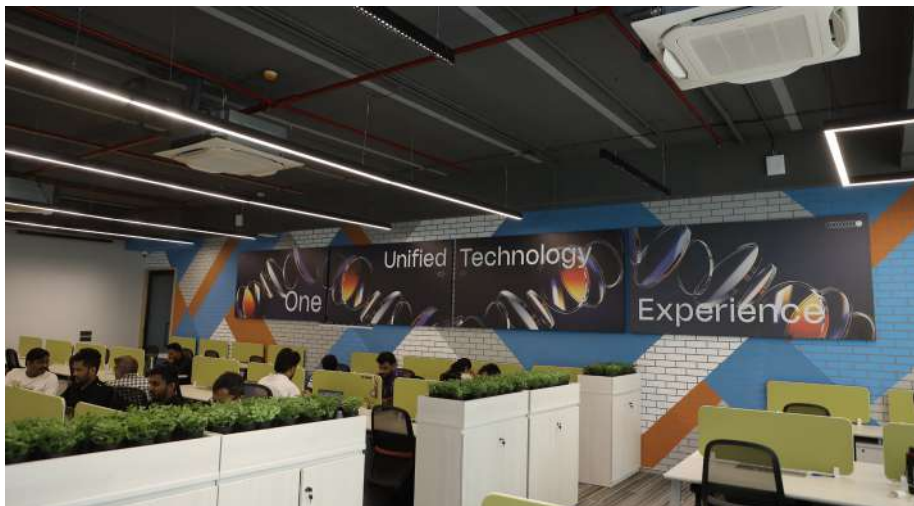
“AI data centers demand both massive performance and deep protection,” said Nirav Shah, Senior Vice President of Products and Solutions at Fortinet.

5Tattva Recognized Among 'Top 100 Channel Accelerators - Cybersecurity' at the 'Channel Accelerator Awards' 2025

5Tattva, a leading CERT-In empanelled cybersecurity solutions provider, has been honored with the prestigious ‘Top 100 Channel Accelerators – Cybersecurity’ title at the Channel Accelerator Awards 2025. Further strengthening this milestone, Zeroday Ops—recently acquired by 5Tattva—also secured a place among the Top 100 Channel Accelerators, highlighting the unified strength and strategic alignment of the two organizations.

The Channel Accelerator Awards recognize companies that enable partner growth, accelerate technology adoption, and contribute significantly to India's digital landscape. Against this backdrop, the dual win for 5Tattva and Zeroday Ops reflects their shared vision of advancing a secure, innovation-led, and future-ready technology ecosystem.

Bringing together more than 150 vendors, SIs, VARs, distributors, key Government stakeholders, and major industry associations, this year's event served as a powerful convergence of leaders shaping India's IT channel ecosystem. Held under the theme “Empowering the Future of the IT Channel: Innovation, Collaboration, Excellence,”



ORIENTING WITH A NEW TURBE SERVICE DELIVERY CENTRE WITH NEXT-GEN NOC & SOC

The new Turbe centre is designed to provide 24/7 monitoring, proactive threat detection, digital forensics, and infrastructure performance management, powered by cutting-edge automation and a high-availability architecture

Orient Technologies Limited, a leading IT Infrastructure and Digital Transformation service provider, announced the opening of its new state-of-the-art Service Delivery Centre (SDC) in Turbe, Navi Mumbai, featuring an advanced Network Operations Centre (NOC) and Security Operations Centre (SOC).

The new Turbe centre is designed to provide 24/7 monitoring, proactive threat detection, digital forensics, and infrastructure performance management, powered by cutting-edge automation and a high-availability architecture. It enhances Orient Technologies' ability to deliver uninterrupted, future-ready IT services to enterprises across BFSI, Pharma, Manufacturing, ITES, Government, and large enterprise sectors.

Strengthening SOC Capabilities Through Strategic Partnership with Securonix

The launch also builds on Orient Technologies' recent strategic alliance with Securonix, a five-time Leader in the Gartner Magic Quadrant for SIEM and Customers' Choice in the 2024 Gartner Peer Insights Voice of the Customer. The partnership brings Unified Defense SIEM powered by Agentic AI to Orient's SOC operations, significantly elevating threat detection, investigation,

and response capabilities.

The collaboration integrates Securonix's agentic AI, advanced analytics, and ML-driven security intelligence with Orient's strong MSSP expertise and India-wide presence. This combination enables organisations to stay ahead of the growing wave of AI-powered attacks, complex malware threats, regulatory requirements, and an increasing cybersecurity talent gap.

A Major Milestone in Orient's Growth Journey

Ajay Sawant, Chairman & Managing Director, Orient Technologies, said: "The new Turbe Service Delivery Centre symbolizes our commitment to delivering secure, scalable, and intelligent managed services. With expanded NOC-SOC capabilities and our strategic partnership with Securonix, we are providing customers with a next-generation operations environment designed for resilience and rapid response."

Engineering Resilience Through Next-Gen Operations

The new Turbe Service Delivery Centre offers:

- Next-gen NOC for real-time IT infrastructure monitoring and performance management
- 24/7 SOC with advanced threat detection, digital forensics, and incident response



AJAY SAWANT
CHAIRMAN & MANAGING DIRECTOR,
ORIENT TECHNOLOGIES

"WITH EXPANDED NOC-SOC CAPABILITIES AND OUR STRATEGIC PARTNERSHIP WITH SECURONIX, WE ARE PROVIDING CUSTOMERS WITH A NEXT-GENERATION OPERATIONS ENVIRONMENT DESIGNED FOR RESILIENCE AND RAPID RESPONSE."

capabilities

- High-availability, redundant architecture ensuring uninterrupted service delivery
- Integrated ITSM, ITAM, and automation-backed operations
- Specialized teams for multi-vendor management, cloud operations, cybersecurity, ITes, and end-user support
- A secure, scalable environment built to meet global compliance frameworks

Strengthening Customer Confidence, Enhancing Business Continuity

With this expansion, Orient Technologies enhances its ability to serve its rapidly growing customer base while ensuring business continuity, minimal downtime, and proactive protection against emerging cyber threats.

Shrihari Bhat, Chief Executive Officer, Orient Technologies, added: "Securonix's Unified Defense SIEM powered by Agentic AI empowers our SOC teams to detect and contain threats with unmatched precision. Together, we are delivering an advanced cybersecurity ecosystem built for the

To access more info login to:

<https://www.smechannels.com>



GUY DIEDRICH

SENIOR VICE PRESIDENT AND GLOBAL INNOVATION OFFICER, CISCO

“WHEN TECHNOLOGY, PEOPLE, AND PURPOSE COME TOGETHER, WE CREATE THE CONDITIONS FOR RESILIENT, HEALTHY, AND THRIVING COMMUNITIES EVERYWHERE.”

STARK GEOGRAPHICAL AND GENERATIONAL DIVIDES IN AI UPTAKE AND DIGITAL WELLBEING

The Cisco study provides a call to action for citizens, business and government leaders worldwide to bridge the digital skills gap, foster digital literacy at every age, and prioritize well-being alongside innovation

Generative AI is moving rapidly from novelty to habit. But adoption rates may not tell the full story. Cisco, the worldwide leader in networking and security, partnered with the Organisation for Economic Cooperation and Development (OECD) on the Digital Well-being Hub to study the relationship between technology's risks and benefits, and how AI is impacting people's lives. New data from the Hub reveals that, beneath the headlines of youthful enthusiasm for AI, geographic and generational divides are emerging, shaping who benefits from AI, who bears the risks, and how digital life can affect well-being. This research provides Cisco's Digital Impact Office with essential insights that can support its aim to connect millions of people to the digital economy, help close the digital divide, and build a global learning culture through initiatives like Cisco Networking Academy and Country Digital Acceleration programs.

AI adoption is only part of the story

According to the current research, young adults, globally, are voracious consumers of digital content, with under-35s showing the highest use of social media, online devices and active use of GenAI. But the real standouts are people in emerging economies, particularly India, Brazil, Mexico, and South Africa. They lead AI adoption globally with the highest usage rates, greatest trust levels, and most active engagement in AI training. In contrast, those surveyed in European countries show less trust and more uncertainty around the use of AI. This marks a departure from historical trends where emerging economies are typically slower to access and use new technologies.

However, these same populations, in India, Brazil, Mexico, and South Africa, report the highest recreational screen time, greatest reliance on digital-only socializing, and the most pronounced emotional highs and lows from tech use, when compared to those surveyed in other countries. The research also shows that, globally, more than five hours of daily recreational screen time is associated with decreased well-being and lower life satisfaction. So, while correlation is not causation, it's clear we need to focus on digital well-being so advances in technology don't come at the cost of health and happiness.

"Empowering emerging economies with AI skills is not just about technology, it's about unlocking the potential of every individual to shape their future. With the rapid integration of AI into our daily lives and workplaces, we must ensure that these tools are designed responsibly, with transparency, fairness, and privacy at their core. AI's greatest potential can be realized if it enhances wellbeing, by streamlining tasks, improving collaboration, and creating opportunities for growth and learning. When technology, people, and purpose come together, we create the conditions for resilient, healthy, and thriving communities everywhere," said Guy Diedrich, Senior Vice President and Global Innovation Officer, Cisco.

From generative AI to generation AI

Generational splits are equally stark, tracking existing trends in digitalization. Younger adults worldwide report that most or all of their social interaction takes place online and they express higher confidence in AI's usefulness. More than 50% of under-35s surveyed actively use AI, more

than 75% say it is useful, and almost half of 26 to 35-year-olds have completed some training.

In contrast, adults over 45 are less likely to view AI as useful, and more than half do not use it at all. Among over-55s surveyed, many say they "don't know" if they trust AI, suggesting their uncertainty may be driven by a lack of familiarity rather than outright rejection. This familiarity gap also mirrors differences in expectations for AI's impact on jobs, with under-35s and those in emerging economies anticipating the highest impact.

"Generational divides in digital and AI adoption are not inevitable, they are challenges we can all address through targeted action. While younger generations may readily embrace new technology, people of all ages bring their own unique and invaluable experience and insights," said Diedrich. "So far at Cisco, 26,000 of our staff have undergone AI training and we are a founding member of the AI Workforce Consortium, a group of 10 leading companies working to prepare the workforce to leverage the transformational opportunity of AI on ICT jobs across all industries. A key measure of AI's success should not be speed of adoption, but whether people across all ages, skill levels, and geographies can use AI to genuinely improve their lives. That way we can ensure 'Generation AI' truly includes everyone," he continued.

This research provides a call to action for citizens, business and government leaders worldwide to bridge the digital skills gap, foster digital literacy at every age, and prioritize well-being alongside innovation. Only then can we

ensure the digital future we build is truly for everyone. **SME**



CHANNEL ACCELERATOR AWARDS 2025: A CELEBRATION OF EXCELLENCE, INNOVATION, AND INDUSTRY LEADERSHIP

Attracting robust participation from over 200 key partners from areas as diverse as digital transformation, cloud, cyber security, automation, AI, etc, representing top Partners, Vendors. ISVs, SIs and VADs, India's largest channel fiesta came up as a spectacular success

Further building upon the success of its previous editions, the much awaited annual channel fest SME Channels Accelerator Awards 2025 has become a spectacular success. The event has received rave response from the channel fraternity, which has been keenly waiting for the D-day.

Over 200 Key Partners & Vendors in Attendance

Conducted with a lot of fanfare on 21st November at ITC Sheraton Saket, New Delhi, India's largest channel event recorded robust participation from over 200 key partners of the \$50 billion-plus domestic IT industry from areas as diverse as digital transformation, cloud, cyber security, automation, AI, etc, representing various organizations into ISV practices, VARs, consultants, SIs, Local/Regional/National Resellers, Distributors, Industry Associations, and Vendors. Their sheer keenness for participation in such good numbers is a testimony to SME Channels' much appreciated efforts to add considerable acceleration to the Channel to unleash the potential of channel

power.

Welcome Note

With a perfect blend of thought leadership, recognition, and networking, the event successfully celebrated the trailblazers driving India's digital transformation and fostering channel innovation across the region.

The evening opened with elegant networking lunch and a ceremonial lamp lighting, setting a tone of inspiration and camaraderie. Sanjay Mohapatra, Group Editor of Accent Info Media, delivered a powerful welcome address, emphasizing the growing role of channel partners as strategic enablers of enterprise innovation. "Today's channel leaders are not just distributors; they are architects of digital growth, shaping how businesses adopt cloud, cybersecurity, AI, and managed services," he said, highlighting the evolving significance of the IT channel ecosystem.

Key Note Address

The Keynote Address on "Leveraging AI by Channel to scale up Business Model" was delivered

by Bhaskar Basu, Country Head - Enterprise Partnerships, Microsoft India & South Asia. The powerful presentation was much appreciated and well received by the partner community.

Underscoring the importance and potential of branding and marketing in the AI era, Ankesh Kumar, Director & CMO, Ingram Micro made a compelling address on "Why Businesses should Focus on Branding and Marketing."

Ankesh stressed upon how focusing on branding and marketing is no longer optional for businesses—it is a strategic necessity for long-term growth and differentiation. Strong branding builds trust, credibility, and recall in a crowded marketplace, helping customers choose one business over another beyond just price or features. Effective marketing amplifies this brand value by clearly communicating purpose, expertise, and outcomes to the right audience at the right time.

"Together, branding and marketing enable businesses to attract quality leads, command premium value, foster customer loyalty, and remain resilient amid competition and disruption. In an era where attention is scarce and choices are



SANJAY MOHAPATRA (TOP LEFT), GROUP EDITOR OF ACCENT INFO MEDIA, DELIVERING A POWERFUL WELCOME ADDRESS. KEYNOTE ADDRESS BY BHASKAR BASU (TOP CENTRE), COUNTRY HEAD - ENTERPRISE PARTNERSHIPS, MICROSOFT INDIA & SOUTH ASIA. PRESENTATION BY AJAY SHIRKE (TOP RIGHT), HEAD OF CHANNELS - EMERGING PARTNERS, INDIA & SAARC, FORTINET



(FROM LEFT TO RIGHT) MATHEW PHILIP , SENIOR DIRECTOR & HEAD INDIA BUSINESS & GLOBAL SIS, GOTO; RAMESH TIWARI, CO- FOUNDER & HEAD OF SALES, EVEREST IMS; AND ASHISH SHUKLA, NATIONAL HEAD - CHANNEL SALES, PROSTARTM

abundant, businesses that invest consistently in branding and marketing position themselves not just to be seen, but to be remembered and preferred,” Ankesh advised.

Defending Against Tech Disruptions

Another key highlight of the event has been a futuristic Panel Discussion on “Protecting Your Business Model from Next-Gen Tech Disruptions.” Moderated by Manash Ranjan Debata, Editor, SME Channels, the panel provided lot of food for thought and useful and practicable suggestions to help the partner community to tackle tech disruptions. The panel discussion brought together industry leaders, channel partners, and technology experts to examine how emerging forces such as AI, automation, cybersecurity

threats, and platform-led ecosystems are reshaping traditional business models. The conversation focused on practical strategies for businesses to stay resilient—ranging from future-ready digital adoption and partner-led innovation to risk mitigation, talent upskilling, and customer-centric transformation. Panelists emphasized the importance of agility, continuous learning, and proactive technology governance, offering actionable insights on how businesses can not only safeguard their existing models but also unlock new growth opportunities in an increasingly disruptive technology landscape.

The panel featured a distinguished lineup of industry veterans whose diverse expertise added depth and credibility to the discussion. Sushil Dutt, National Business Head at Iris Global,

brought valuable perspectives on large-scale distribution, partner ecosystems, and adapting national business strategies to rapid technology shifts. Gurpreet Singh, Founder & Managing Director of Arrow PC Network, shared insights rooted in entrepreneurial leadership and channel-led growth, highlighting how solution providers can future-proof their offerings. Jitesh Chauhan, Managing Director of Rubik Infotech Pvt Ltd, emphasized innovation-driven business resilience and the evolving role of value-added services. Representing the cybersecurity domain, Dipesh Kaura, Country Director for India & SAARC at Securonix, underlined the critical importance of security-first business models in an era of advanced threats, while Sunny Vaghela, CEO of TechDefence Labs, offered a forward-looking view



on cyber defense, skills development, and proactive risk management—making the panel both insightful and highly relevant for today's SME ecosystem.

AI and Channel Business Transformation

The theme for this edition was "AI and Channel

Business Transformation" under which the partners and the 'who is who of Indian IT' thronged together to brainstorm their growth strategies, challenges before the industry and chalked out blueprints for the future, riding the wave of Digital Acceleration.

The event witnessed highly power-packed sessions, and awards and recognitions to stars of the

industry throughout the day.

Keynote speakers and panelists delivered actionable insights on market shifts, partner enablement, next-gen IT consumption, and sustainable business models. Industry experts echoed a common sentiment: collaboration, digital readiness, and customer trust are the new currencies for channel growth.





POWERFUL PRESENTATIONS BY SYED MANSOOR ALI, CHANNEL ENABLEMENT MANAGER INDIA, AMD; MANOJ DHANDA, FOUNDER & CEO, UTHO CLOUD; RAJESH SHARMA, PRODUCT SPECIALIST - COMMERCIAL MASTER TRAINER, MICROSOFT; ROHIT MAHAJAN RSM - NORTH & EAST, LENOVO COMMERCIAL TABLETS BUSINESS; PRAMOD SHARDA, CEO, ICEWARP INDIA & MIDDLE EAST; BHASKAR NANDI, REGIONAL SALES DIRECTOR, GURUCUL AND RAHUL SHARMA, SR. SALES SOLUTIONS CONSULTANT, GURUCUL; AND ANKESH KUMAR, DIRECTOR & CMO, INGRAM MICRO.



Importance of MSPs Underlined

The event hosted a power-packed special MSP Panel Discussion. Moderated by Jaspreet Singh, Partner-Cyber Advisory, Grant Thornton Bharat, the panel had an enviable line up of speakers. The panel discussion on “Creating a Service-Led Economy” brought together industry leaders to explore how services are becoming the primary driver of sustainable growth in the technology ecosystem. Akshay Thakkar, Chief Executive Officer of Shiviom Cloud LLP, highlighted the shift from product-centric models to outcome-driven cloud and managed services. Akshay Kumar Sharma, Director-Technology at Medley India, emphasized building robust, scalable service architectures that deliver consistent value to customers. Vishal Bindra, CEO of ACPL Systems

Pvt. Ltd, shared insights on leveraging customer experience, long-term relationships, and recurring revenue models to strengthen service-led businesses, while Ritesh Dhawan, Marketing Head at Redington Limited, discussed the role of distribution, enablement, and go-to-market strategies in accelerating service adoption. The discussion offered clear takeaways on how organizations can transition from transactional sales to value-driven, service-oriented ecosystems.

Enviable line-up of Industry Think-Tanks

The full-day event lined up renowned speakers and key industry think-tanks to enlighten the audience on the inner matrixes and future blueprints of the IT ecosystem. The event presented

a long list of eminent speakers which includes Ajay Shirke, Head of Channels - Emerging Partners, India & SAARC, Fortinet; Manoj Dhanda, Founder & CEO, Utho Cloud; Ashish Shukla, National Head Channel Sales, PROSTARM INFO SYSTEMS; Rajesh Sharma, Product Specialist-Commercial Master Trainer, Microsoft; Bhaskar Nandi, Regional Sales Director, Gurukul and Rahul Sharma, Sr. Sales Solutions Consultant, Gurukul; Rohit Mahajan, RSM - North & East, Lenovo Commercial Tablets Business; Syed Mansoor Ali, Channel enablement Manager India, AMD; Mathew Philip, Senior Director & Head India Business & Global SIs, GOTO; and Pramod Sharda, CEO, IceWarp India & Middle East.

Recognizing Over 150 Key Partners &



Vendors

Besides the immense food for thought and opportunities for business networking, the event witnessed over 100 top awards awarded to leading

players of the industry in various categories. Top Partners, Vendors, VADs, ISVs, star marketers, companies with most ethical practices, as well as, movers and shakers of the IT industry were recog-

nized for their stellar efforts and decisive contribution to turbo-charge the IT industry.

The awards ceremony recognized high-impact contributors across categories such as Emerg-



ing Channel Champion, Cloud Transformation Partner, Cybersecurity Innovator, Managed Services Leader, and Partner of the Year. Each award reflected a benchmark in innovation, delivery excellence, and customer trust.

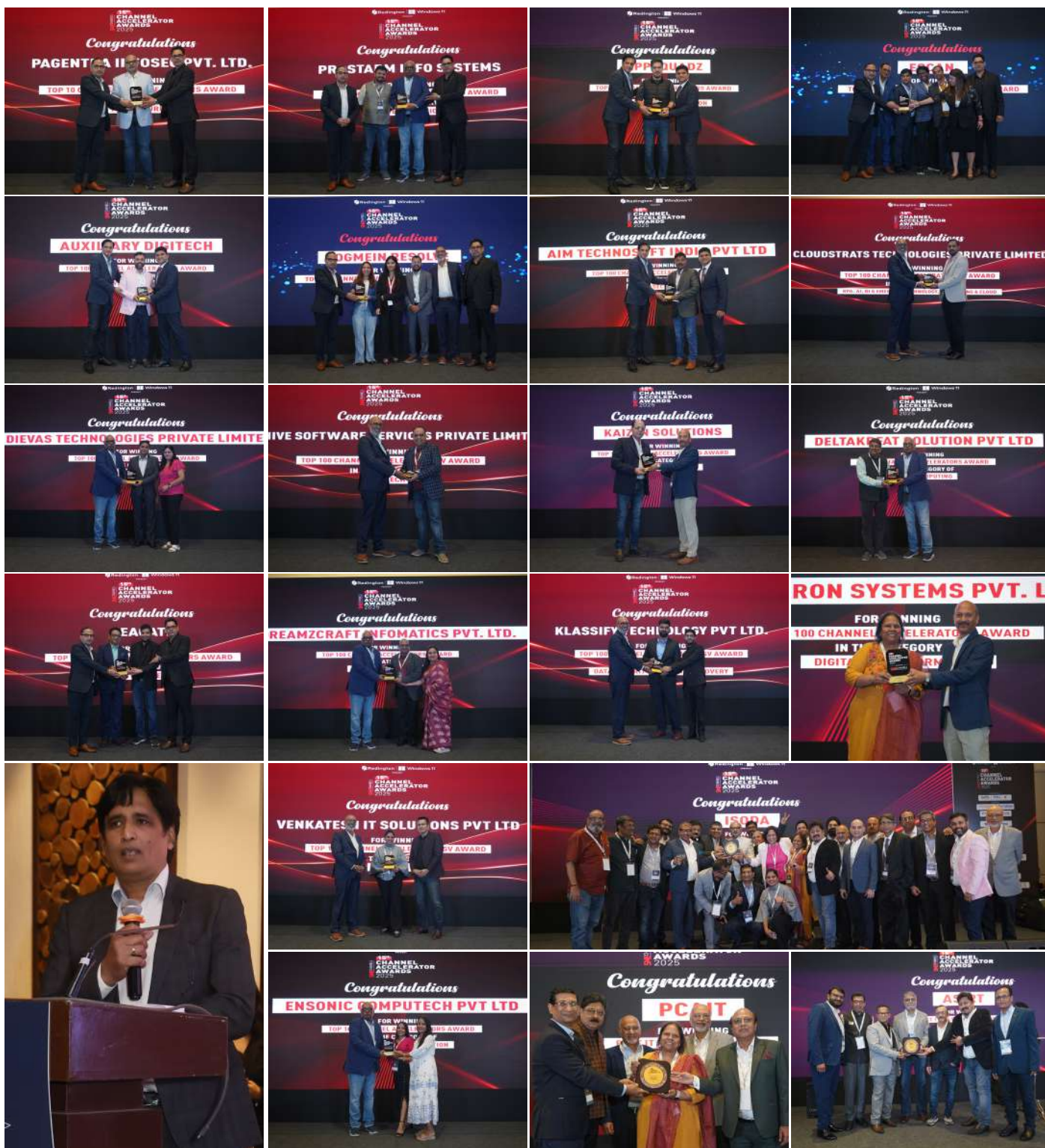
In recognition of his exemplary contribution to the growth of IT Industry, industry veteran Mr Sanjiv Krishen, CMD and Chairman of Iris Global Services, was awarded with the most coveted "IT Man of the Year" award.

Vote of Thanks

At the fag end of the event, appreciating the contribution of the sponsors, the participants and the channel fraternity's much hallowed presence which together contributed to make the event a splendid success, Sanjib Mohapatra, Publisher, Accent Infomedia, delivered the vote of thanks.

Recognizing the strong industry response and appreciating the people behind the big show, Mr Mohapatra said, "Most of the participants have

travelled from far and wide from different nooks and corners of the country and make lot of efforts to make this event a roaring success. Our heartfelt thanks and deep appreciation for that. First of all, I would extend our special thanks to the distinguished members of our most valued Partner community. Their robust participation has always made this event a splendid success. We expect a repeat of the splendid success of this edition next time too. It's really a rare occasion where you will



find over 200 key partners of the 50 billion-dollar-strong domestic IT industry from such diverse specialized areas like digital transformation, cloud, cyber security, automation, AI, etc, representing various organizations into ISV practices, VARs, consultants, SIs, Local/Regional/National Resellers, Distributors, Industry Associations, and Vendors under one roof.”

“My special thanks to our esteemed sponsors and deep admiration and congratulations to all the award winners and thanks to those who have not won the awards this time for their keen interest and participation. We look forward to welcome you again at the next edition of SME Channels Accelerator Awards,” he concluded.

A vibrant Music Show by Kirti Mishra and Pra-

senjit Mukherjee regaled the audience. Apart from series of insightful sessions, high-voltage networking, and very useful media opportunities, at the end, the participants were treated with cocktails and dinner. A truly successful evening—where recognition met opportunity, and innovation met leadership. **SME**



REDINGTON INDIA DEEPENS CHANNEL ENGAGEMENT AT SME CHANNEL AWARDS

Driving SMB growth with AI-ready solutions and partner-led innovation

Redington India reaffirmed its commitment to the channel ecosystem through its active participation in the SME Channel Awards, positioning the event as a strategic platform to engage partners, exchange insights, and demonstrate the real-world impact of modern workplace technologies. The company's presence reflected a shared vision with Microsoft to enable partners to deliver secure, intelligent, and scalable solutions to SMB customers.

A key highlight of the engagement was a focused reseller workshop that addressed critical industry transitions, including the end of support for Windows 10 and the growing urgency for migration to Windows 11. The session provided partners with practical guidance on upgrade pathways, customer readiness, and the commercial opportunities emerging from large-scale refresh cycles. Special emphasis was placed on Copilot+

PCs and their ability to unlock new value propositions for SMBs through AI-enabled productivity.

Redington also emphasised how AI-powered PCs are redefining everyday business operations for small and mid-sized organisations. By embedding AI capabilities directly into devices, Copilot+ PCs allow SMBs to automate routine tasks, improve collaboration, and derive actionable insights without increasing IT complexity. This approach enables businesses to adopt AI seamlessly while enhancing performance and efficiency.

In partnership with Microsoft, Redington continues to invest heavily in partner enablement initiatives designed to support this transformation. These include structured technical training programmes, certifications, marketing and demand-generation support, and co-selling opportunities that help partners lead customer conversations around AI readiness and modern





"REDINGTON INDIA HIGHLIGHTED ITS COMMITMENT TO CHANNEL PARTNERS AT THE SME CHANNEL AWARDS, SHOWCASING WINDOWS 11 AND COPILOT+ PCS IN COLLABORATION WITH MICROSOFT TO HELP SMBS BOOST PRODUCTIVITY, SECURITY, AND GROWTH IN AN AI-DRIVEN ECONOMY."



workplace adoption.

Looking ahead, Redington anticipates that AI adoption, secure cloud platforms, and hybrid work environments will define the next phase of growth for the SMB and channel ecosystem.

With Microsoft's sustained focus on innovation and partner success, Redington aims to ensure its reseller community remains well-positioned to capitalise on emerging opportunities and deliver long-term value to customers.

Through platforms such as the SME Channel Awards, Redington continues to strengthen its role as a trusted distributor and ecosystem enabler—bridging technology innovation with channel capability to drive sustainable SMB success. **SME**



MELODY LOPEZ

Director and Chief of Staff, Crayon
Software Experts India

PROFILE

As Chief of Staff at Crayon India, Melody Lopez drives the execution of the Company's Strategy and Vision. She also drives engagement with Employees, Internal Stakeholders, Business Heads, Channel Partners and Customers. Melody truly understands the power of listening to and collaborating with Employees, Customers and Partners, and she knows that long-term relationships are built on transparency, communication, and accountability.

THE RISE OF ANTI-FRAGILE WORKFORCES: HOW HR CAN HELP ORGANIZATIONS THRIVE AMID DISRUPTION

Disruption can be harnessed as an opportunity for growth and 'antifragility' captures this shift in mindset, offering a powerful opening to shape a workforce that evolves, innovates and accelerates

The world of work is shifting faster than ever, but this pace of change presents unprecedented possibilities. Today's leaders are no longer tasked with merely responding to disruption; we have the opportunity to harness it as fuel for growth. The concept of anti-fragility captures this shift in mindset. It is the belief that people and organizations can become stronger through volatility. For HR, this moment offers a powerful opening to shape a workforce that evolves, innovates and accelerates every time the environment does.

Why antifragility matters now

The velocity of technological change and the growing frequency of geopolitical, climate and market shocks mean that skill sets and operating models will be tested constantly. Forecasts show rapid role turnover and skills shifts: recent global employer surveys estimate that the set of jobs created will equal roughly 14 percent of today's employment while 92 million roles will be displaced by the same forces over the next five years. This is not remote. It requires workforce strategies that convert disruption into advantage.

Five principles HR leaders must adopt today

Treat learning as continuous strategic investment - Organizations that commit to continuous reskilling and internal mobility create optionality for both the business and the employee. Evidence from broad human capital research shows that organizations investing in human performance and capability building are measurably more likely to unlock productive outcomes. HR must shift budgets and attention from one-off training to durable learning architectures aligned to strategy.

Build talent systems that benefit from variability - Antifragility requires mechanisms that convert small failures into learning loops. That means rapid

experimentation with cross-functional rotations, internal talent marketplaces, shadowing programs and stretch assignments. These practices reduce single points of failure and accelerate tacit knowledge transfer. They also create a distributed network of capability that strengthens under stress. Practical adoption is already visible in enterprises that are redesigning career pathways to privilege adaptability over tenure.

Use technology to amplify human judgment without replacing it - AI and automation will continue to alter work. Forecasts indicate that a material share of jobs will be affected by AI technologies. Leaders must adopt responsible, augmented approaches to technology in HR rather than reflexive replacement. For example, embedding AI in skills management and internal mobility systems can accelerate redeployment of people into emerging roles while preserving human oversight and context. By 2025 a majority of enterprises are expected to formalize responsible AI frameworks for HR applications, enabling trust and adoption at scale.

Harden psychological and operational safety nets - Antifragile workforces are not built on brittle optimism. They require psychological safety, clear escalation paths, robust well-being programs and contingency benefits that reduce the human cost of transition. When employees know the organization will support them through failure or redeployment, they are more likely to take productive risks and contribute novel solutions during stress events. Policies should quantify these supports and measure their impact on retention and redeployment rates.

Measure antifragility with leading indicators - Traditional HR metrics emphasize lagging indicators. To manage antifragility, we must track leading indicators such as time to redeploy, percent of workforce in cross-functional rotations, internal

To access more info login to:

<https://www.smechannels.com>


VIVEK SRIVASTAVA
COUNTRY MANAGER, INDIA & SAARC AT FORTINET

"AT FORTINET, WE ARE HELPING CUSTOMERS EMBRACE THIS SHIFT BY EMBEDDING AI ACROSS THE PLATFORM, ENABLING FASTER DETECTION, SMARTER RESPONSES, AND MORE RESILIENT OPERATIONS AS CYBER RISKS BECOME MORE COMPLEX AND DISTRIBUTED."

AI ADOPTION IN CYBERSECURITY SURGING AHEAD

The IDC study, commissioned by Fortinet, reveals that AI has moved beyond hype to become a critical enabler of speed, accuracy, and scale in security operations, and is now shaping hiring priorities, investment strategies, and the architecture of modern cybersecurity teams

Fortinet, the global cybersecurity leader driving the convergence of networking and security, today announced the findings of a 2025 IDC survey highlighting how organizations across India are adopting AI as the frontline of their cyber defence strategy. The IDC study, commissioned by Fortinet, reveals that AI has moved beyond hype to become a critical enabler of speed, accuracy, and scale in security operations, and is now shaping hiring priorities, investment strategies, and the architecture of modern cybersecurity teams.

AI's Growing Influence on the Cyber Landscape

AI is transforming both sides of the cybersecurity equation. For defenders, it offers the potential to automate detection, accelerate response, and scale threat intelligence with unprecedented speed. But the same capabilities are now being leveraged by attackers, who are using AI to launch stealthier, faster, and more adaptive attacks. According to the IDC Study, nearly 72% of organizations across India say they have encountered AI-powered cyber threats in the past year. Of those, 70% reported a 2X increase and 12% reported a 3X increase in threat volume. These attacks are harder to detect and often exploit blind spots in visibility, governance, and internal processes.

AI Adoption Accelerates from Pilot to Production

AI is no longer a future consideration; it's an operational reality. More than nine in ten organizations across India are already using AI in their security environment. Organizations are rapidly progressing from AI-powered detection to more advanced use cases such as automated response, predictive threat modelling, AI-driven incident response, AI-powered threat intelligence, and behavioural analytics. These top five use cases reflect how detection has become table stakes, while response, prediction, and orchestration are now the next frontier.

GenAI is also gaining traction, with adoption focused on light-touch tasks such as running playbooks, updating rules and policies, social engineering detection, writing detection rules, and guided investigations. However, trust in autonomous action remains limited. Use cases like auto-remediation and guided remediation are not widely deployed, signalling that we are still in the "co-pilot" phase of adoption.

AI Skills Redefining the Security Workforce

The shift toward AI-first cybersecurity is also reshaping how teams are built. Across India, the top five cybersecurity roles in demand include security data scientists, threat intelligence analysts, AI security engineers, AI security researchers, and AI-specific incident response professionals. Organizations are no longer just deploying AI tools; they are building their cybersecurity teams

around AI capabilities. This reflects a broader trend where the workforce is rapidly evolving to match the pace of technological adoption.

Strategic Investments: From Infrastructure to Intelligence

Cybersecurity budgets are trending upward, with nearly 82% of organizations reporting an increase. However, the vast majority of these increases were modest, 64% reported an uplift of less than 5%, and 18% saw increases between 5–10%. This suggests that while budgets are growing, spending remains focused on covering rising operational and talent costs. Organizations appear to be carefully prioritizing how and where these limited increases are deployed. The top five areas of investment over the next 12–18 months include identity security, network security, SASE/Zero Trust, cyber resilience, and cloud-native application protection, indicating a strategic shift from infrastructure-heavy spending toward more targeted, risk-centric priorities that reflect the evolving threat landscape.

Teams Remain Under-Resourced and Overwhelmed

While cybersecurity is gaining executive attention, many teams remain under-resourced and lack dedicated focus. Only 6% of an organization's

To access more info login to:
<https://www.smechannels.com>

AWS RE:INVENT 2025: ADVANCING NEXT-GEN SIEM AND CLOUD SECURITY ACCESS ON AWS

CrowdStrike becomes the first cybersecurity partner to deliver an enhanced version of SaaS Quick Launch in AWS Marketplace for fully integrated Falcon Next-Gen SIEM; CrowdStrike Falcon Next-Gen SIEM and Falcon Cloud Security are available on a pay-as-you-go basis for new AWS customers

At the ongoing AWS re:Invent 2025, CrowdStrike, in collaboration with Amazon Web Services (AWS), announced new integrations and consumption options in AWS Marketplace that make it even easier for customers to secure and operationalize workloads on AWS in an integrated, out-of-the box experience.

Delivering enhanced SaaS Quick Launch in AWS Marketplace

CrowdStrike is the first cybersecurity partner to deliver an enhanced version of SaaS Quick Launch in AWS Marketplace for Falcon Next-Gen SIEM, combining automated configuration with new pay-as-you-go access. This streamlined deployment model gives organizations an even faster, more flexible, and cost-efficient way to adopt CrowdStrike's industry-leading protection for AWS customers globally. Falcon Cloud Security is also available on a pay-as-you-go basis through AWS Marketplace.

Accenture also joins as the inaugural launch partner to help organizations accelerate adoption of Falcon Next-Gen SIEM for AWS and optimize third-party data integrations across complex environments.

Simplified Onboarding with Falcon Next-Gen SIEM for AWS

The enhanced onboarding experience for Falcon Next-Gen SIEM in AWS Marketplace delivers a single location, guided setup that connects directly to core AWS security services – including AWS CloudTrail, AWS Security Hub, and Amazon GuardDuty. This simplified workflow automatically discovers active data sources and begins ingesting telemetry within minutes, eliminating manual configuration and accelerating time-to-value.

By streamlining how customers connect their AWS environments to CrowdStrike, organizations can unify data from endpoints, cloud workloads, and identities with AWS telemetry to deliver comprehensive, cross-domain threat detection and response.

"CrowdStrike and AWS are transforming how

security is delivered in the cloud," said Daniel Bernard, chief business officer at CrowdStrike. "Together, we're removing friction so customers can innovate fearlessly, accelerate outcomes, and stop breaches faster."

Flexible, Pay-As-You-Go Consumption

To meet customers where they are, CrowdStrike is introducing pay-as-you-go pricing for both Falcon Next-Gen SIEM and Falcon Cloud Security in AWS Marketplace. The new model enables customers to start protecting AWS workloads in minutes, pay only for what they use, and scale as their environments grow – all through AWS's unified billing and procurement system. This approach makes advanced protection accessible to organizations of any size while simplifying how security is purchased and managed in the cloud. Pay-as-you-go customers also become strong candidates for CrowdStrike's Falcon Flex subscription model as they expand platform adoption.

Connecting Falcon Next-Gen SIEM to critical AWS services

"AWS Marketplace is the fastest, most efficient way for customers to procure cloud solutions with unified billing, streamlined purchasing, and simplified configuration," said Matt Yanchyshyn, vice president of marketplace at AWS. "With CrowdStrike's enhanced onboarding experience in AWS Marketplace, we're making it seamless for customers to connect Falcon Next-Gen SIEM to critical AWS services like AWS CloudTrail, AWS Security Hub, and Amazon GuardDuty – all through a guided setup experience. Combined with pay-as-you-go pricing, customers can discover, configure, and deploy protection faster than ever, ensuring a seamless experience from purchase to protection."

Expanded Integrations for Faster, Cost-Efficient Operations

CrowdStrike is expanding Falcon Next-Gen SIEM capabilities for AWS with real-time response powered by Amazon EventBridge, eliminating the latency of traditional batch processes. Detections from AWS Security Hub and Amazon GuardDuty now stream into the Falcon platform



DANIEL BERNARD
CHIEF BUSINESS OFFICER
CROWDSTRIKE

"CROWDSTRIKE AND AWS ARE TRANSFORMING HOW SECURITY IS DELIVERED IN THE CLOUD. TOGETHER, WE'RE REMOVING FRICTION SO CUSTOMERS CAN INNOVATE FEARLESSLY, ACCELERATE OUTCOMES, AND STOP BREACHES FASTER."

instantly, enabling immediate investigation and response.

CrowdStrike is also introducing new federated search capabilities via Amazon Athena, providing fast and flexible access to data stored in Amazon Simple Storage Service (Amazon S3). Customers can query data in place – without re-ingestion or duplication – to investigate incidents, perform audits, and build operational insights. Together,

To access more info login to:

<https://www.smechannels.com>

ESCAN ENHANCES ENTERPRISE DLP WITH CHATGPT TENANT CONTROL, ADDRESSING CRITICAL DATA SOVEREIGNTY GAP

The new capability ensures employees use only corporate ChatGPT accounts, preventing confidential data leakage through personal AI tools

EScan, a leading cybersecurity solutions provider, has introduced an advanced tenant control feature for ChatGPT within its Enterprise DLP platform. The new capability directly addresses one of the biggest barriers to enterprise AI adoption: the risk of sensitive data leaking through unmanaged personal AI accounts.

As enterprises increasingly adopt ChatGPT, a critical gap has emerged. Even when organizations procure ChatGPT Enterprise licenses for their workforce, employees can still access ChatGPT using personal accounts via Google, Apple, or Microsoft authentication providers, completely bypassing corporate oversight and creating ungovernable data risks.

The Data Sovereignty Problem

When employees use personal ChatGPT accounts for work-related queries, organizations lose all visibility and control over what information gets shared. Unlike corporate accounts where IT teams can access conversation logs through compliance tools, personal account usage creates blind spots that compliance and security teams cannot monitor or remediate.

This isn't theoretical risk. Consider recent incidents where confidential information found its way into AI systems. Samsung discovered employees had accidentally leaked proprietary semiconductor designs and meeting notes into ChatGPT. A law firm faced scrutiny when attorneys used personal AI accounts to analyze confidential client documents. In each case, the data entered personal AI platforms where organizations had no ability to retrieve, audit, or ensure proper handling.

The challenge becomes more acute as AI adoption accelerates. Organizations recognize that tools like ChatGPT, Claude, and other AI interfaces dramatically improve productivity - Microsoft reports that knowledge workers using AI assistants save an average of 90 minutes per day. Yet adoption remains cautious. IBM's 2024 Global AI Adoption Index found that 65% of enterprises cite data security and privacy as their primary barrier to AI deployment.

How the Solution Works

eScan's Enterprise DLP already offers Workspace Tenant Control across major platforms such as Google Workspace, Microsoft 365, Dropbox, Atlassian, Slack, Webex, and many others. When employees attempt to access these platforms using personal credentials, the system blocks the login attempt. Authentication succeeds only when employees use their corporate domain credentials, maintaining workflow while ensuring data sovereignty.

The ChatGPT tenant control extends this capability to AI platforms. When an employee attempts to authenticate to ChatGPT, the eScan DLP system monitors the OAuth authentication flow. If the user attempts to authenticate via personal Google, Apple, or Microsoft identity providers, the DLP intercepts and blocks the authentication API request. Only authentication through corporate domain credentials - linked to the organization's ChatGPT Team or Enterprise workspace - is permitted.

This approach solves multiple problems simultaneously. Employees can still use ChatGPT productively for legitimate work purposes. Organizations maintain complete visibility through their ChatGPT Enterprise compliance capabilities. Security teams can audit AI usage patterns. And most critically, confidential information stays within corporate-controlled environments where proper data handling policies apply.

Why This Matters Now

The deployment comes as organizations worldwide grapple with AI governance. Gartner predicts that by 2026, enterprises without comprehensive AI data governance will face three times more data breaches related to AI usage than those with proper controls. The challenge isn't preventing AI use - that ship has sailed. The challenge is channelling AI use into controlled environments.

"This capability directly addresses what CIOs tell us keeps them up at night," said Govind Rammurthy, CEO of eScan. "They know their employees are using AI tools regardless of policy. The question is whether that usage happens in corpo-



GOVIND RAMMURTHY
CEO, ESCAN

"THIS CAPABILITY DIRECTLY ADDRESSES WHAT CIOs TELL US KEEPS THEM UP AT NIGHT. THEY KNOW THEIR EMPLOYEES ARE USING AI TOOLS REGARDLESS OF POLICY."

rate accounts where security teams have visibility, or in personal accounts that create ungovernable risk."

The feature is now part of eScan's Enterprise DLP solution, with support for additional AI platforms planned based on customer requirements. As AI tools proliferate and become embedded in daily workflows, the ability to ensure corporate data sovereignty across these platforms becomes not just a security feature but a fundamental requirement for responsible AI adoption. **SME**



PRANAY AHLAWAT

CHIEF TECHNOLOGY AND AI OFFICER AT COMMVAULT

“WITH COMMVAULT DATA ROOMS, ENTERPRISES CAN CONFIDENTLY EXPORT THEIR SECONDARY DATA AND HARNESS IT WITH THE AI PLATFORM OF THEIR CHOICE TO UNLOCK NEW OPPORTUNITIES FOR INTELLIGENCE, INNOVATION, AND BUSINESS GROWTH.”

COMMVAULT'S DATA ROOMS: SAFELY CONNECTING ENTERPRISE DATA WITH AI PLATFORMS

New offering gives organizations a secure way to activate and share trusted backup data across internal and external AI platforms

Commvault, a leading provider of cyber resilience and data protection solutions for the hybrid cloud, introduced Data Rooms, a secure environment that enables enterprises to safely connect their trusted backup data to the AI platforms they rely on, or to their own AI initiatives, such as internal data lakes. By combining governed, self-service access with built-in classification and compliance controls, Data Rooms bridges the gap between data protection and data activation, helping organizations transform backup data into AI-ready assets without adding new risk or complexity.

Trust @ the core of responsible AI

As enterprises accelerate AI adoption, many still struggle to make their data both accessible and trustworthy. In fact, nearly three quarters of IT leaders say using AI makes their organizations more vulnerable to cyberattacks. Trust is at the core of responsible AI — trust that sensitive data remains confidential, governed, and compliant as it's ready for use. Yet, the process of identifying, preparing, and exporting data from multiple sources into a single source through the traditional extract, transform, and load (“ETL”) workflow, remains time-consuming and can introduce compliance risks when not properly governed.

Most enterprises don't need yet another AI platform to manage — Commvault's Data Rooms offering is designed to address these challenges.

Turning Data Protection into Data

Activation

With the new Data Rooms offering, authorized users can locate and prepare data directly from backup repositories across on-premises and cloud environments. Built-in governance helps maintain control so that approved, access policy-compliant datasets can be safely shared and exported, with classification, sensitivity tagging, and audit trails automatically applied. Additionally, Data Rooms operate within Commvault Cloud's zero-trust architecture, leveraging role-based access controls (RBAC) and encryption at rest and in transit. These safety measures can give organizations confidence that their data remains protected, governed, and traceable from backup to activation.

“AI initiatives often stall because organizations can't safely access or prepare the data they already have,” said Jonathan Brown, Lead Analyst at Omdia. “Commvault's Data Rooms connect resilience and analytics in a controlled, auditable way, helping enterprises operationalize AI faster without increasing risk.”

By integrating directly with Commvault Cloud, Data Rooms gives authorized users governed access to files, emails, and objects across environments. It automates data discovery, and classification, simplifying the creation of curated, AI-ready datasets. As enterprises move from data protection to data utilization, Commvault preserves data trust, and supports compliance and readiness throughout the activation process.

Key Benefits for Enterprises:

- **Accelerate Insights:** Bridge the gap between backup and analytics. Discover and export historical data in open-standard, AI-ready formats such as Apache Iceberg or Parquet to fuel model training and business intelligence.
- **Support Compliance:** Advance governance across the data lifecycle with AI-enabled classification, policy-based redaction, and audit-ready controls that help protect sensitive data even as it's activated for AI and analytics.
- **Simplify Operations:** Reduce manual ETL processes with automated data discovery, curation, and delivery to analytics platforms like Snowflake and Microsoft Azure.

“Organizations are beginning to realize that their historical data is more than just insurance, it's a powerful, untapped strategic asset,” said Pranay Ahlawat, Chief Technology and AI Officer at Commvault. “With Commvault Data Rooms, enterprises can confidently export their secondary data and harness it with the AI platform of their choice to unlock new opportunities for intelligence, innovation, and business growth.”

The Commvault Data Rooms offering is currently available in early access and is targeted for general availability in early 2026, with pricing details to be shared at that time.

Commvault's Data Rooms offering and the introduction of conversational resilience capabilities underscore the company's leadership in bringing together cyber resilience and responsible AI. **SME**

RISKPROFILER MAKES IT TO ONSTAGE'S TOP 100 STARTUPS LIST

The global recognition highlights RiskProfiler's ongoing innovation and growing impact in external threat intelligence

RiskProfiler, a leading provider of external threat intelligence and cybersecurity solutions, has been recognized among Onstage's Top 100 Startups. The recognition comes from a pool of over 1,500 startups evaluated by more than 350 venture capitalists, underscoring RiskProfiler's consistent commitment to innovation and intelligence-driven defense on a global scale.

Addressing potential risks before they escalate

As a rising name in the cybersecurity landscape, RiskProfiler works closely with organizations around the world — including India, one of its key focus markets — to enhance visibility into digital risks and strengthen resilience against evolving threats. Its AI-powered intelligence solutions provide real-time monitoring, risk assessment, and automated response across the open, deep, and dark web — helping businesses anticipate and address potential risks before they escalate.

"This recognition reflects the strength of our vision, the innovation of our technology, and the trust of our global clients," said Setu Parimi, Co-founder & CTO, RiskProfiler. "As we continue to scale, our mission remains clear — to empower enterprises worldwide to anticipate, quantify, and mitigate cyber risk before it becomes business disruption."

Accelerating India-focused growth strategy

While RiskProfiler's European recognition marks a key milestone in its global journey, the company is simultaneously accelerating its India-focused growth strategy — making its advanced external risk management capabilities available to Indian enterprises seeking proactive cyber resilience.

"External risk isn't a list of assets; it's the set of paths an adversary can actually traverse," added Setu Parimi. "RiskProfiler models those paths with Agentic AI and a living knowledge graph to reveal which attack vector is most likely to compromise you tomorrow — and what to fix today. By unifying EASM, DRP, CTI, and TPRM, we cut the path at the optimal point and route the right work to the right team first. The result: fewer alerts, faster risk reduction, and measurable impact."

Setting new benchmarks in proactive security

Through its integrated External Threat Exposure Management platform and deep dark web and brand intelligence, RiskProfiler is setting new benchmarks in proactive security — combining Agentic AI, automation, and continuous intelligence to give organizations the foresight they need in an increasing volatile threat landscape.

This inclusion among Europe's Top 100 Startups reflects not just RiskProfiler's innovation, but also



SETU PARIMI
CO-FOUNDER & CTO
RISKPROFILER

"THIS RECOGNITION REFLECTS THE STRENGTH OF OUR VISION, THE INNOVATION OF OUR TECHNOLOGY, AND THE TRUST OF OUR GLOBAL CLIENTS."

its emerging global relevance — bridging continents and cybersecurity ecosystems with a unified vision of predictable, preventable, and measurable cyber resilience. SME



Look Ahead

Introducing **HID Amico**[™] Facial Recognition Readers

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

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



COREEL ACQUIRES AEROSPACE & DEFENCE DIVISION OF LEKHA WIRELESS TO EXPAND ITS MILITARY COMMUNICATION PORTFOLIO

The acquisition reflects a wider industry shift with Indian defence technology companies investing in indigenous IP and communication systems to meet the growing expectations of the armed forces under the country's self-reliance initiatives

CoreEL Technologies India Private Limited (CoreEL), a leading provider of advanced electronic system-level products and solutions for the Aerospace and Defence as well as the commercial sectors, has announced the acquisition of Aerospace and Defence System (ADS) division of Lekha Wireless, a Bangalore based wireless communications company. The acquisition brings proven wireless communication technologies, indigenous IP, and a specialised engineering team, strengthening CoreEL's position in Military Communication domain.

Strengthening CoreEL's role in India's communication ecosystem

The acquisition comes at a time when India's market demand for secure communication solutions specifically in the Aerospace and Defence sector is undergoing significant transition. Customers are increasingly seeking indigenous and product-ready communication systems. The addition of Lekha ADS's capabilities enhances CoreEL's ability to serve these requirements with an advanced set of scalable portfolio of products. But above all, it accelerates research & development to develop the next-generation, world-class communication products and solutions.

A more comprehensive Communications portfolio

With this acquisition, CoreEL gains expanded engineering bandwidth and ready-to-deploy IPs that broaden its offering across Tactical SDRs, Vehicle SDRs, Mesh Radios, Secure Commercial Communications equipment, MIL-standard radios, Data Links, Missile Communication & Telemetry and UAV communication systems. These capabilities complement CoreEL's ongoing work in communication, airborne systems, secure data links and SATCOM-enabling the company to address a wider set of operational needs. The combined technology portfolio strengthens CoreEL's ability to meet rising global demand for reliable and innovatively engineered communication systems.

Financial details of the transaction remain undisclosed.

Delivering advanced communication solutions

Vishwanath Padur, Managing Director & CEO, CoreEL Technologies, said, "Secure Communication in India is evolving rapidly, creating opportunities for companies with strong indigenous capabilities. The ADS division of Lekha brings deep wireless expertise, a strong set of communication IPs and a culture that aligns well with CoreEL. By combining our system design and integration strengths with Lekha's wireless technologies, we are better positioned to deliver advanced, locally engineered communication



VISHWANATH PADUR
MD & CEO, COREEL TECHNOLOGIES

"BY COMBINING OUR SYSTEM DESIGN AND INTEGRATION STRENGTHS WITH LEKHA'S WIRELESS TECHNOLOGIES, WE ARE BETTER POSITIONED TO DELIVER ADVANCED, LOCALLY ENGINEERED COMMUNICATION SOLUTIONS TO OUR VALUED CUSTOMERS."

solutions to our valued customers."

Amarnadha Reddy and Ramu Srinivasaiah, Founder Directors of Lekha Wireless, added, "By integrating Lekha's ADS division with CoreEL, we are bringing a strong culture of innovation, product development, and technological excellence. CoreEL's high engineering competence aligns perfectly with Lekha ADS's wireless communication expertise, creating a powerful synergy. This integration strengthens the ability to deliver reliable, next-generation communication solutions to defence customers."

To access more info login to:

<https://www.smechannels.com>



Amarnadha Reddy, Founder Director, Lekha Wireless, Vishwanath Padur, Managing Director & CEO, CoreEL Technologies, Ramu Srinivasaiah, Founder Director, Lekha Wireless at the announcement of the acquisition



**SUNDAR
BALASUBRAMANIAN**
Managing Director for India and
SAARC at Check Point Software
Technologies

PROFILE

A seasoned and much accomplished business leader with diverse sales, business and partner leadership experience in the IT industry, Sundar has sizeable experience in working with industry leaders like EMC, VMware, Microsoft and IBM. With a strong grip over various business processes, he has always led from the front and has driven direct sales, new business creation, partnerships, channel management and service delivery. Sunder has also been credited with building high performance businesses and teams, and executing swift turnaround for troubled businesses.

AI IN 5 YEARS: PREPARING FOR INTELLIGENT, AUTOMATED CYBER ATTACKS

AI is not only transforming productivity but fundamentally rewriting the cyber risk landscape that enterprises and individuals must urgently address

Organisations around the world are rapidly adopting AI to drive efficiency and transform operations, marking a shift into an era where cybersecurity is entering a turning point where AI fights AI. The phishing scams and deepfakes of today are only precursors to a coming era of autonomous, self-optimising AI threat actors capable of planning, executing, and refining attacks with little to no human involvement.

India, in particular, faces a significant cybersecurity challenge amid rapid AI adoption. Organisations worldwide are embracing AI for efficiency, but this evolution is shifting cybersecurity into a new era where AI battles AI. In India, phishing scams and AI-fueled deepfakes foreshadow a future dominated by autonomous, self-optimizing AI threat actors capable of planning, executing, and refining attacks with minimal human oversight.

In September 2025, Check Point Research's global threat intelligence found that 1 in every 54 GenAI prompts from enterprise networks posed a high risk of sensitive-data exposure, affecting 91 percent of organisations that use AI tools regularly.

These developments highlight that AI is not only transforming productivity but fundamentally rewriting the cyber risk landscape that enterprises and individuals must urgently address. These statistics show that AI isn't just reshaping productivity, it's rewriting the rules of cyber risk.

The Expanding Attack Surface of AI: Four Critical Threat Vectors Organisations Must Consider

As artificial intelligence (AI) and generative AI become deeply integrated into modern business operations, they are also transforming the cyber threat landscape. Attackers are no longer relying solely on traditional tools — they are embedding AI into their tactics, techniques, and procedures to launch more scalable, adaptive, and sophisticated campaigns. The following four vectors are already emerging from today's AI ecosystem and represent some of the most pressing security considerations for organisations in 2025 and beyond.

1. Autonomous AI Attacks: Machine-Driven Threat Campaigns

Cybercriminals are increasingly experimenting with autonomous AI-driven attacks, where machine agents independently plan, coordinate, and execute multi-stage campaigns. These AI systems share intelligence, adapt in real time to defensive measures, and collaborate across thousands of endpoints — functioning like self-learning botnets without human oversight.

Recent examples, such as prototypes like ReaperAI, show how autonomous AI can chain reconnaissance, exploitation, and data exfiltration into a seamless operation. This machine-speed evolution presents a major challenge for security operations centres (SOCs), which risk being overwhelmed by swarms of adaptive, self-organising attacks that generate thousands of alerts, test policies and shift tactics in real time.

2. Adaptive Malware Fabrication: Self-Evolving Malicious Code

In 2024, multiple underground forums began advertising "AI malware generators" capable of writing, testing, and debugging malicious code automatically. These tools use feedback loops to learn which variants bypass detection — turning each failed attempt into fuel for the next success.

The use of AI-generated polymorphic malware is redefining how attackers build and deploy malicious software. Where traditional malware relied on minor code changes to bypass detection, modern generative models — from GPT-4o to open-source LLMs — can now produce unique, functional malware variants in seconds.

3. Synthetic Insider Threats: AI-Powered Impersonation and Social Engineering

The insider threat is rapidly evolving with the rise of synthetic identities and AI-generated personas. Built from stolen employee data, voice samples, and internal messages, these AI agents can convincingly mimic real users — sending authentic-looking

emails, joining video calls with deepfaked voices, and infiltrating collaboration platforms with precise linguistic and behavioural patterns.

Recent “vibe hacking” cases showed how threat actors embedded social-engineering goals directly into AI configurations, allowing bots to negotiate, deceive, and persist autonomously. As AI voice cloning becomes indistinguishable from the real thing, verifying identity will shift from who is speaking to how behaviourally consistent their actions are, a fundamental change in digital trust models.

4. AI Supply Chain and Model Poisoning: Compromising the Core

The rapid adoption of third-party and open-source AI models has created a vast new attack surface: the AI supply chain. In 2025, several research labs demonstrated data-poisoning attacks where altering just 0.1% of a model's training data could cause targeted misclassification — for example, instructing an AI vision system to misidentify a stop sign as a speed-limit sign. In cyber security contexts, this could mean an intrusion-detection model misclassifying a malicious payload as benign.

Why These AI Threats Are Different

AI-driven cyberattacks stand apart because they combine speed, autonomy, and intelligence at a scale human attackers can't match.

Unlike traditional threats, machine-made attacks learn and adapt continuously. Every failed exploit becomes training data, creating a self-improving threat ecosystem that evolves faster than conventional defences. Check Point Research notes that AI-driven tools like Hex-strike-AI framework, originally built for red-team testing, was weaponised within hours to exploit Citrix NetScaler zero-days.

These attacks also operate with unprecedented precision. Generative AI enables personalised phishing, multilingual deepfakes, and synthetic insider personas that mimic tone and behaviour so well they bypass human suspicion and automated filters alike. At the same time, AI execution removes the “human fingerprint” like typing errors, time-zone patterns, or linguistic traces. This makes attribution and detection increasingly difficult.

Finally, AI is democratising cybercrime. Tools that automate scanning, exploitation, and negotiation are lowering barriers for less-skilled attackers, expanding the threat landscape. By 2030, ransomware and data theft will be orchestrated almost entirely by autonomous AI systems capable of running 24/7 operations without human oversight.

What Organisations Must Do Now to Prepare

The risks associated with AI-driven threats are real — but they don't mean businesses should abandon vibe coding, AI-assisted development, or generative AI tools. Much like the early days of cloud migration or the shift to hybrid work, the challenge now is learning how to embrace AI securely without creating new vulnerabilities.

To reduce risk and build long-term resilience, organisations should focus on these four core strategies:

1. Choose Security-Aware AI Tools and Guide Them Wisely

Select AI platforms that are built or configured with security-first principles. Shape how large language models (LLMs) operate by including prompts that reference validation, encryption, and safe defaults — so secure practices are integrated from the start. Always limit the data you expose to AI tools, keeping sensitive files, credentials, or production datasets out of reach. If testing is needed, use sanitised or synthetic data and review permissions to ensure AI only accesses what it needs.

2. Implement Zero Trust for AI

Apply least-privilege access to AI systems. Authenticate every API call, enforce continuous verification, and monitor AI-to-AI interactions to prevent lateral movement. All code generated by AI should be peer-reviewed, tested, and scanned for vulnerabilities before deployment. Human oversight ensures logic, security, and compliance requirements are properly met — and helps catch red flags that AI may overlook.

3. Secure the Supply Chain and Dependencies

AI can accelerate development, but it also introduces new risks through third-party libraries, plugins, and code suggestions. Every new dependency should be treated as untrusted until verified. Validate sources, check reputation, and run security scans before integration. Robust supply chain security is essential, especially as AI-assisted coding tools can make dependency sprawl harder to track.

4. Automate and Embed Security Throughout the Development Lifecycle

Make DevSecOps a standard part of your AI strategy. Automate security checks across your CI/CD pipeline to detect insecure code, exposed secrets, and misconfigurations before they reach production. Pair these automated guardrails with continuous training for developers, analysts, and

business teams so they understand fundamentals like input validation, access control, and secure data handling.

5. Govern GenAI Usage Company-Wide

Unchecked AI tool use is a growing source of data leakage. CPR's September 2025 cyberattack statistics research found 15 percent of enterprise AI prompts contained potentially sensitive information such as customer records and proprietary code.

Conclusion: Building Resilience for the AI Era

The AI arms race has begun and the rise of GenAI data leakage shows how quickly automation is redefining risk for enterprises worldwide. As we look ahead, the evolution of AI will not just accelerate — it will fundamentally redefine how organisations secure their digital future.

From synthetic insiders impersonating employees to adaptive malware that rewrites its own code, the threat landscape is transforming rapidly. To stay ahead, organisations must fight fire with fire. Prevention-first, AI-powered, cloud-delivered platforms are now essential — integrating predictive analytics, behavioural intelligence, and autonomous remediation to stop threats before they occur. Security will need to evolve from reactive tools into AI-powered, cloud-delivered platforms that predict and pre-empt attacks before they occur, integrating threat-informed intelligence, autonomous remediation, and continuous governance.

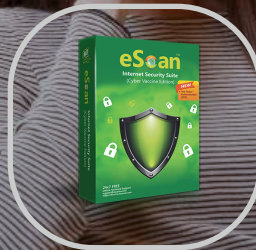
Check Point's Infinity AI Threat Prevention Engine, powered by ThreatCloud AI, already analyses millions of indicators from over 150,000 networks to block zero-day attacks in real time, while Harmony SASE and Harmony Browse secure GenAI usage and browser interactions at the cloud edge.

The future of cyber security will belong to those who embrace this platform-centric mindset — consolidating visibility and control across the digital estate and embedding Zero Trust and secure-by-design principles at every layer, turning AI from a risk into a decisive advantage.

As we celebrated Cybersecurity Awareness Month a few weeks ago, organisations should focus on raising literacy around both the benefits and risks of AI, preparing their people and infrastructure for a world where prevention, automation, and intelligence are the only sustainable strategies. Those who act now will transform AI from a risk into a decisive advantage — and build true digital resilience for the decade ahead. 

SOHO SPECIAL

Small Office Home Office Solution for India Market



Small Office and Home Office has been attracting lot of vendor attraction for quite some time. However, the segment attained critical significance with the advent of the Work from Home (WFH) culture triggered by the global pandemic. As an unprecedented migration of data to the cloud, kick-started by massive digitization across the globe, became the most visible phenomenon, it only further reinforced and provided the much required tailwind to the SOHO segment. Although the WFH culture has weathered a bit, it hasn't lost steam altogether. In fact today, enterprises have gleefully embraced a hybrid work culture. The WFH culture has resulted in a massive uptick in demand for SOHO products. Be it the ubiquitous wireless, optical mouse or the desktop mounted webcams; be it video collaboration software like zoom or Microsoft

Teams, connecting individuals with their teams across geographies or cybersecurity solutions that can protect your data privacy even on the face of expansive exposure of attack surface; be it visual output delivering monitors or powerful keyboards yielding raw performance; be it presentation spotlighting projectors or trendy Bluetooth PC Speakers, the SOHO segment is for sure passing through an interesting phase. It's overwhelmingly marked by three trends: TRACTION, TRACTION & TRACTION.

Given this, we, at SME Channels, have endeavored to bring before this SOHO Special Feature, which catalogues only the most impactful SOHO Products across business segments. Due care has been taken to map out only those select products that our editorial team feels can positively impact performance in a Home office environment. **SME**

BRAND NAME

XElectron

MODEL NAME

XElectron Techno Android 13 Smart Projector

WHAT'S UNIQUE ABOUT IT

The XElectron Techno Android 13 Smart Projector brings smart entertainment and productivity together in a compact, portable form. Powered by the latest Android 13 OS, it eliminates the need for external devices like laptops or streaming sticks by offering direct access to popular OTT platforms, apps, and online content. Designed for both home users and SOHO environments, it delivers a seamless viewing experience for movies, online meetings, digital classrooms, and presentations.

For entertainment lovers, it transforms any room into a personal home theatre with vibrant visuals and immersive sound. It supports wireless screen mirroring, making presentations, virtual meetings, and learning sessions.

KEY HIGHLIGHTS:

- Full HD Projection Support
- High Brightness Output for clear visuals
- Built-in Wi-Fi & Bluetooth Connectivity
- Wireless Screen Mirroring
- Dual Built-in Stereo Speakers
- Multiple Input Ports (HDMI, USB, AV)
- Compact, Lightweight & Portable Design

SOHO FRIENDLY QUOTIENT

With its Android 13 platform, wireless connectivity, screen mirroring, and compact design, the XElectron Techno Smart Projector is perfectly suited for small offices, home offices, coaching centres, and classrooms. It supports presentations, video conferencing, training sessions, without requiring heavy hardware setups.





XElectron

BRAND NAME

XElectron

MODEL NAME

XElectron iProjector 2 Plus Auto Focus

WHAT'S UNIQUE ABOUT IT

The XElectron iProjector 2 Plus Auto Focus is designed to deliver a seamless and intelligent projection experience for both entertainment and professional use. Its standout feature is the **auto-focus technology**, which automatically adjusts the image for perfect clarity within seconds of setup. This removes the hassle of manual focus and ensures a sharp display every time. Built for modern users, the projector supports smart connectivity and high-resolution projection, making it ideal for home theatres, classrooms, and business presentations.

KEY HIGHLIGHTS:

- **Auto Focus Technology for instant clarity**
- **Full HD Projection Support**
- **High Brightness for clear viewing in various lighting conditions**
- **Built-in Wi-Fi & Bluetooth**
- **Wireless Screen Mirroring**
- **Dual Built-in Speakers**
- **Multiple Connectivity Options (HDMI, USB, AV)**
- **Portable and Sleek Design**

SOHO FRIENDLY QUOTIENT

With its auto-focus precision, wireless connectivity, and quick plug-and-play setup, the XElectron iProjector 2 Plus is perfectly suited for small offices, home offices, coaching centres, and classrooms. It enables smooth presentations, online training sessions, video conferencing, and digital content sharing without complex installations. Its portability, smart features, and reliable performance make it a highly practical and cost-effective projection solution for SOHO users.

BRAND NAME

FRONTECH

MODEL NAME

FRONTECH 2.4G & Bluetooth Wireless Mouse

WHAT'S UNIQUE ABOUT IT

The FRONTECH 2.4G & Bluetooth Wireless Mouse is a dual-mode connectivity device designed for modern users who demand flexibility, efficiency, and comfort. Its key advantage lies in its ability to switch seamlessly between **2.4GHz wireless and Bluetooth modes**, allowing users to connect the same mouse to multiple devices such as laptops, desktops, tablets, and smart

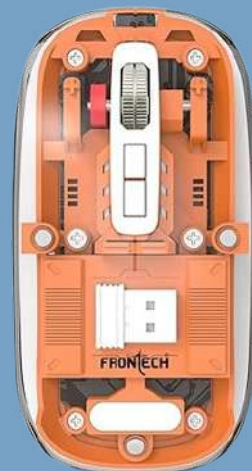
TVs. This makes it an ideal companion for professionals working across multiple screens and platforms.

KEY HIGHLIGHTS:

- **Dual-Mode Connectivity (2.4G Wireless + Bluetooth)**
- **Smooth Optical Sensor for Precise Tracking**
- **Ergonomic & Comfortable Design**
- **Silent Click Buttons for Noise-Free Working**
- **Long Battery Life with Power-Saving Mode**
- **Plug & Play USB Receiver**
- **Wide Device Compatibility (Laptop, PC, Tablet, Smart TV)**
- **Lightweight & Portable Build**

SOHO FRIENDLY QUOTIENT

With its dual-device connectivity, quiet operation, and ergonomic comfort, the FRONTECH 2.4G & Bluetooth Wireless Mouse is perfectly suited for small offices, home offices, students, and remote professionals. It supports multitasking across devices, improves efficiency during presentations and meetings, and ensures all-day comfort during work.



Frontech

BRAND NAME

Xiaomi

MODEL NAME

Xiaomi Power Bank 4i 20000mAh 33W

WHAT'S UNIQUE ABOUT IT

The Xiaomi Power Bank 4i 20000mAh 33W is a high-capacity fast-charging power solution designed for users who need reliable backup power on the go. What makes it truly stand out is its **33W super-fast charging capability**, which supports quick charging for smartphones, tablets, and even certain laptops. With a massive 20000mAh capacity, it is ideal for long trips, heavy users, and professionals who depend on their devices throughout the day.

KEY HIGHLIGHTS:

- 20000mAh High-Capacity Battery
- 33W Fast Charging Support
- Dual USB-A & USB-C Output Ports
- USB-C Fast Input for Quick Recharging
- Smart Power Management & Safety Protection
- Premium Build Quality
- Multi-Device Compatibility (Smartphones, Tablets, Accessories)
- Compact & Travel-Friendly Design

SOHO FRIENDLY QUOTIENT

With its high capacity, fast charging performance, and multi-device support, the Xiaomi Power Bank 4i 20000mAh 33W is perfectly suited for small offices, home offices, remote professionals, and students. It ensures uninterrupted power for smartphones, wireless devices, and work accessories during long meetings, travel, and power outages. Its reliability, speed, and portability make it a highly practical power backup solution for SOHO environments.



Xiaomi

BRAND NAME

Primebook

MODEL NAME

Primebook 2 Pro 2025

WHAT'S UNIQUE ABOUT IT

The Primebook 2 Pro 2025 is a next-generation budget-friendly laptop designed specially for students, educators, and SOHO users who want smart performance at an affordable price. What makes it unique is its **Android-based operating system optimized for laptops**, which allows users to enjoy the simplicity of Android with the productivity of a full keyboard and trackpad. It supports thousands of Android apps, making learning, browsing, content consumption, and light office work smooth and efficient.

KEY HIGHLIGHTS:

- Android-Based Laptop Operating System
- Large Full HD Display
- Lightweight & Portable Design
- Long Battery Life for All-Day Usage
- Built-in Wi-Fi & Bluetooth
- Full-Size Keyboard with Trackpad
- Multiple USB Ports & Connectivity Options
- Ideal for Students, Learning & Office Work

SOHO FRIENDLY QUOTIENT

With its affordable pricing, lightweight design, long battery life, and Android app support, the Primebook 2 Pro 2025 is perfectly suited for small offices, home offices, students, and digital learning centres. It supports online classes, video conferencing, document work, and billing.



Primebook

FROM THE GROUP EDITOR'S DESK



DRIVING GROWTH THROUGH TECHNOLOGY ADOPTION: A STRATEGIC IMPERATIVE FOR IT PARTNERS IN INDIA

■ **SANJAY MOHAPATRA**
sanjay@Accentinfomedia.com

As India's digital economy accelerates, 2026 will be a defining year for IT partners. The country's IT spending is projected to exceed \$176 billion, with double-digit growth driven by cloud, AI, and cybersecurity investments. For IT partners, this surge represents more than an opportunity—it's a mandate to embrace emerging technologies and reposition themselves as transformation enablers.

AI and Automation: The New Growth Engine

Artificial Intelligence is no longer a futuristic concept; it's becoming the backbone of enterprise operations. Indian businesses are moving from pilot projects to full-scale AI deployments, creating demand for partners who can deliver AI-driven solutions across verticals. Generative AI and hyperautomation will dominate, enabling predictive analytics, automated workflows, and personalized customer experiences. IT partners that invest in AI capabilities—whether through proprietary tools or alliances—will unlock new revenue streams and strengthen client relationships.

Cloud and Data Sovereignty: Building Trust

Cloud adoption continues to surge, with hybrid and multi-cloud strategies gaining traction. Microsoft's \$17.5 billion investment in India, including new hyperscale data centers, underscores the strategic importance of cloud infrastructure and AI integration for businesses nationwide. Partners must leverage these developments to offer secure, scalable solutions while addressing evolving data sovereignty requirements. Those who can combine global cloud platforms with localized compliance expertise will stand out in a competitive market.

Cybersecurity and Compliance: A Non-Negotiable Priority

With digital transformation comes heightened risk. Cybersecurity spending in India is expected to cross \$3.5 billion, driven by stricter regulations and rising threats. IT partners should expand their portfolios to include advanced threat detection, zero-trust architectures, and compliance automation. Solutions like predictive enforcement and privacy compliance tools are gaining traction, offering partners a chance to differentiate through proactive security services.

Empowering MSMEs and Tier-2 Markets

Government initiatives such as DXEdge and AI-driven public platforms are creating pathways for MSMEs to adopt digital technologies. IT partners can tap into this segment by offering affordable, modular solutions tailored to smaller enterprises. Additionally, emerging tech hubs in Tier-2 cities present untapped potential for partners willing to invest in localized talent and infrastructure.

The Bottom Line

For IT partners in India, technology adoption is no longer optional—it's the cornerstone of sustainable growth. By embracing AI, cloud, cybersecurity, and compliance solutions, and by extending reach to MSMEs and new geographies, partners can transform from service providers into strategic growth catalysts. The future belongs to those who innovate, collaborate, and lead with trust. **SME**

Deliver Next-Gen Remote IT Solutions to Your Customers

LogMeIn Rescue

Enterprise-ready
remote support
solution for rapid,
secure, customizable,
AI-powered
troubleshooting
across any device.

LogMeIn Resolve

Unified endpoint
management
platform for secure
all-in-one device
management,
Empower organizations
with proven tools for
secure, seamless
IT support and
management.

Join a network trusted for reliability, innovation, and partner growth.

Get in touch with our partner managers: rupali.rokde@goto.com for North and West and kaushik.mitra@goto.com for East and South India

PROSTARM

Power Redefined

ONE POINT CUSTOMISED POWER SOLUTIONS PROVIDER



BIS for UPS



ISO 9001:2015



ISO 45001:2018



ISO 20000-1:2018



ISO 14001:2015



ISO 50001:2018



ISO 27001:2022



TL 9000: 2016



Railways



IT Data Centre



Aviation



Power & Energy



Heavy Industrial



Defence



Materials Engineering



Solar Industries



PROSTARM INFO SYSTEMS LTD

EL-79, Mahape, TTC Industrial Area,
Navi Mumbai 400710

**PUNE | NAGPUR | AHMEDABAD | GUWATI | PATNA | RANCHI | BHUBHANESWAR |
KOLKATA | MOHALI | JAIPUR | LUCKNOW | JAMMU | NOIDA | BENGALURU | CHENNAI |
HYDERABAD | COIMBATORE | TELANGANA | UTTARAKHAND | BHOPAL | RAIPUR**