@entitworld @enterpriseitworld @enterpariseitworld

RS 350 | PAGES 40 | VOLUME 10 | ISSUE 11 WWW.ENTERPRISEITWORLD.COM

Enterprise IT WORLD

FOR THE CIOs. BY THE CIOs.

MARCH 2026

BUILDING THE FACTORY OF THE FUTURE:

SHARAD KUMAR AGARWAL'S DIGITAL VISION FOR JK TYRE

With cutting-edge AI, IoT, cloud ecosystems and human-centred digital design, JK Tyre aims to become one of the world's most advanced manufacturing organizations...**page no. 16**

micron™

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

HOW GULF TENSIONS AND MARKET GROWTH IN 2026 WILL IMPACT INDIA'S **TECHNOLOGY AND BUSINESS LANDSCAPE**

The year 2026 places India at a crucial strategic juncture. The Gulf region one of India's most important economic partners is experiencing a dual reality: heightened geopolitical tensions and strong diversified economic growth. For Indian enterprises, the intersection of these forces will define how the technology, energy and business landscape evolves over the next 12 months.

The Gulf remains central to India's stability. With millions of Indian workers in the GCC, critical energy dependencies, and expanding digital trade partnerships, even minor disruptions in the region reverberate across India's economy. Rising tensions involving Iran, Israel, and regional blocs have amplified concerns over supply-chain security, energy pricing, and maritime safety.

For Indian CIOs and CXOs, this emerging risk landscape makes resilience, redundancy, and real-time intelligence essential. Enterprises must prepare for volatility in energy costs, potential delays in imports, and fluctuations in global capital flows all of which influence IT budgets, cloud investments, and digital transformation roadmaps.

Despite uncertainty, the Gulf's economic trajectory remains strong. Driven by aggressive diversification efforts, investments in AI, digital infrastructure, advanced manufacturing, and financial services, the GCC is rapidly emerging as one of the world's most future-ready regions.

For India, this opens multiple high-impact opportunities:

Gulf governments and enterprises are accelerating cloud adoption, cybersecurity modernization, and AI deployment. Indian IT companies both large and mid-tier are uniquely positioned to deliver these capabilities at scale.

Saudi Arabia, UAE, and Qatar are expanding hyperscale data center capacity and AI supercomputing clusters. This aligns with India's strengths in system integration, GPU infrastructure, edge computing, and managed services.

As GCC economies invest in AI-driven transformation, demand for Indian cloud architects, cybersecurity specialists, and AI engineers is surging strengthening India's role as a global talent hub.

Any spike in Gulf-driven oil prices impacts India directly through higher inflation, IT procurement costs, and delayed enterprise spending. As a result, Indian organizations are prioritizing cost-optimized cloud strategies, automation-driven efficiency, and hybrid infrastructure to absorb volatility.

India's enterprise ecosystem must operate with both strategic caution and market confidence. While Gulf tensions pose undeniable risks, the region's economic transformation presents unmatched potential for India's IT services, digital infrastructure companies, and innovation-driven enterprises.

The winners will be businesses that invest early, diversify intelligently, and build resilient architectures capable of navigating uncertainty while capturing growth. ENT

SANJAY MOHAPATRA
SANJAY@ACCENTINFOMEDIA.COM

NEXT MONTH SPECIAL

COVER STORY

FUTURE OF DATA CENTRE

The next issue is dedicated to the Future of Data Centre. We would like to take feedback from the CIOs and OEMs and create our judgment on the same.

SUPPLEMENT

QUOTES FROM TOP CIOS

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

PLUS

Interviews and Case Studies

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

Send in your inputs to sanjay@accentinfomedia.com

CONTENTS

VOLUME 10 | ISSUE 11 | MARCH 2026 | WWW.ENTERPRISEITWORLD.COM

COVER STORY

SECURITY /20

PHILIPPA COGSWELL

"Palo Alto Networks Unit 42 Warns of AI-Accelerated Attacks in Global Incident Response Report 2026"

MORE INSIDE

Enterprise IT WORLD
FOR THE CIOs. BY THE CIOs.

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

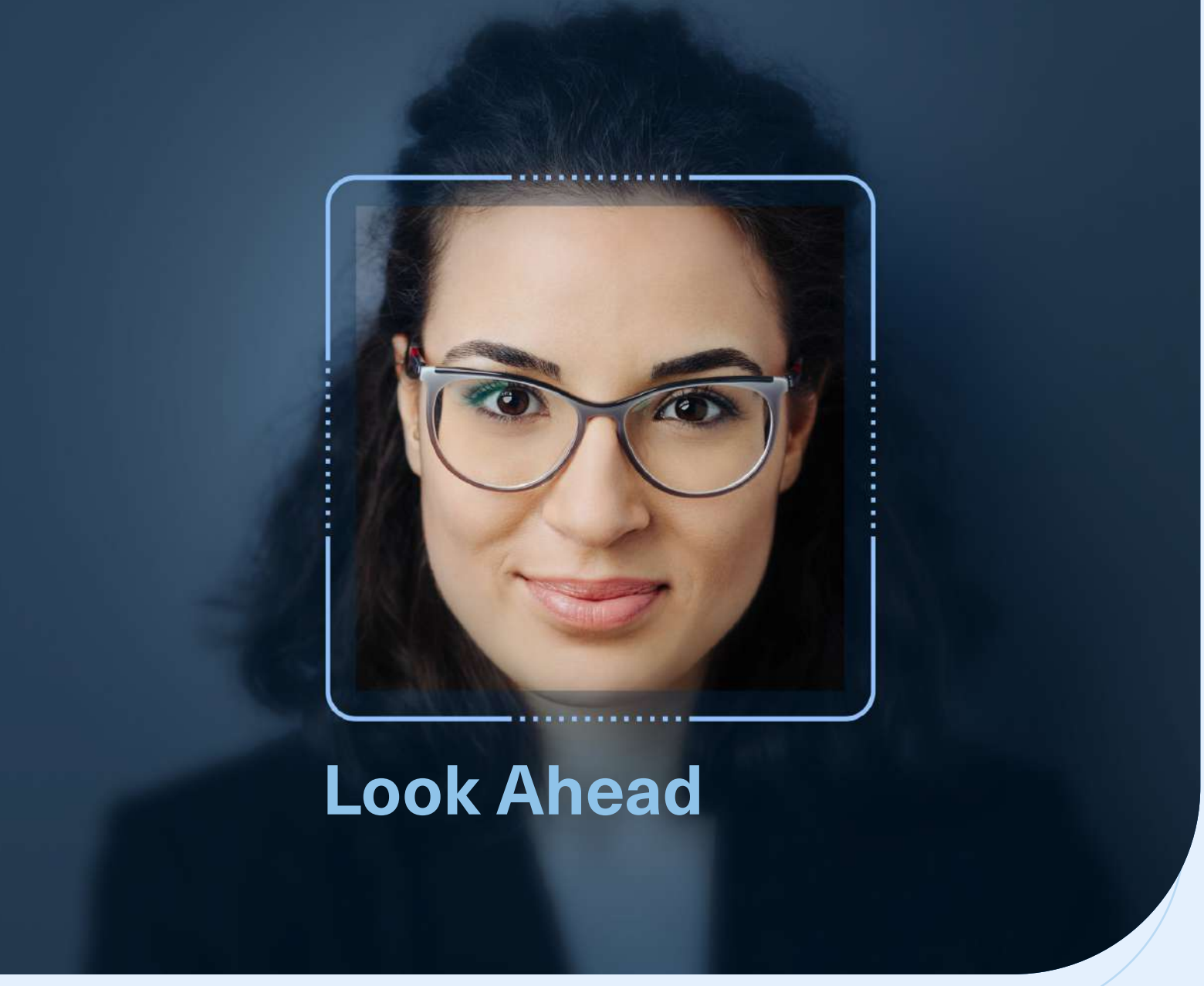
MARKETING
Print & Advertising: Annie Garg
Marketing Manager: Sangram R. Barpanda

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

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

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

Subscription: Rs.4000 (12 issues)
All payments favouring: Accent Info Media Pvt. Ltd.

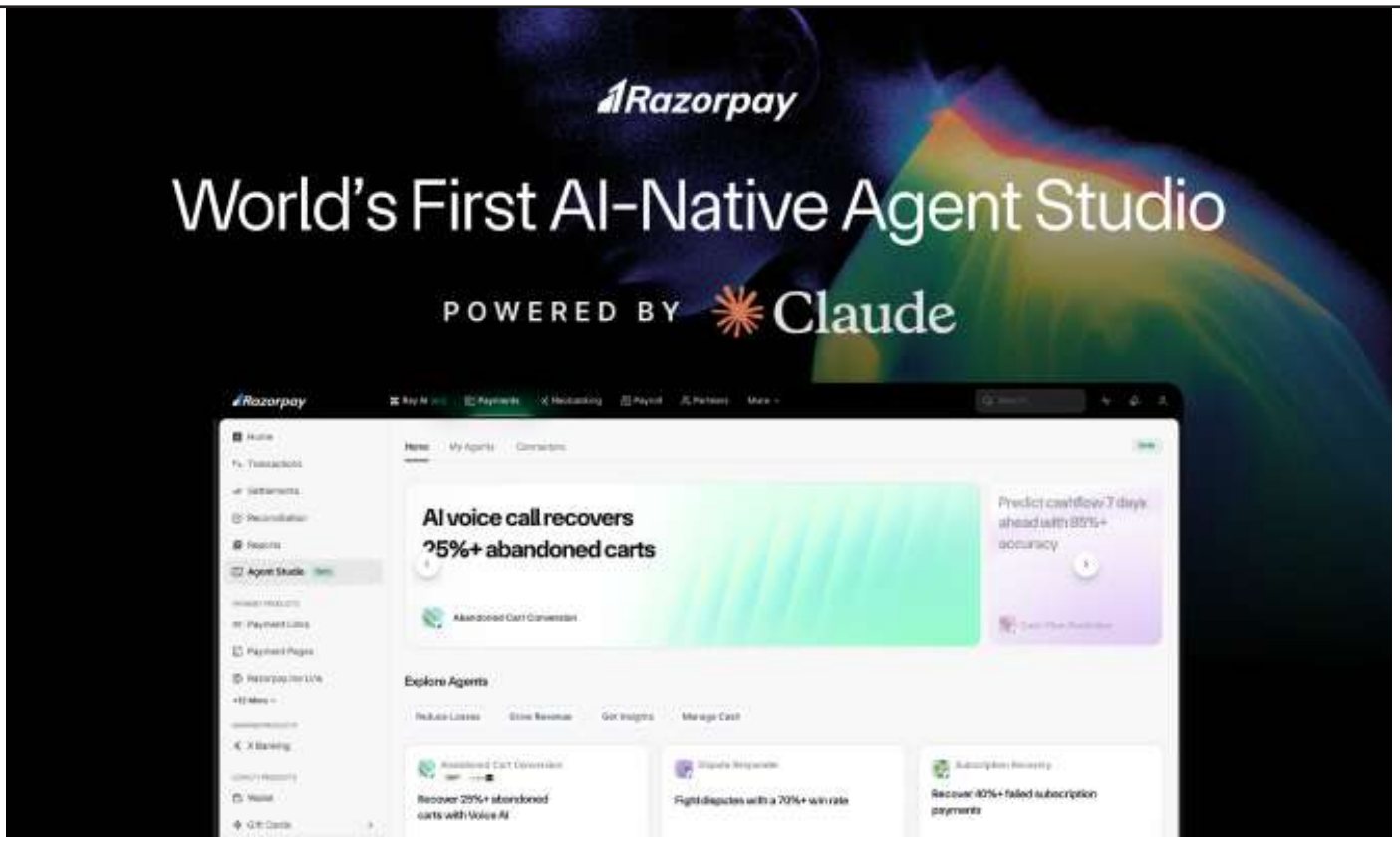


HID® Amico™ Facial Recognition Reader: **Built for Speed**

Ready to modernize your access control system?
hidglobal.com/products/amico

HID
Powering **Trusted Identities**

ITWORLD ROUND UP



Razorpay Unveils World's First AI Agent Studio at FTX'26

At FTX'26, excitement filled the hall as Razorpay introduced a breakthrough that promised to reshape payment operations. The company launched Agent Studio, the world's first AInative agent studio for payments, powered by Anthropic's Claude.

For years, businesses struggled with the behindthescenes chaos of transactions failed subscriptions, abandoned carts, disputes, and unpredictable cashflows. Agent Studio aimed to change that entirely. It brought together a suite of intelligent, nocode AI agents capable of handling tasks that once required manual effort or multiple disconnected tools.

During the live demo, the audience watched as one agent revived a failed subscription instantly, another resolved a dispute contextually, and a third forecasted cashflow with remarkable accuracy. All of it happened through simple instructions, proving how accessible AIdriven automation could be.

"With Agent Studio, we're making advanced AI practical and powerful for every merchant," the presenter announced, drawing murmurs of approval from industry experts who saw it as a major shift toward autonomous "agentic" financial systems.

Razorpay also unveiled the Agentic Experience Platform, a conversational AI interface designed to support merchants through onboarding, integrations, troubleshooting, and daily operations reducing friction across the payment lifecycle.

As transaction volumes rise and customer journeys grow more complex, Razorpay's new AI-powered ecosystem promises to handle operational intricacies so businesses can focus on growth and innovation. With these launches, the company signaled the beginning of a new era in automated payment management.

DATA BRIEF

"HR Survey Reveals 45% of Managers Report AI Has Lived Up to Their Expectations in Improving Their Teams' Work": Gartner

Zendesk to Buy Forethought as AI Agents Set to Outperform **Humans in 2026**

Zendesk's latest announcement sent a clear signal across the customer service world: the era of AIfirst support has officially begun. The company revealed a definitive agreement to acquire Forethought, a move it says will accelerate the shift toward what it calls the "agentic service era."

According to Zendesk, 2026 will be the first year autonomous AI agents resolve more customer service interactions than human agents a structural pivot in how service organisations operate. The Forethought acquisition is designed to fasttrack that future.

By integrating Forethought's advanced workflow automation and reasoning capabilities into the Zendesk Resolution Platform, the company plans to deploy AI agents that can handle complex tasks across chat, email, voice, and even internal enterprise systems. Zendesk says this integration will advance its AI roadmap by more than a year and give customers immediate access to smarter, selfimproving automation.

CEO Tom Eggemeier emphasised that customer service is quickly moving beyond managing conversations to ensuring outcomes. "Resolution is our identity, and loyalty is the outcome," he said. "With Forethought, we're scaling AI that learns from every interaction and resolves issues endtoend."

Forethought CEO Sami Ghoche echoed this vision, calling the acquisition the fastest path to bringing transformative AI to global enterprises.

Currently, Zendesk's AI resolves over 80% of routine inquiries for many customers. With Forethought, these agents will gain new abilities from autonomous workflow creation to expanded voice capabilities and execution of multistep processes across systems without APIs.

The deal is expected to close by the end of March, pending regulatory approval.

NETSCOUT Flags Surge in HyperScale DDoS Attacks as Global I**ncidents Top 8 Million**

The threat landscape took a darker turn in 2025, and NETSCOUT's latest DDoS Threat Intelligence Report makes it unmistakably clear: attackers are evolving faster than defenders can react. The company's secondhalf 2025 findings reveal more than eight million DDoS attacks worldwide, signalling a dramatic rise in both scale and sophistication.

At the core of this escalation are AIcoordinated threat campaigns, resilient botnets, and an expanding army of compromised IoT devices. NETSCOUT reports peak attack volumes hitting 30 terabits per second, a milestone that marks the emergence of hyperscale DDoS operations capable of overwhelming even heavily fortified networks.

The report highlights a shift toward adaptive, multivector strategies. Nearly 42% of attacks combined multiple vectors, often switching tactics midstream to evade mitigation systems. Critical services such as DNS and NTP continue to face relentless pressure, underscoring the need for globally resilient architectures.

"Adversaries are scaling faster than traditional defences can keep up," said Richard Hummel.

CIO **EVENTS**

02-05 MAR, 2026

MWC Barcelona 2026
The world's biggest mobile, connectivity, 5G/6G, IoT, and edgecomputing event.

PLACE:
BARCELONA, SPAIN

16-19 MAR, 2026

NVIDIA GTC 2026
One of the largest global AI events covering GPUs, LLMs, robotics, enterprise AI, and accelerated computing.

PLACE:
SAN JOSE, USA

02-05 MAR, 2026

4YFN (4 Years From Now) at MWC
Global startup and innovation showcase under GSMA.

PLACE:
BARCELONA, SPAIN

04-05 MAR, 2026

Affiliate World Dubai
Major event for performance marketing, martech, and digital commerce technologies.

PLACE:
DUBAI, UAE

MTCTE CERTIFIED

D-Link®

TRANSFORMING SMART HOME NETWORKS

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

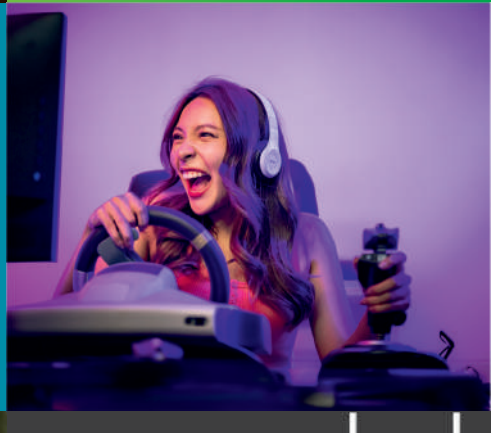
Whole Home Mesh Router

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

in.dlink.com | sales@in.dlink.com

Follow us:

Cohesity Unveils Enterprise AI Resilience Strategy to Secure and **Scale AI Adoption**

As enterprises rush to embed AI into their core operations, Cohesity has stepped forward with a bold new framework designed to tackle the growing risks in the AI ecosystem. The company launched its Enterprise AI Resilience strategy, a unified approach aimed at protecting AI infrastructure, securing enterprise data, and mitigating threats arising from increasingly autonomous AI agents.

With AI now moving from pilot projects to missioncritical workflows, organizations face new vulnerabilities from volatile AI agents to sensitive training datasets and complex vector databases. Traditional cybersecurity methods, Cohesity warns, were never designed for this level of automation or machinespeed disruption.

"Resilience can no longer be reactive it must be built into the AI stack from day zero," said Karen Townsend, Chief Product Officer.

Cohesity's approach centers on layered protection for AI components, including model configurations, agent memory, vector stores, and training data. Using immutable snapshots and precise pointintime recovery, the platform enables rapid restoration from both unintentional failures and malicious activity.

The strategy also targets one of the biggest emerging risks: rogue automation. Through integrations with ServiceNow and Datadog, Cohesity can turn risk signals into automated, APIdriven recovery workflows, dramatically reducing downtime during AIrelated incidents.

Data governance remains a pillar of the framework. Cohesity's DSPM capabilities powered by Cyera help organizations discover sensitive data, monitor access, and enforce compliance across AI environments.

In India, Cohesity says adoption is accelerating quickly. "Enterprises are moving AI into core operations," said Mayank Mishra. "We're enabling them to protect infrastructure.

S/HE SAID IT

IDC GLOBAL IT OUTLOOK 2026

"A conflict lasting up to three months would reduce global IT market growth by roughly one percentage point."

"Incidents of this scale typically generate tens of millions of dollars in combined operational losses."

MATVII DIADKOV, TECH INVESTOR

QUICK BYTE ON SECURITY

GTT Integrates Insurants AI to Boost Global I**nsurance Intelligence**

GTT Data Solutions has taken a major step toward expanding its global insurance technology footprint with the integration of Insurants AI Limited. The move aligns with GTT's mission to build Indiadeveloped AI and data platforms for worldwide deployment, strengthening its presence across regulated markets including the US, UK, Europe, India, and APAC.

Founded in 2018, Insurants AI brings deep expertise in insurance data intelligence, advanced analytics, and data harmonization critical capabilities for sectors with stringent regulatory requirements such as insurance and financial services. Its integration significantly enhances GTT's ability to deliver nextgeneration platforms supporting underwriting, claims automation, compliance workflows, and full policy lifecycle intelligence.

Databricks Unveils Genie Code, Ushering In the Era of **Agentic Data Engineering**

Databricks has introduced Genie Code, a breakthrough autonomous AI agent designed to transform how data engineering, data science, and analytics teams build and operate production systems. The launch marks a major step toward what the company calls "Agentic Data Work", where AI agents move beyond code assistance to fully planning, executing, validating, and maintaining data workflows with minimal human intervention.

Built as an extension of the Genie platform which already enables conversational access to enterprise data using Unity Catalog semantics Genie Code pushes automation deeper into technical domains. Databricks says the agent can autonomously construct data pipelines, debug failures, ship dashboards, and maintain endtoend production workloads. In realworld testing, it more than doubled the taskcompletion success rate of leading coding agents.

"We're moving from AIassisted coding to AI agents doing the work, guided by humans," said Ali Ghodsi, Cofounder and CEO of Databricks.

Alongside the launch, the company announced the acquisition of Quotient AI, a startup specializing in evaluating and improving AI agents through reinforcement learning technology that will now be integrated into both Genie and Genie Code for continuous performance monitoring.

Designed to act like an expert data professional, Genie Code handles ML workflows, enforces enterprise governance via Unity Catalog, monitors pipelines, resolves anomalies, and ensures productiongrade reliability. Early adopters such as SiriusXM and Repsol report faster data delivery.

Netskope Launches 'One AI Security' to Protect the Full AI Stack **Amid Surging Enterprise Risks**

As AI adoption accelerates across global enterprises, Netskope has introduced Netskope One AI Security, a comprehensive security suite built to safeguard the rapidly expanding AI ecosystem from agents and applications to models, data flows, and user interactions.

Integrated directly into the unified Netskope One platform, the new suite features One Agentic Broker, AI Guardrails, AI Gateway, and AI Red Teaming. Together, they target emerging risks such as Shadow AI, data leakage, manipulative prompts, prompt injection, jailbreaking, and unsafe autonomous agent behaviour. Netskope says this architecture addresses security gaps that legacy tools can no longer manage in an era of self-directed AI systems.

The company also debuted the AI Index, a global dashboard offering realtime visibility into AI usage patterns, adoption trends, and risk levels across regions including India and broader Asia giving enterprises a dynamic understanding of how AI is evolving.

"AI's explosive growth demands a new security architecture built for autonomous, agentic systems," said Sanjay Beri, CoFounder and CEO of Netskope.

EXECUTIVE MOVEMENT

Deepak Bhardwaj Joins Pinnacle Infotech as Global CIO, to Lead Global IT & Cybersecurity Transformation

GoTo Appoints Sivakumar Ekambaram as New India Site Leader

LatentView Analytics Appoints Former Google and Amazon Leader Kiran Muddana to Advisory Council

Redis Strengthens India Leadership with Appointment of Abhoy Kumar Sarkar

CrowdStrike Appoints Jonathon Dixon to Lead JAPAC Growth and Drive AI-Powered Cybersecurity Transformation

GLOBAL UPDATE

Brahma AI, Google Cloud Partner to Scale HyperReal Digital **Humans for Global Enterprises**

Brahma AI has entered a multiyear strategic partnership with Google Cloud, aiming to bring highfidelity, interactive digital humans called ATMANS to enterprises worldwide. Built on the same Academy Awardwinning technologies used in Interstellar and Dune, Brahma AI will now tap into Google Cloud's advanced AI stack, including Veo for generative video and Gemini for multimodal intelligence, to scale productiongrade digital likenesses across industries.

The collaboration targets sectors such as healthcare, media, sports, retail, and global services, enabling organizations to deploy digital humans capable of realtime, multilingual, emotionally rich interactions. Each ATMAN is crafted with identityaware precision, reflecting an individual's likeness, persona, and performance attributes to create experiences nearly indistinguishable from live human engagement.

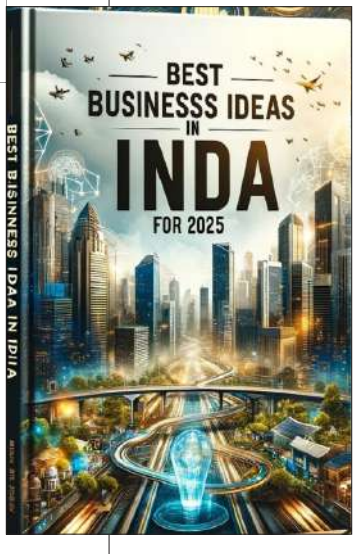
"Enterprises don't just need AI generation they need trusted systems that preserve identity, consent, and creative control," said Prabhu Narasimhan, CEO of Brahma AI.

A core differentiator is Mind², Brahma AI's governance framework built on strict consent workflows and C2PAaligned tamperevident watermarking, ensuring traceability and protection against synthetic media misuse. Thomas Kurian, CEO of Google Cloud, emphasized that the partnership brings "fidelityrich, enterprisegrade digital experiences built on secure AI foundations."

Use cases range from physicianguided patient navigation in native languages to artistdriven global campaigns, athlete fan engagement, and hightouch retail concierge services all powered by ethically.

BOOK SHELF

Best Business Ideas in India for 2025



PRICE: 299 (KINDLE EDITION)

Author : CHETAN KUMAR

About The Book

Best Business Ideas in India for 2025 by Chetan Kumar is an insightful and timely guide for aspiring entrepreneurs looking to build a futureready venture in one of the world's fastestgrowing economies. The book opens with a clear focus on India's entrepreneurial spirit and the macro trends shaping the country's economic trajectory including digital adoption, ecoconscious consumer behavior, and the expanding opportunities across both rural and urban markets.

One of the book's strongest aspects is its wellstructured, categorywise breakdown of business ideas. Kumar covers a wide spectrum from AIdriven services, Web 3.0 solutions, and cybersecurity for SMEs to sustainable ventures like solar installations, organic farming, and recycledproduct manufacturing.

SailPoint Launches Adaptive Identity Upgrades to Secure Human, Machine & AI Identities **in Real Time**

SailPoint has unveiled major enhancements to its AIpowered SailPoint Platform, marking the first wave of innovations under its new adaptive identity vision. Designed for modern, cloudfirst, AIdriven enterprises, the upgraded platform brings realtime identity governance across human users, machine identities, and fastgrowing autonomous AI agents.

With organisations rapidly scaling cloud workloads and deploying AI across business processes, traditional periodic identity reviews can no longer keep pace. SailPoint's new capabilities shift enterprises toward continuous, automated, riskaware governance an approach the company says is essential for today's dynamic environments.

"The old way of identity governance is no longer effective. Enterprises now need continuous, AIpowered, realtime governance to stay secure," said Chandra Gnanasambandam, EVP of Product & CTO.

A standout addition is SailPoint's new privilege discovery and classification engine, which automatically identifies unmanaged privilege, maps risk exposure, and secures access across sprawling enterprise environments. The platform also introduces expanded governance for nonhuman identities including AI agents from ecosystems such as Microsoft 365 Copilot, Databricks, Amazon Bedrock, and Google Vertex AI.

SailPoint is also strengthening machine identity protection with full lifecycle management, while a new AIpowered Harbor Pilot agent simplifies access requests through guided conversations.

Additional enhancements include deeper threat detection through Observability & Insights, unified data access visibility via the Identity.

Fortinet Rolls Out FortiOS 8.0 with AIDriven Security, NextGen SASE, and Quantum**Safe Protection**

Fortinet has unveiled FortiOS 8.0, the latest version of its flagship operating system powering the Fortinet Security Fabric. Announced at Accelerate 2026, the new release introduces a wave of AIdriven capabilities, nextgeneration SASE enhancements, and expanded quantumsafe cryptography advancing Fortinet's vision of tightly converged networking and security for the AI era.

Ken Xie, Founder and CEO of Fortinet, said the launch reflects "over 25 years of innovation at the intersection of networking and security," emphasizing that enterprises now require a unified platform capable of handling AI, encrypted traffic, and distributed cloud architectures.

FortiOS 8.0 brings deep AIaware visibility and governance as organizations increasingly adopt generative AI and autonomous agents. New features include FortiView for AI to track sanctioned and shadow AI usage, AIaware application controls, and enhanced DLP with OCR to detect data leakage through images and screenshots. The OS also supports Model Context Protocol (MCP) and agenttoagent visibility to uncover hidden AI interactions.

Bounteous x Accolite and Agile Network India Spotlight Data Strategy & Digital **Trust at Chennai Meetup**

Bounteous x Accolite partnered with Agile Network India to host the Chennai chapter meetup, "Beyond Clicks: Data, Decisions and Digital Trust," on February 28, 2026. The event brought together more than 40 technology leaders, agile practitioners, and industry experts to examine how data strategy, AI readiness, and digital trust are reshaping enterprise decisionmaking.

Agile Network India, known for its practitionerdriven community focus, facilitated open discussions on how organizations are moving beyond traditional engagement metrics toward intelligencedriven, privacyaware digital ecosystems. A recurring theme was the tension between personalization and privacy, especially as AI models rely heavily on behavioral and contextual data. Speakers stressed that trust must be architected into digital systems from the start, not added later as a compliance layer.

Anuradha Balasubramanian, EVP of Delivery at Bounteous x Accolite, noted that the enterprises that win will be those building AIdriven systems that deliver insights responsibly while safeguarding user trust.

Delta Electronics India & TNSDC Open Robotics and Automation Centre of **Excellence in Krishnagiri**

Delta Electronics India, in partnership with the Tamil Nadu Skill Development Corporation (TNSDC), has inaugurated a stateoftheart Centre of Excellence (CoE) in Robotics and PLC Automation at the College of Engineering, Bargur, in Krishnagiri district. The facility aims to bridge the gap between classroom learning and industry-ready automation skills, strengthening Tamil Nadu's position as a national hub for advanced manufacturing.

Implemented by the Tamil Nadu Apex Skill Development Centre for Automobile (TN AutoSkills), the new CoE will cater to engineering students, working professionals, and jobseekers seeking hands-on training in robotics, programmable logic controllers (PLC), and smart assembly systems core technologies powering Industry 4.0. The centre houses 4axis and 6axis industrial robots, PLC workstations, and a smart screwdriver assembly cell that replicates real factory environments.

"This collaboration brings advanced robotics and automation training closer to our youth, preparing them to drive Tamil Nadu's manufacturing growth," said District Collector Thiru C. Dinesh Kumar.

Benjamin Lin, President of Delta Electronics India, emphasized the company's long-term commitment to strengthening India's industrial ecosystem, while Managing Director Niranjan Nayak highlighted that the CoE mirrors real-world factory conditions to maximize practical learning.

DIGEST

OPTIVALUE TEK AND SFJ FORM GLOBAL ALLIANCE TO DRIVE FORTUNE 500SCALE ENTERPRISE TRANSFORMATION

OptiValue Tek and SFJ Business Solutions have entered into a highimpact global alliance aimed at delivering multimilliondollar transformation programs for Fortune 500 companies. The partnership brings together OptiValue Tek's global execution capabilities with SFJ's expertise in strategic advisory and enterprisewide transformation governance, forming a unified engine designed to accelerate modernization at unprecedented scale.

At the center of the collaboration is a shared mission: empowering enterprises to transition into intelligent, autonomous, selfoptimizing organizations. With large companies facing intensifying pressure to modernize technology stacks, strengthen operational resilience, and embed AIdriven decision systems, the alliance positions both organizations as strategic partners for nextgeneration enterprise reinvention.

HEXNODE LAUNCHES HEXNODE IDP, ADDING NATIVE IDENTITY MANAGEMENT TO ITS UNIFIED SECURITY PLATFORM

Hexnode, the enterprise software arm of Mitsogo, has expanded its security portfolio with the launch of Hexnode IdP, a native Identity Provider built directly into the Hexnode UEM ecosystem. Arriving shortly after the introduction of Hexnode XDR, the new release marks a major step toward Hexnode's vision of a fully unified, endtoend enterprise security architecture.

Unlike standalone identity tools, Hexnode IdP is embedded at the platform level, combining identity, device intelligence, and access control into a single security fabric.

HEALTHCARE SEES SURGE IN GENAIDRIVEN DATA LEAKS AS SENSITIVE RECORDS DOMINATE VIOLATIONS

Healthcare organisations are confronting a fastescalating internal datarisk crisis as employees increasingly rely on generative AI tools and cloud applications. Netskope Threat Labs' latest annual healthcare threat report reveals that regulated healthcare data accounts for a staggering 89% of all GenAIrelated violations, nearly triple the 31% crossindustry average. Patient records, diagnostic files, and clinical notes are being pasted into prompts or uploaded into AI apps often without security oversight.

Ray Canzanese, Director at Netskope Threat Labs, warned: "Without strong guardrails around cloud and AI usage, regulated patient data will continue to leak at alarming rates."

MANAGEMENT **MANTRA**

“Own the problem, own the outcome.”

Sundar Pichai

NETGEAR Academy Unites 12 Top AV Brands on a Single Free **AVoverIP Learning Platform**

NETGEAR has expanded NETGEAR Academy (academy.netgear.com) into one of the industry’s most comprehensive free training hubs for AVoverIP professionals. With training content now contributed by twelve leading AV and broadcast manufacturers, the platform aims to address AsiaPacific’s mounting skills shortage as organizations shift rapidly toward IPcentric AV infrastructure.

As enterprises, education institutions, governments, live event operators, and broadcasters accelerate adoption of converged AVIT systems, demand for skilled AVoverIP professionals has surged. NETGEAR Academy’s unified, vendor-agnostic model responds to this gap by offering a complete curriculum spanning networking fundamentals, AVoverIP protocols, configuration practices, and realworld deployment scenarios. Unlike traditional training programs that operate in silos, NETGEAR Academy brings the ecosystem together helping learners understand how multivendor technologies interoperate in modern deployments.

The platform is also AVIXAaccredited, enabling learners to earn Renewal Units (RUs) toward CTS and ANP certifications, boosting career growth for AV and IT.

Intuit and Anthropic Forge Bold Alliance to Build the Future **of Financial AI**

Intuit has embarked on a transformative journey by partnering with Anthropic to bring a new era of intelligent, customizable financial AI agents to consumers and midmarket businesses. The multi-year collaboration will weave Anthropic’s Claude AI directly into Intuit’s ecosystem TurboTax, QuickBooks, Credit Karma, Mailchimp, and the Intuit Enterprise Suite unlocking automated decisionmaking once reserved for experts.

At the heart of the initiative lies a simple but powerful promise: anyone, even without technical skills, can build AI agents that understand the intricacies of their finances and workflows. These agents will merge Intuit’s decades of tax, accounting, and financial expertise with Claude’s advanced Agent SDK, enabling businesses to orchestrate previously complex processes with ease.

Imagine a restaurant chain where an AI agent continuously analyzes inventory, payroll, and operational costs across every outlet surfacing margin drops before they become problems. Or a construction subcontractor managing multiple projects, where an agent automatically tracks compliance deadlines, predicts cashflow gaps.

Everpure Emerges: Pure Storage Rebrands to Lead the Next Era **of AIDriven Data Management**

Pure Storage has officially stepped into a new chapter of its evolution reintroducing itself to the world as Everpure, a brand identity designed to reflect its expanding ambition beyond storage and into fullscale, AIready data management. The rebrand marks one of the company’s most significant transformations and arrives alongside its intent to acquire 1touch, a leader in data intelligence, discovery, and orchestration.

At the core of Everpure’s new mission is a bold objective: to provide enterprises with fully contextualized, instantly available, continuously protected data the kind required to unlock real, productiongrade AI. This vision is powered by the company’s Enterprise Data Cloud (EDC) architecture and strengthened by the Evergreen financial model, both of which aim to streamline the fragmented and laborintensive data estates that have long hindered AI initiatives.

CEO Charles Giancarlo positioned the transformation as a natural next step in the company’s journey. “Everpure reflects the company we have become as we help enterprises unleash the full power of their data,” he said. The planned acquisition of 1touch will extend this mission by adding deep data discovery, classification, and semantic enrichment critical capabilities for enterprises preparing to scale AI into production.

1touch CEO Ashish Gupta echoed the importance of context in the AI era, stating that meaningful intelligence depends on organizations understanding their data at the deepest level.

Everpure will begin trading under its new identity on the NYSE starting March 5, 2026, retaining its existing ticker symbol, PSTG but signaling a dramatically expanded future.

Akamai and NVIDIA Break New Ground with Agentless Zero Trust **for Critical Infrastructure**

In a major leap for industrial cybersecurity, Akamai and NVIDIA have unveiled a breakthrough solution that finally brings true Zero Trust segmentation to the world's most sensitive operational technology (OT) environments without the need for software agents. Designed for sectors like energy, water, manufacturing, and transportation, the integration between Akamai Guardicore Segmentation and NVIDIA BlueField DPUs targets one of the industry's most persistent challenges: securing legacy or highperformance systems that cannot tolerate traditional security tools.

For decades, operators of critical infrastructure have faced a painful dilemma deploy modern security and risk disrupting fragile systems, or maintain stability at the cost of increased exposure. This new Akamai–NVIDIA solution eliminates that compromise entirely. By offloading segmentation, traffic analysis, and threat isolation to the BlueField DPU, the approach delivers hardwareisolated protection that never touches the host machine.

"We're giving critical infrastructure a way to stop attacks without slowing down what keeps the world running," said Ofer Wolf, SVP of Enterprise Security at Akamai. With security functions executed entirely offhost, organizations gain realtime visibility, anomaly detection, and microsegmentation all without taxing CPU performance or risking operational downtime.

The launch arrives as governments worldwide intensify scrutiny of OT security, warning of rising attacks.

Prudent Technologies Enters GSMA Open Gateway to Shape the Future of Global **Telecom APIs**

Prudent Technologies has taken a significant step onto the world stage by joining the GSMA Open Gateway initiative, a global effort to standardize network APIs and strengthen digital trust across telecommunications. The move positions the Indian ICT provider among a powerful consortium of operators and technology players working to harmonize CAMARAbased Open Gateway APIs that now span more than 300 mobile networks worldwide.

Built around secure, interoperable APIs, the GSMA Open Gateway program allows operators to expose network intelligence such as number verification, SIMswap detection, and identity authentication essential tools as global fraud surges and enterprises seek more secure, seamless onboarding experiences.

By joining the initiative, Prudent Technologies brings longstanding expertise in secure messaging, authentication frameworks, and telcograde API infrastructure. The company's involvement is expected to accelerate the commercial rollout of standardized network capabilities across markets, enabling banks, fintechs, ecommerce platforms, and government agencies to adopt stronger, more reliable fraudprevention mechanisms.

AHEAD India Leadership Calls for Moving Beyond AI **Hype to RealWorld Enterprise Execution**

Global enterprise technology leaders gathered at AHEAD India are pushing for a decisive shift from AI experimentation to practical, scaled execution calling it the next defining moment for enterprise transformation. In a series of closeddoor leadership roundtables, senior executives including CTO Eric Kaplan, CIO Donnie Lochan, Managing Director Sumed Marwaha, Chief Security Officer Grant Sewell, and SVP of Enterprise AI Engineering Dave Dowsett emphasized that AI's future impact will depend on disciplined operating models, seamless integration, and securityfirst design.

Across the discussions, one theme dominated: AI pilots no longer suffice. Leaders stressed that enterprise success hinges on embedding AI into core workflows, decision systems, and digital platforms rather than treating it as a parallel experiment. Kaplan captured this sentiment clearly, noting that measurable outcomes only emerge when AI is tightly aligned to real business challenges and deployed at scale.

The sessions also spotlighted the evolving human dimension of AI adoption. Technology alone is not enough, leaders agreed organizations must invest in skills transformation, leadership alignment, change management, and a governance structure capable of absorbing continuous AIdriven change.

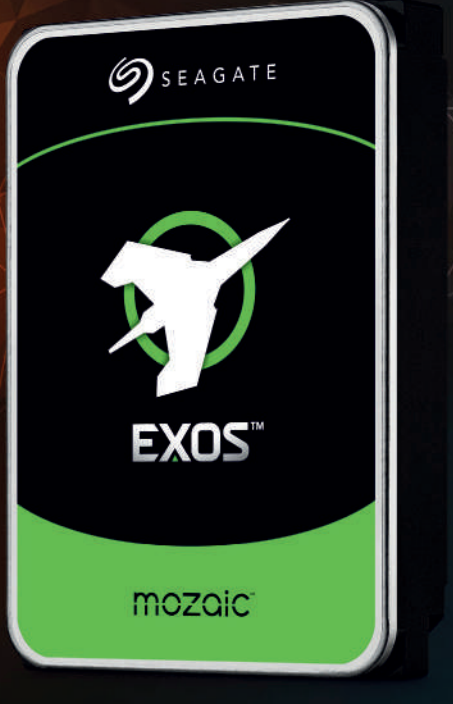
On cybersecurity, the message was equally urgent. As identity becomes the new control plane for both humans and machines, participants highlighted the browser's growing role as the enterprise workspace. Sewell reinforced that operational resilience is paramount, positioning security as "an operating model, not a department," with AI enhancing human expertise rather than replacing it.

The roundtables also affirmed India's rising global role in AI engineering, 24×7 security operations, and enterprisescale delivery. AHEAD India's depth in cloud, data, AI, and cybersecurity.

SEAGATE | mozaic 3+ | EXOS™

Maximize scale. Optimize TCO. Sustain the future.

Powered by Seagate's Mozaic 3+ technology, the Exos M 32TB hard drive breaks through data center limitations with an exceptional 3TB per platter density.



Best-fit applications

- Scalable hyperscale applications/cloud data centers.
- Massive scale-out data centers.
- Big-data applications.
- High-capacity, high-density RAID storage.
- Mainstream enterprise external storage arrays.
- Distributed file systems, including Hadoop and Ceph.
- Enterprise backup and restore–D2D, virtual tape.

www.seagate.com

For sales enquiries, contact: **Sanjay Khushlani (Supertron)** - 98110 59025. Email: sanjay.khushlani@supertronindia.com
For marketing support, contact: **Talwinder Singh** - 96438 99527. Email: talwinder.singh@seagate.com

Seagate Authorised Distributor SUPERTRON

BUILDING THE FACTORY OF THE FUTURE: SHARAD KUMAR AGARWAL'S DIGITAL VISION FOR JK TYRE

With cutting-edge AI, IoT, cloud ecosystems and human-centred digital design, JK Tyre aims to become one of the world's most advanced manufacturing organizations.

BY SANJAY@ACCENTINFOMEDIA.COM

JK Tyre & Industries stands today as one of India's most forward-looking manufacturing organizations, not just in the tyre sector but across the broader landscape of industrial digital transformation. The company's technology leadership is spearheaded by Sharad Kumar Agarwal, Chief Digital & Information Officer (CDIO), whose vision and stewardship are accelerating JK Tyre's evolution from a traditional IT-driven enterprise to a digitally empowered, AI-first, value-centric organization. In a conversation that spans culture, technology, sustainability, digital transformation, manufacturing modernization, cybersecurity, talent, and the future of AI, Sharad offers a rare and detailed look into how JK Tyre is building the digital enterprise of tomorrow.

From the outset, Sharad emphasizes that JK Tyre has always recognized the importance of technology. Long before digital transformation became a buzzword, the company implemented SAP and adopted modern systems when most Indian manufacturers were still evaluating their technology roadmaps. The IT function itself has gone through a remarkable evolution what began decades ago as a "Systems Department" later became EDP (Enterprise Data Processing), then MIS, then IT, and finally, in 2020, was renamed Digital & IT Solutions. This evolution in nomenclature is not cosmetic but a reflection of the expanding role IT plays in the organization. As Sharad explains, the function has transitioned from being a back-end service provider to a business enabler and now stands firmly as a strategic value driver, influencing some of the most critical decisions across the enterprise.

A major symbolic milestone of this evolution was the establishment of the Digital & AI Center of Excellence (DNA COE), inaugurated on 9th November 2024. This state-of-the-art facility, designed with a contemporary, minimalist approach, reflects global benchmarks not just in aesthetics but in collaboration philosophy. "We were clear that it should not be benchmarked against Indian peers," Sharad notes. "The goal was to create a workplace at par with the best in the world Google, Amazon, cutting-edge technology companies. And today, this center embodies that spirit." The DNA COE is not just a workplace it's a cultural statement about transparency, collaboration, freedom, empowerment, and innovation.

The scope of operations supported by the Digital & IT function at JK Tyre is massive. The ERP landscape alone supports between 2,500 and 3,000 internal users. The dealer ecosystem, enabled through the JK Connect portal, includes around 10,000 external partners. With nine plants in India, three plants in Mexico, and nearly 150 offices, CNFs, feeder godowns, and third-party logistics partners, the digital team supports nearly 200 unique locations across continents. In short, the technology organization enables the digital backbone that supports tens of thousands of users and mission-critical processes globally.

Yet, despite this scale, Sharad is clear about one thing: JK Tyre does not see its journey as "digital transformation" alone it sees it as business transformation. This distinction is important. Transformation, for JK Tyre, is not about chasing new technologies for their own sake but about enhancing stakeholder value across the board. Stakeholders include shareholders, management, employees, customers, vendors, and society at large aligning strongly with JK Tyre's sustainability commitments, ESG performance, and CSR initiatives.

Transformation at JK Tyre is happening function by function. The earliest focus was on sales, marketing, and customer experience, collectively referred to as SMCC. Product technology and manufacturing soon followed, especially because manufacturing holds immense untapped value both in efficiency gains and cost optimization. One of the most significant achievements was the organization's lightning-fast SAP RISE migration, completed in just 100 days, covering seven SAP products (including three completely new ones) and integrating 28 systems. For perspective, most partners expected this to take 6–12 months. Yet, JK Tyre's digital team, backed by strong business support, delivered it flawlessly demonstrating not only capability but organizational alignment and clarity of purpose.

Sharad explains that JK Tyre follows a rigorous, structured approach to identifying and prioritizing digital initiatives. Everything begins with a deep discovery process, where teams examine processes end-to-end. They challenge decades-old SOPs, evaluate relevance, remove redundancies, and discover new opportunities. They measure each use case on value metrics such as efficiency, effectiveness, revenue enhancement, cost reduction, morale improvement, and safety enhancement. Once use cases are sized and sequenced, they are taken through the investment approval process ensuring clear ROI and business ownership.

Ownership is a recurring theme in Sharad's thinking. "We are co-owners," he explains. "But if a business function is not excited about the change, nothing meaningful can happen. Every stakeholder must see what's in it for them." This is why change management is central to their model. Adoption is not assumed it is designed through engagement, communication, and a human-centered approach.

The DNA COE workplace reinforces this philosophy. It is designed around openness and non-hierarchy, with no fixed seating even for section heads and function heads. The office is completely wireless, paperless, and pin-less. Employees choose where they sit each day, and interactions happen naturally through shared spaces phone booths, amphitheaters, high tables, breakout zones. This environment encourages curiosity, dialogue, speed of decision-making, and cross-functional thinking.

Not everyone adjusts easily, Sharad admits. Employees accustomed to hierarchy, rigid

SHARAD KUMAR AGARWAL
CDIO, JK Tyre & Industries.

"Digital transformation is not an IT project it is a **business value movement. Technology succeeds only when it elevates people,** processes, and performance together."

structures, or "yes-boss culture" may initially find the environment challenging. But the shift is intentional JK Tyre is building a digital-first, Gen-Z-friendly culture where value matters more than titles or seating positions. Weekly knowledge-sharing sessions enable engineers from one domain to understand what others are doing, creating an ecosystem of learning and innovation.

At the core of JK Tyre's digital strategy lies data unification. The organization is building a unified enterprise data lake that will power its new "One JK One Dashboard" vision. Reporting will no longer be plant-specific or person-specific; dashboards will be standardized and automated, with manual entries digitized wherever needed. This unification is not just technical it is cultural, allowing JK Tyre to run operations with visibility, transparency, and data-driven decision-making.

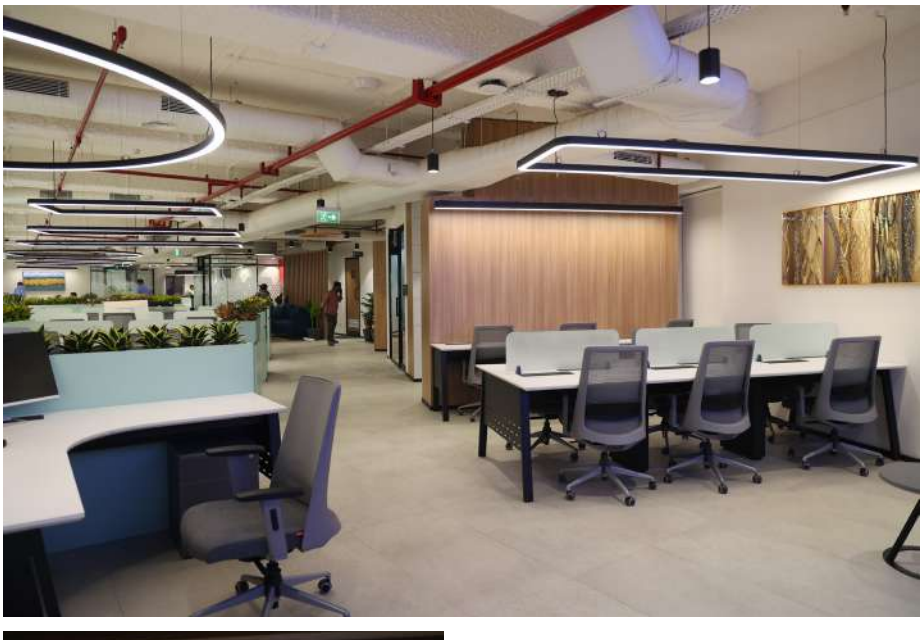
Manufacturing is undergoing a profound transformation driven by IoT, AI, automation, cloud, MES-ERP integration, and cyber-physical systems. Sharad describes these technologies as "different sides of the same cube." The manufacturing digitization roadmap aligns with the Purdue model starting from sensors and PLCs at level 0, moving through MES and ERP layers, and culminating in decision intelligence powered by AI.

Yet, Sharad is clear-eyed about AI's realities.

While the world sees AI as magical, Sharad understands that AI is the top of the pyramid requiring strong foundational layers such as infrastructure, connectivity, clean data, talent, and governance. AI is not a button to push but a capability to build. And the biggest enabler of success is not technology it is people. JK Tyre invests heavily in training, reskilling, and upskilling. Training is perhaps the single most important pillar of their digital manifesto. Shop floor employees, office staff, and leadership all undergo tailored learning programs.

One of the most impactful digital initiatives at JK Tyre is Project Infinity, a large-scale transformation of manufacturing. At one plant alone, over 600 to 1,000 new sensors were added, in addition to thousands already present. This created a completely connected factory, with all data flowing into the unified data lake. Over this foundation, JK Tyre has built digital twins of assets, inventory, processes, and quality. These digital twins are not schematic they are built using LiDAR with 3D visualization tools that allow employees to

> "A connected factory is not about machines talking to machines it is about the business finally hearing what the machines have been trying to say."



"walk through" the plant using 3D glasses. Project Infinity is improving uptime, enhancing quality, reducing downtime and accelerating decision cycles. The financial value measured in GVA (Gross Value Addition) is substantial and soon to be shared publicly.

JK Tyre's cyber-resilience strategy is equally forward-thinking. Sharad uses a powerful analogy from tyre design where grip, wet resistance, and rolling resistance must be balanced despite counteracting forces. Cybersecurity requires a similar approach. New threats emerge constantly, and while attackers need to succeed only once, defenders must succeed every time. JK Tyre has been ISMS-certified since 2015, a rare achievement for manufacturing organizations at the time. A dedicated CISO leads the effort with a single KPI: zero incidents. The organization continually evaluates new security technologies and ensures board-level visibility of its cybersecurity posture.

> "Technology can modernize a company, but culture transforms it. Our goal at JK Tyre is to build a workplace where openness, collaboration and curiosity are everyday behaviour."

As important as technology is, digital fluency remains a foundational pillar. JK Tyre invests heavily in training across personas shop floor operators, office staff, managers, engineers ensuring that every employee can use digital tools effectively. Every program includes refresher sessions, Q&A, and hands-on practice. In Sharad's words: "The only thing saving us is training, training, and training."

Sharad's view of the future is ambitious and forward-looking. He expects JK Tyre to emerge as one of the best manufacturing facilities in the world, not just in India or among tyre makers. The focus will remain on giving employees the best tools, platforms, and digital ecosystems. On the technology horizon, he sees Quantum Computing as the next breakthrough likely within five years and Artificial General Intelligence (AGI) as a real possibility within 8–10 years. Quantum computing, he believes, will help unlock AGI and redefine the speed and capabilities of enterprise decision-making.

In closing, Sharad reflects on the cultural fabric of JK Tyre: a family-like organization built on trust, openness, and collaboration. Technology is not seen as an outsider or separate function but as a partner. The digital team is not the "IT department" they are co-creators of value, often sitting shoulder-to-shoulder with manufacturing, sales, marketing, and product teams. It is this combination of technology excellence, people-first culture, leadership vision, and organizational alignment that positions JK Tyre as a trailblazer in digital manufacturing.

Finally...

What JK Tyre is building under Sharad's leadership is not merely a digital workplace or a modern IT stack but a future-ready enterprise, powered by data, AI, automation, transparency, and empowered people. It is a transformation rooted in thoughtfulness, rigor, and clarity of purpose. And it reflects the promise of what Indian manufacturing can achieve in the coming decade. EIT

PALO ALTO NETWORKS UNIT 42 WARNS OF AI-ACCELERATED ATTACKS IN GLOBAL INCIDENT RESPONSE REPORT 2026

Identity abuse, supply chain infiltration and AI-driven automation redefine the global cyber threat landscape

PHILIPPA COGSWELL
VICE PRESIDENT, UNIT 42 – ASIA PACIFIC & JAPAN, PALO ALTO NETWORKS

"Attackers are combining AI acceleration with identity-based access to move faster **and blend in better than ever before. What's most striking is that over 90% of breaches** stem from preventable weaknesses misconfigurations, inconsistent controls and excessive identity trust. Security is solvable. Organisations that consolidate visibility, enforce least privilege and automate response can dramatically reduce both the likelihood and impact of a breach."

TheCyber adversaries are evolving at a pace that now outstrips enterprise digital transformation, according to the newly released Unit 42® Global Incident Response Report 2026 from Palo Alto Networks®. The report reveals a striking shift toward AI-enabled attack automation, identity misuse, and supply chain exploitation trends that are reshaping how modern intrusions unfold across global organisations.

Based on more than 750 major incident response engagements across over 50 countries between October 2024 and September 2025, Unit 42's latest findings show that attackers are combining accelerated techniques with authenticated access to breach environments faster than ever before.

AI compresses attack timelines

One of the most alarming shifts is the rapid reduction in time-to-impact.

In 2025, the fastest 25% of intrusions reached data exfiltration within 72 minutes, a dramatic drop from 285 minutes in the previous year. Threat actors are increasingly using AI to automate reconnaissance, phishing, scripting, evasion and extortion enabling parallelised attacks at unprecedented scale.

Identity vulnerabilities, meanwhile, have become the softest target. Nearly 90% of all investigations involved identity-related weaknesses, confirming that in cloud-first ecosystems, identity has emerged as the primary attack surface.

Attacks now span the entire enterprise surface

Modern intrusions are no longer isolated events. According to the report:

- 87% of attacks spanned multiple surfaces — including endpoints, cloud, networks, SaaS and identity layers.
- 48% involved browser-based activity, cementing the browser as a major frontline in today's threat landscape.

Extortion evolves beyond encryption

Ransomware remains widespread but enter a new phase.

In 2025, encryption appeared in 78% of extortion incidents, a sharp decline from over 90% in previous years. Attackers are increasingly relying on:

- pure data theft
- exposure threats
- multi-vector extortion techniques

Median ransom demands surged from US$1.25 million in 2024 to US$1.5 million in 2025.

Key Findings from the Unit 42 Global Incident Response Report 2026

- AI as an attack force multiplier: Automates reconnaissance, phishing, scripting and extortion, massively reducing time-to-impact.
- Identity is the main entry point: 65% of intrusions leverage compromised credentials, MFA bypass or IAM misconfigurations.
- Software supply chain exposure widens: SaaS integrations, vendor management layers and open-source dependencies create inherited trust risks.
- Nation-states evolve tactics: Greater focus on infrastructure compromise, virtualisation layer

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

ASHOK SOOTA COUNTERS VINOD KHOSLA'S AI DOOMSDAY FORECASTS, CALLS FOR OPTIMISM, BALANCE, AND EVIDENCE-LED PERSPECTIVE

Industry veteran urges optimism and balance, asserts AI will strengthen IT services and healthcare rather than replace workers

Veteran technology leader Ashok Soota has issued a strong and measured rebuttal to the sweeping predictions made by Silicon Valley investor Vinod Khosla at the India AI Impact Summit 2026. Khosla had argued that IT services and BPO roles would "vanish within five years," further claiming that traditional IT outsourcing as an industry would cease to exist by 2030 a statement that triggered widespread debate across India's technology ecosystem.

Soota, one of the most respected figures in India's IT industry and the Founder & Chairman of Happiest Minds, Happiest Health, and the medical research trust SKAN, dismissed these predictions as overly simplistic and disconnected from real-world evidence. In his detailed response, he emphasised that every technological wave from mainframes to mobility, from cloud to automation has ultimately created far more opportunities than it displaced.

"AI is a catalyst for growth, not a replacement for humans. Technology expands opportunities; it does not eliminate them," Soota said, urging the industry to adopt a mindset rooted in optimism, pragmatism, and historical context.

AI Will Strengthen, Not Destroy, IT Services

Countering Khosla's claim that IT services will disappear, Soota pointed out that the sector is already leveraging AI to accelerate innovation, enhance productivity, and open new market avenues. Far from becoming irrelevant, global enterprises today depend even more on specialised service providers to integrate AI into core business processes, modernise legacy infrastructure, and build secure, scalable systems.

"IT services will remain essential for enterprises that need customised solutions, faster innovation cycles, and superior business outcomes," Soota said. "The industry is not dying; it is growing as the essential partner for enterprises navigating the disruptive AI age."

He argued that the IT workforce is not shrinking but evolving shifting toward AI engineering, data platforms, cybersecurity, cloud architecture, product-aligned delivery models, and responsible AI frameworks. AI is eliminating repetitive tasks, he said, not erasing the need for human expertise.

Healthcare Will Need More Human Expertise Not Less

Responding to Khosla's assertion that many expertise-driven professions, including doctors, could be overtaken by AI by 2050, Soota strongly disagreed, calling the prediction "misguided and overly reductionist."

Soota highlighted how AI is transforming healthcare globally not by replacing clinicians, but by giving them powerful diagnostic, research, and decision-support tools. "AI is augmenting diagnostics, speeding up data analysis and enabling personalised treatment planning but strong human oversight remains indispensable," he said.

He cited international studies from organisations such as the WHO, World Economic Forum, and KPMG, all of which emphasise that the highest-value healthcare outcomes emerge from human-AI collaboration, not substitution. AI models still struggle with contextual reasoning, empathy, complex ethics, and edge-case diagnosis all areas where clinicians remain irreplaceable.

A Call for Confidence in India's Tech Future

Soota warned that aggressive doomsday predictions risk undermining confidence in India's globally admired IT ecosystem a sector that contributes significantly to national GDP, exports, and employment.

He stressed that AI is expanding markets, enabling knowledge-intensive jobs, and reinforcing India's position as a global digital transformation powerhouse. The country's leadership in AI engineering, data science, cybersecurity, cloud operations, and full-stack development ensures that India is positioned not at the receiving end of disruption, but at the forefront of shaping it.

ASHOK SOOTA
FOUNDER & CHAIRMAN, HAPPIEST MINDS & HAPPIEST HEALTH

"AI is a catalyst for growth not a replacement for **humans. Technology expands opportunities; it** does not eliminate them."

"Far from disappearing, IT services are becoming the trusted bridge between cutting-edge AI and real-world enterprise needs," he said. ENT

AI YOU CAN TRUST: HOW DYNATRACE AND AWS ARE BUILDING THE NEXT ERA OF INTELLIGENT AND COMPLIANT CLOUD FOR INDIA

Enterprises in India are moving rapidly from AI experimentation to full-scale deployment, but the real transformation is happening beneath the surface, in observability, governance and cloud intelligence. This story explores how the Dynatrace–AWS partnership is powering that shift, helping organizations innovate at scale while ensuring trust, reliability, and compliance.

India's digital economy is stretching into a new phase one where AI is no longer an add-on to business strategy, but a defining layer of it. Banks are automating decision engines. Telecom operators are modernizing networks. Public sector institutions are pushing citizen services into cloud-native architectures. And IT services providers are integrating AI into global delivery models.

Yet the real test for AI adoption isn't in how quickly enterprises can deploy it, but in how confidently they can run it. AI systems are complex; they involve interconnected services, multi-agent architectures, high-volume data, and autonomous decision loops that require constant oversight. Without visibility, AI becomes a risk rather than a growth driver.

This is the backdrop in which the Dynatrace–AWS partnership has taken on strategic importance for India and the broader SAARC region. The collaboration blends Dynatrace's AI-powered observability with AWS's scalable, resilient, and locally hosted cloud infrastructure, enabling organizations to innovate fast but with guardrails.

ARUN BALASUBRAMANIAN
Managing Director, India & SAARC, Dynatrace

"AI will only create meaningful business value when it is observable, governable, and **aligned with outcomes. Our partnership with AWS gives enterprises across India and the SAARC region** the foundation to scale AI securely, compliantly, and confidently."

A Partnership Built Around India's Digital Priorities

One of the most strategic aspects of the alliance is that the Dynatrace platform is hosted in the AWS Mumbai region. For Indian enterprises navigating the Digital Personal Data Protection (DPDP) Act and sectoral regulations, data residency and sovereignty are non-negotiable. The ability to use an enterprise-grade observability platform without data leaving national borders removes a significant barrier to cloud and AI modernization. But the advantage extends beyond location. Deep cloud-native integrations on AWS allow Dynatrace to provide visibility across highly distributed systems—containers, microservices, serverless environments, and modern AI workloads. In sectors like BFSI and telecom, where even milliseconds of latency or blind spots in monitoring can affect millions of users, this level of clarity is critical. As Balasubramanian puts it, the priority for Indian enterprises is clear: "Move fast, but with confidence."

Crossing USD 1 Billion: A Marketplace Milestone with Meaning

Dynatrace recently crossed USD 1 billion in lifetime sales on AWS Marketplace, a milestone that reflects both customer trust and a shift in how enterprises purchase technology.

Marketplace procurement has simplified what was once a drawn-out, compliance-heavy process. It brings software onboarding, billing, governance, and AWS credits under one integrated mechanism. For Indian organizations, especially those with strict procurement frameworks, this streamlining translates to faster decision-making and quicker deployment.

In markets like India where performance, compliance, and operational resilience are prerequisites this level of traction signals that enterprises see Dynatrace as a scalable, mature, and deeply integrated solution for cloud transformation.

INR Billing: Removing Friction from

Procurement

One of the most practical but transformative steps for Indian enterprises has been the introduction of INR billing for Dynatrace on AWS Marketplace. This change eliminates long-standing hurdles:

- No more foreign exchange complications
- Simpler GST compliance
- Faster approvals from finance and procurement teams
- Alignment of observability spending with AWS cloud commitments

It also supports the broader push for data residency and local cloud operations, since procurement, billing, and deployment can now happen fully within India's regulatory environment.

What used to take months can now begin within days a critical advantage in sectors racing to modernize.

Agentic AI Has Arrived and So Have the Governance Challenges

Around the world, nearly half of agentic AI projects have entered some form of limited production. Indian enterprises are experiencing the same surge, but with it come new challenges:

- How do you track decisions made by autonomous AI agents?
- What happens when model behavior drifts?
- How do you maintain DPDP compliance when AI executes complex, multi-step workflows?
- Can you audit an AI's decision trail the same way you audit a human process?

Without deep observability, these questions become unanswerable.

Dynatrace's platform provides the ability to trace decisions, detect anomalies, and establish auditable records across multi-agent systems a capability that Indian enterprises increasingly see as foundational for safe AI deployment.

Beyond Monitoring: The Era of Causal, Intelligent Observability

The cloud environments that India's large enterprises operate today are too dynamic for traditional monitoring tools. Dynatrace's approachbuilt on AI, automation, and causal intelligence goes a step beyond.

The platform automatically maps dependencies across thousands of services, correlating telemetry data and pinpointing root causes instead of generating scattered alerts. It connects performance issues to business impact, giving stakeholders from SREs to CIOs a unified view of system health.

This is particularly important for the public sector. Government departments and public institutions need predictable, reliable digital services delivered within a tightly governed ecosystem. With Dynatrace operating seamlessly on AWS, these organizations gain clarity into performance, security, and compliance in real time.

Real Transformations in BFSI and IT Services

India's BFSI sector, one of the most highly regulated and sensitive to service disruptions, has become an early beneficiary of the Dynatrace–AWS collaboration. Banks and insurers rely on observability to:

- Detect and resolve issues before they affect customer transactions
- Maintain compliance with regulatory bodies
- Manage peak traffic loads during seasonal events
- Protect digital experiences in high-volume environments

Similarly, India's IT services industry supporting global clients across continents uses Dynatrace to maintain availability across complex hybrid systems, meet SLAs, and speed up root-cause investigation.

Across both sectors, the trend is consistent: early detection, faster resolution, and higher resilience.

Making Autonomous AI Safer Through Observability

As organizations adopt autonomous AI systems, the risks expand as well. Observability for agentic AI provides:

- Real-time insights into decision-making
- Drift detection with immediate intervention
- Detailed audit trails to meet compliance standards
- Impact assessments for risk mitigation

Enterprises gain control not just over incidents, but over the long-term governance of AI ecosystems.

Cloud Spend Optimisation: Visibility as a Financial Strategy

With cloud usage expanding across every sector, cost management has become a boardroom topic. Dynatrace helps organizations:

- Identify cloud waste
- Optimize compute and storage usage
- Align consumption with AWS discount programs
- Prioritize investments in high-value workloads

In high-growth markets like India, where scaling is constant, this transparency becomes a competitive advantage.

Post re:Invent 2025: What's Resonating in India

Following AWS re:Invent 2025, several AI-centric capabilities gained strong traction among Indian enterprises:

- Enhanced visibility for AI agents and Amazon Bedrock
- Developer productivity tools that reduce manual work
- Operational guardrails for large-scale AI deployments

Early adopters in cybersecurity, telecom, and IT services report faster AI rollouts and improved compliance readiness.

The shift is unmistakable: India is moving from AI experimentation to disciplined, large-scale adoption.

The Next Two Years: Observability as the Backbone of Digital India

In the coming 24 months, observability-led transformation in India will be driven by three priorities:

- Resilience, especially as AI workloads expand
- Governance, supported by clearer regulations and stronger AI controls
- Cost management, driven by expanding cloud footprints and sharper budgets

With local cloud regions and maturing digital ecosystems, India is poised for sustained leadership in cloud and AI innovation.

Recognition That Reinforces Purpose

Dynatrace's recognition as the 2025 AWS Public Sector Technology Partner of the Year for LATAM reflects a broader global trajectory. The company's AI-driven observability platform has become vital to governments, education institutions, and nonprofits modernizing secure cloud environments.

It also validates the strength of the Dynatrace–AWS partnership a collaboration advancing scalable, secure, and reliable services for mission-critical public sector workloads worldwide.

Looking Ahead: Scaling Innovation with Trust

For Dynatrace, the recognition becomes fuel for the next phase. The company will continue strengthening its AI-driven observability capabilities, deepen its collaboration with AWS, and expand accessible procurement models across high-growth markets. The goal is clear: empower organizations to innovate boldly without sacrificing trust, security, or performance.

As India accelerates into an AI-powered future, the winners will be those who can understand their systems deeply, govern them confidently, and scale them responsibly. With Dynatrace and AWS working in tandem, that future is becoming not just possible but predictable. ENT

HEALTHCARE'S HIDDEN CRISIS: REGULATED DATA AT THE HEART OF CLOUD AND GENAI POLICY VIOLATIONS

New research from Netskope Threat Labs reveals that healthcare organisations are facing a widening security gap as staff rapidly embrace cloud services and generative AI tools. With regulated patient data making up nearly all AI-related policy violations, the sector must now balance innovation with strict oversight to prevent large-scale breaches and compliance failures.

BY SANJAY@ACCENTINFOMEDIA.COM

Healthcare is undergoing a profound digital shift. Electronic health records are now standard, remote consultations continue to grow, and hospitals increasingly rely on intelligent systems to streamline diagnostics and administrative workloads. But as the sector modernises, a quieter, more insidious threat is emerging: the rapid, often unmonitored adoption of cloud services and generative AI (genAI) tools.

The latest annual healthcare threat report from Netskope Threat Labs shines a bright light on this evolving landscape. Based on thirteen months of analysis, the findings reveal that regulated healthcare data patient records, clinical histories, diagnostic scans, claims information now accounts for the vast majority of cloud and genAI-related data policy violations inside healthcare settings.

This is not a marginal trend but a structural shift with far-reaching implications for security leaders, regulators, and healthcare organisations trying to bridge the gap between innovation and compliance.

GenAI Becomes a New Source of Risk as Staff Adoption Surges

The advent of genAI tools has been transformative for many frontline healthcare workers. Doctors use them to summarise clinical notes, nurses rely on them to generate documentation, and administrative staff use AI for scheduling and correspondence. But this adoption comes with a significant, under-recognised risk: the potential for accidental leakage of sensitive patient information.

According to the report, 89% of all data policy violations tied to genAI use in healthcare involve regulated data, a figure nearly triple the cross-industry average of 31%. The sensitivity of clinical data means the consequences of missteps are far greater than in most other sectors.

The problem is not the technology itself, but how it is being used. Employees often paste patient details into AI prompts, upload medical documents for summarisation, or use AI chatbots to assist with workflow tasks all actions that can expose confidential information to platforms outside the organisation's control.

Personal GenAI Accounts: A Hidden Exposure Pathway

A significant portion of the risk stems from staff using personal genAI accounts on unmanaged devices and networks. Although there has been a sharp decline over the past year, 43% of healthcare workers still rely on personal genAI tools at work. Security teams cannot monitor or restrict what data flows into these platforms, creating an invisible channel for sensitive information to leak.

To counter this, healthcare organisations have accelerated efforts to deploy company-approved AI applications. Over the same thirteen-month period, usage of managed genAI tools increased dramatically from 18% to 67% a rate of adoption that outpaced all other industries.

This shift reflects both the urgency and the scale of the challenge. Organisations recognise that banning genAI outright is unrealistic; instead, they must provide secure, approved alternatives that meet staff needs without compromising patient confidentiality.

Internal AI Deployments Introduce New Governance Challenges

While employees increasingly use approved genAI tools, organisations themselves are also building internal AI applications tailored to clinical workflows. These range from decision-support models and analytics engines to administrative AI agents. But internal deployment does not eliminate risk.

Most internal AI tools still rely on cloud-based large language models (LLMs) accessed through APIs. These API integrations create additional visibility and security requirements, especially when patient data interacts with external model endpoints.

According to Netskope, nearly two-thirds of healthcare organisations observed API traffic connecting to OpenAI (63%) and AssemblyAI (62%), and over a third (36%) detected traffic to Anthropic. This trend signals a growing reliance on embedded AI capabilities inside clinical and operational systems.

Such integrations bring tremendous value, but they also expand the attack surface. Without strong security controls around API connections, organisations risk exposing regulated data or enabling unauthorised access to critical systems.

Personal Cloud Apps: Convenience at the Cost of Compliance

Beyond genAI, healthcare employees continue to rely on personal cloud platforms Google Drive, Gmail, OneDrive to save or transfer work files. The report notes that regulated healthcare data once again dominates this category, making up 82% of all data policy violations associated with personal cloud usage.

Even seemingly innocent actions, like emailing a document to oneself to work from home, can lead to serious exposure of patient information.

Healthcare organisations have responded with stronger enforcement policies. Over half (56%) of those using preventive controls blocked uploads to personal Google Drive accounts, followed closely by Gmail (39%) and OneDrive (30%). These numbers illustrate the frequency and severity of attempted data movement to personal environments.

Attackers Exploit Trust in Cloud

RAY CANZANESE
Director, Netskope Threat Labs

"Healthcare sits at the intersection of strict regulation **and rapid digital transformation. Without guardrails for cloud and AI** usage, organisations risk exposing sensitive patient data at unprecedented scale."

Ecosystems

While internal risks are rising, external threats have not diminished. Attackers increasingly weaponise trusted cloud platforms to distribute malware because employees are more likely to download files from familiar services. Netskope's analysis shows that in healthcare:

- Azure Static Web Apps were used in malware distribution attempts for 8.2% of organisations.
- GitHub accounted for 8% of such incidents.
- Microsoft OneDrive saw 6.3% of employees attempt to download malicious content.

These services are not malicious themselves, but their credibility makes them attractive distribution channels for cybercriminals looking to bypass filtering and exploit human trust.

In healthcare where operational disruptions can delay treatments or jeopardise patient outcomes the stakes are particularly high.

Internal Risk Is Now as Critical as External Threats

Ray Canzanese, Director of Netskope Threat Labs, emphasises that the security landscape in healthcare is shifting. Historically, organisations focused on defending against ransomware, phishing, and external intrusions. Today, however, internal data exposure driven by cloud adoption and AI usage poses equally urgent risks.

"Healthcare has always been a prime target for attackers," Canzanese notes. "But without policies governing cloud and AI, organisations face another looming threat: accidental or unmanaged data exposure from within."

He warns that organisations lacking proper guardrails are "very likely" to suffer leaks of regulated patient and clinical data, exposing them to costly remediation efforts, reputational harm, and potentially large regulatory penalties.

Balancing Innovation and Security: The Way Forward

Healthcare's digital evolution is not slowing down. Hospitals are incorporating AI assistants, predictive analytics, automated documentation, and more sophisticated cloud-based systems. At the same time, workforce pressures from staff shortages to rising administrative workloads make AI adoption almost inevitable.

But to adopt AI safely, healthcare organisations must establish strong governance frameworks. These include:

- Company-approved genAI tools with strict data handling policies
- Automated, real-time guidance to prevent risky uploads
- Controls to block personal cloud usage
- Monitoring of AI-related API traffic
- Full visibility into data flows across internal and external systems

The goal is not to restrict innovation, but to ensure that modernisation does not come at the cost of patient privacy.

A Sector at a Crossroads

The findings from Netskope Threat Labs paint a picture of a sector undergoing rapid transformation while grappling with unprecedented security challenges. Healthcare organisations now face a dual responsibility: harness the power of AI and cloud platforms, while protecting some of the most sensitive data that exists.

The path ahead requires investment not just in technology, but in training, governance, and culture. As AI becomes embedded in clinical and operational workflows, the healthcare sector must build the safeguards necessary to protect patients and maintain trust. The message from the report is unmistakable: innovation without oversight is risky, but innovation with strong guardrails can reshape healthcare for the better. ENT

THE ART AND SCIENCE OF CLOUD MIGRATION

A disciplined approach to cloud migration is the difference between cost overruns and long-term strategic value. This framework brings clarity, structure, and financial rigor to every stage of the journey.

The Art and Science of Cloud Migration

Why Strategic Discipline — Not Enthusiasm — Determines Success

Cloud migration has moved from experimentation to expectation.

Boards ask about it. Investors assume it. Vendors accelerate it. Stakeholders experience it.

Yet despite its ubiquity, cloud transformation remains one of the most misunderstood executive decisions in modern enterprise technology.

The industry narrative suggests inevitability. The financial reality demands discipline.

Cloud migration is not an infrastructure refresh. It is a strategic reallocation of capital, risk, and operational responsibility. Organizations that approach it as a technical relocation project frequently overspend, underdeliver, and in some cases, reverse course. Those that treat it as a structured transformation journey create durable advantage.

True cloud mastery requires both art and science: strategic judgment balanced by financial modeling, architectural rigor reinforced by governance discipline.

The journey unfolds across seven distinct but interdependent stages.

1. The Go / No-Go Decision: Timing Is Strategy

The first decision is not "Which cloud?" It is "Should we move — now?"

Cloud adoption must begin with an honest assessment of the existing environment.

Questions like below should form the foundation of the assessment:

- When was the infrastructure last refreshed?
- What is the remaining lifecycle of core hardware?
- What are the warranty and maintenance commitments?
- What capital investments are still being depreciated?

Migrating recently refreshed infrastructure will erode capital efficiency. Conversely, infrastructure approaching end-of-life presents a natural inflection point.

Equally critical is the software landscape. Licensing complexity is frequently the hidden driver of cloud economics. Perpetual agreements, subscription models, enterprise contracts, and portability rights must be mapped precisely.

Technology stacks — whether Microsoft-centric or Oracle-dependent — materially influence cost structures in cloud environments.

Financial modeling must move beyond optimistic cost comparisons. A credible analysis includes:

- Total Cost of Ownership (TCO) considering the lifespan of the existing hardware
- Breakeven timeline
- Net Present Value (NPV)
- Internal Rate of Return (IRR)
- Opportunity cost of delayed innovation

Cloud does not automatically reduce cost. It converts fixed capital expenditure into variable operational expenditure. That shift alters financial behaviour, accountability, and risk exposure.

The disciplined organization asks not whether cloud is modern — but whether it creates measurable business value at this moment.

The next step depends only on this answer.

2. Data-Driven Cloud Selection: Alignment Over Popularity

Once migration is justified, provider selection must be analytical, not aspirational.

The public hyperscale market is led by:

- Amazon Web Services (AWS)
- Microsoft Azure (Azure)
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)

Each platform brings its own architectural strengths, pricing nuances, and ecosystem advantages. The right choice depends on workload alignment.

Microsoft-centric environments often benefit from Azure's integration model. Oracle-heavy estates may find economic alignment with OCI. Data Science or Kubernetes-intensive organizations may leverage GCP's container heritage. Diversified enterprises frequently adopt AWS for breadth and maturity.

Region selection is equally strategic. Compute pricing, data transfer charges, regulatory boundaries, and latency considerations vary across geographies. Production region decisions must be made alongside disaster recovery design — active-active, active-passive, pilot light, or warm standby.

Provider selection defines cost trajectory, compliance posture, resilience strategy, and long-term flexibility. It should withstand board-level scrutiny.

3. Migration Architecture: Execution

Cloud migration is a board-level priority — However, some enterprises approach it as a technical upgrade rather than a strategic capital decision. The result is predictable: Cost overruns, Architectural sprawl, and thereby causing workload repatriation.

The Art and Science of Cloud Migration try to make the journey as a structured transformation across seven disciplined stages — from the initial Go/No-Go evaluation to multi-cloud maturity.

It emphasizes financial modeling before migration, workload-aligned provider selection, architecture-first execution, selective modernization, continuous optimization, and rigorous FinOps governance.

Cloud does not automatically reduce cost. It converts fixed capital investment into variable operational exposure. Without executive oversight and financial discipline, flexibility becomes volatility.

Organizations that balance strategic judgment with technical precision do not simply migrate workloads — they build sustainable cloud economics and competitive agility.

The destination of the cloud journey is the mastery to manage it effectively.

VENKATA SUDHAKAR NAGANDLA
SENIOR VICE PRESIDENT & GLOBAL HEAD – IT INFRASTRUCTURE & CLOUD | TRANSFORMATION LEADERSHIP.

"Cloud migration is not a technical milestone it is a strategic financial decision. Discipline, not **enthusiasm, is what ultimately determines whether** the cloud becomes an asset or an exposure."

Determines Credibility

Migration is not replication. It is orchestration.

Execution requires clarity on two fronts: the source environment and the destination architecture.

On the source side, organizations must map interdependencies with precision:

- Application relationships
- Database integrations
- Infrastructure topology
- Data flow patterns

Workloads should be grouped into migration waves (interdependent buckets) based on criticality, complexity, and downtime tolerance. Incremental replication — rather than a "big bang" cutover — mitigates risk. Change Data Capture, staged synchronization, and rehearsal cutovers transform migration from disruption to managed transition.

On the destination side, a structured landing zone is non-negotiable. Identity frameworks, network segmentation, security baselines, logging, monitoring, and governance guardrails must precede workload migration.

Backup and recovery architecture along with disaster recovery requirements must be deliberated, leveraging cloud-native tools or enterprise-grade solutions such as:

- Commvault
- Rubrik
- Cohesity
- Veeam

Migration without architectural discipline results in cost sprawl and operational fragility.

4. Application Modernization: Relocation Is Not Transformation

Lift-and-shift delivers relocation. It does not unlock value.

Once workloads stabilize, modernization becomes the differentiator.

Based on the overall application landscape, organizations can evaluate transitions from commercial stacks to open-source alternatives, if financially and operationally viable. Shifting from proprietary operating systems and databases to open ecosystems can reduce licensing exposure and improve portability. However, it comes with challenges such as enterprise-level support maturity and advanced feature capabilities.

Containerization and microservices architecture introduce elasticity, deployment velocity, and platform independence. However, modernization must be pragmatic. Not every application warrants refactoring. Selectivity preserves capital and reduces risk.

Modernization is not ideology. It is strategic optimization.

5. Transformation and Optimization: The Continuous Imperative

Cloud environments do not optimize themselves.

Post-migration, organizations must aggressively pursue consolidation and efficiency.

License rationalization, Bring Your Own License strategies, and commitment models reduce consumption costs. Transitioning from Infrastructure-as-a-Service to managed Platform-as-a-Service offerings lowers operational overhead and enhances resilience.

Rightsizing workloads, eliminating idle resources, automating infrastructure provisioning, and enforcing governance policies create sustainable efficiency.

Optimization is not a milestone. It is an operating discipline.

6. FinOps: Governing the OPEX Reality

Many cloud failures are financial, not technical.

Traditional data centers operate under CAPEX logic. Once infrastructure is purchased, incremental overuse has limited immediate financial impact.

Cloud operates under OPEX logic. Every compute cycle, storage allocation, and data transfer is billable.

Without financial governance, variable cost becomes uncontrolled expenditure — like an open tap.

Adopting principles aligned with the FinOps Foundation introduces accountability through:

- Budget forecasting aligned with business demand
- Showback and chargeback transparency
- Commitment and savings models
- Anomaly detection
- Tagging and policy discipline

FinOps is not cost-cutting. It is financial maturity in a consumption-based world.

Organizations that neglect this discipline often reconsider cloud commitments. Those that embrace it build sustainable economics.

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

THE FUTURE OF SOC IS AUTONOMOUS, OPEN, AND DRIVEN BY BEHAVIORAL INTELLIGENCE.

In this exclusive conversation, Zubair Chowgale, Sales Engineering Manager for APMEA at Securonix, discusses how the company is transforming modern security operations through cloud-native scalability, agentic AI and an open approach to SIEM architecture.

How does Securonix's SIEM architecture differ from traditional SIEM platforms in terms of scalability, analytics, and data handling?

Legacy SIEM platforms were built for a different era. Their proprietary, database-centric architecture struggles to handle the scale, speed, and diversity of data generated by modern enterprises. As data volumes grow, these limitations lead to performance constraints, rising costs, and vendor lock-in, effectively restricting how organizations access and use their own security data.

Securonix Unified Defense SIEM is designed for the realities of today's SOC. Built on an open architecture and powered by agentic AI, it is engineered to scale with each customer's environment and threat landscape. Open by design and supported by extensible APIs, the platform integrates seamlessly across SIEM, SOAR, XDR, EDR, cloud, and on-premises ecosystems without forcing rip-and-replace decisions.

The platform is natively powered by Snowflake and AWS, delivering elastic scale, resilience, and performance. Its big data analytics and long-term retention capabilities enable organizations to ingest and analyze massive volumes of telemetry in real time while maintaining cost-efficient, long-term storage. By using an open data model, Securonix ensures data portability and long-term flexibility, giving customers full control over their security data as their needs evolve.

What specific UEBA (User & Entity Behavior Analytics) capabilities set Securonix apart from other SIEM/XDR vendors?

As cyberattacks grow more sophisticated, traditional rule-based security approaches are increasingly ineffective. They struggle to detect advanced threats and generate large volumes of false alerts that slow investigations and overwhelm security teams.

Securonix UEBA addresses this challenge by continuously analyzing user and entity behavior to identify anomalies, suspicious lateral movement, and insider threats across both cloud and on-premises environments. Built-in integrations and APIs provide visibility across major cloud platforms as well as critical security and business applications.

By applying machine learning and proven, out-of-the-box use cases, UEBA reduces noise and surfaces the highest-risk activity, allowing analysts to focus on what matters most. As part of the industry's first Unified Defense SIEM powered by agentic AI, Securonix helps organizations reduce mean time to respond, stop threats faster, and deliver measurable security outcomes that stand up at the board level.

How does Securonix integrate with existing security stacks EDR, IAM, cloud platforms (AWS/Azure/GCP), threat intel feeds and what native integrations are strongest?

Securonix is designed to work with existing security ecosystems rather than replace them. The platform uses an open architecture and extensible APIs to integrate across EDR, IAM, cloud, and threat intelligence sources, allowing organizations to preserve prior investments while improving visibility and response.

At the endpoint and identity layers, Securonix integrates with leading EDR and IAM platforms to ingest telemetry such as authentication activity, privilege changes, endpoint behavior, and access patterns. This data is enriched and correlated through behavioral analytics to detect insider threats, compromised credentials, and lateral movement that point solutions often miss in isolation.

For cloud environments, Securonix provides deep, native integrations with AWS, Azure, and Google Cloud. These integrations collect identity, audit, network, and workload telemetry to deliver unified visibility across hybrid and multi-cloud environments. Cloud activity is analyzed alongside on-premises data to establish consistent behavioral baselines and detect anomalous access or data movement.

Securonix also integrates with a broad range of commercial and open-source threat intelligence feeds. Threat indicators are contextualized within user, entity, and activity data, improving detection fidelity and reducing false positives. Native integrations are strongest in areas where behavioral context matters most, including identity and access data, cloud audit logs, and endpoint activity. This allows security teams to move beyond isolated alerts and gain a more complete, risk-based view of threats across the enterprise.

ZUBAIR CHOWGALE

SALES ENGINEERING MANAGER, APMEA, SECURONIX.

"The future of the SOC **isn't more alerts it's** autonomous clarity."

What is your approach to AI/ML-driven detection? How do you reduce false positives while maintaining high detection fidelity?

AI and machine learning give SOC teams a critical advantage in today's high-pressure threat landscape. At Securonix, AI is designed to augment analysts by handling the operational workload that slows detection and response, allowing teams to focus on real risk.

The Securonix Unified Defense SIEM continuously analyzes data streams to identify anomalies and suspicious activity that traditional, rule-based controls often miss. By converting raw telemetry into contextualized insights in real time, the platform significantly reduces false positives and analyst fatigue. Alerts are enriched with identity, asset, network, and activity context, giving security teams a clearer and more complete view of risk without manual correlation.

Securonix threat chains connect related activity over time, linking indicators of compromise with attacker tactics, techniques, and procedures to uncover patterns associated with advanced and insider threats. This behavioral analytics approach prioritizes high-fidelity alerts, reduces noise at scale, and enables faster, more confident response. In practice, customers reduce false positives by up to 90 percent and lower SIEM operating costs by more than 50 percent, allowing security teams to operate more efficiently and effectively.

How do you support hybrid and multi-cloud environments, and what visibility do you provide across cloud identities, data access, and workloads?

Securonix supports hybrid and multi-cloud environments through a cloud-native, SaaS-based SIEM platform built on AWS and Snowflake. It delivers unified security monitoring, behavioral analytics, and automated response across cloud and on-premises environments, providing a consistent view of risk regardless of where data or workloads reside.

As organizations accelerate cloud adoption, many struggle to balance agility with security. Gaps in visibility, unclear ownership of assets, data privacy concerns, and inconsistent access controls often introduce risk that traditional tools were not designed to address. These challenges are amplified in hybrid and multi-cloud environments where data and activity are fragmented across platforms.

Securonix addresses these limitations through deep, two-way integrations with cloud infrastructure and applications. Using API-based connectivity, the platform ingests and correlates identity, activity, and configuration data from AWS, Azure, Google Cloud, and on-premises systems to eliminate blind spots and improve detection accuracy. With more than 350 built-in cloud connectors, Securonix simplifies data collection and response, enabling security teams to monitor cloud activity continuously, detect abnormal behavior, and respond quickly with confidence.

What does the Securonix Marketplace offer today? Which pre-built content packs are most valuable for SOC teams?

The Securonix Marketplace extends the value of the platform by providing ready-to-use integrations, detections, and response content that help SOC teams move faster without custom development. It is designed to simplify onboarding of new data sources, accelerate detection coverage, and reduce the operational effort required to maintain security content over time.

Today, the Marketplace offers a broad range of pre-built content, including connectors, parsers, detection use cases, enrichment logic, dashboards, and response workflows. This allows teams to quickly integrate security, cloud, identity, and business applications while ensuring telemetry is normalized and immediately usable for analytics and investigation.

The most valuable content packs for SOC teams tend to focus on areas of highest operational impact. Identity and access monitoring packs are widely adopted because they improve visibility into authentication activity, privilege misuse, and insider risk. Cloud and SaaS content packs for platforms such as AWS, Azure, and Google Cloud help teams monitor user behavior, configuration changes, and data access across hybrid environments. Endpoint and network-focused packs add behavioral context that strengthens detection of lateral movement and advanced threats.

Threat intelligence enrichment and automated response content are also highly valued, as they help reduce noise and speed investigation by providing context and guided actions directly within the analyst workflow. Together, these pre-built packs allow SOC teams to expand coverage quickly, improve detection quality, and focus more time on responding to meaningful risk rather than building and maintaining content from scratch.

How does Securonix handle long-term log retention and analytics without increasing storage or compute costs excessively?

Securonix is designed to support long-term log retention and analytics without forcing organizations to trade cost for visibility. The platform uses a cloud-native architecture that separates storage and compute, allowing each to scale independently based on operational needs rather than peak demand.

Built on Snowflake and AWS, Securonix enables organizations to retain large volumes of security telemetry while maintaining efficient performance. Data can be stored in an optimized, open format and accessed on demand, allowing teams to run advanced analytics and investigations without keeping all data in high-cost, always-on compute tiers.

Through Data Pipeline Manager, customers have fine-grained control over how telemetry is ingested, processed, and stored. This includes deciding which data requires real-time analysis, which data can be retained for compliance or forensics, and where it should live across hot and long-term storage tiers. This flexibility helps reduce unnecessary ingestion, storage, and processing costs while preserving analytic depth.

As a result, security teams can maintain extended retention periods for compliance and investigation, perform historical analysis when needed, and control costs as data volumes grow. The outcome is predictable spend, scalable analytics, and long-term visibility without excessive storage or compute overhead.

What is your roadmap around autonomous SOC capabilities, AI-driven investigation, automatic enrichment, correlation, and SOAR integrations?

We don't typically comment on detailed product roadmap timelines, but we can share the direction we're moving in and the principles guiding our innovation.

Our focus is on advancing autonomous SOC capabilities in a way that delivers real operational value while keeping humans in control. This includes deeper AI-driven investigation, more intelligent automatic enrichment, stronger correlation across identities, assets, and activity, and tighter integration between detection and response through SOAR. The goal is to reduce manual effort, accelerate decision-making, and improve consistency across security operations.

We have several exciting new capabilities in the works that build on these foundations. These enhancements are designed to further streamline investigations, improve detection fidelity, and automate routine response actions without introducing risk or loss of oversight. As always, autonomy is being applied deliberately, with transparency and explainability at the core, so security teams can move faster with confidence

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

THE MOTHER OF ALL DEALS: HOW THE INDIA–EU FTA COULD SHAPE INDIA'S DATA, DIGITAL POWER AND GLOBAL TECH AMBITIONS

Beyond tariffs and trade, the landmark India–EU FTA is emerging as a strategic pact on data flows, digital infrastructure, and trust one that could redefine India's technology diplomacy

In the rapidly evolving landscape of digital finance, three major financial institutions have emerged with fundamentally different approaches to asset tokenization. BlackRock's BUIDL, Goldman Sachs' GS DAP, and J.P. Morgan's Kinexys represent divergent strategic visions for the future of on-chain finance, each targeting distinct segments of the institutional market with purpose-built infrastructure.

While all three initiatives share the common goal of modernizing financial markets through blockchain technology, their architectures, asset classes, and strategic objectives reveal sharply different philosophies about how tokenization will reshape the industry.

Three Platforms, Three Philosophies

BlackRock's BUIDL (USD Institutional Digital Liquidity Fund) has taken the bold step of launching on Ethereum's public blockchain, positioning itself as a tokenized money market fund that provides investors with daily dividend accruals in USD. Launched in partnership with Securitize Markets, BUIDL focuses on tokenized U.S. Treasuries, offering institutional investors on-chain yield with enhanced liquidity and transparency. The platform represents BlackRock's bet that public blockchains can deliver both the transparency and the institutional-grade reliability that traditional investors demand.

Goldman Sachs has charted a different course with its Digital Asset Platform (GS DAP), building on Digital Asset's Canton Network, a permissioned distributed ledger technology. Rather than creating a single product, Goldman has constructed a comprehensive institutional infrastructure designed for issuing, registering, and settling digital assets including securities and bonds. The platform's collaboration with BNY on tokenized money market fund settlement demonstrates its focus on accelerating settlement times and reducing operational costs across the institutional ecosystem.

J.P. Morgan's Kinexys (formerly Onyx Digital Assets) has prioritized speed and scale, developing a private, permissioned blockchain system optimized for instant payment settlements and tokenized collateral management. With over $1.5 trillion in tokenized transactions processed by mid-2025, Kinexys has achieved remarkable adoption through its flagship products: JPM Coin for payment rails and the Tokenized Collateral Network (TCN). The platform's 24/7 programmable payments and instant settlement of intraday repos address critical pain points in institutional treasury management.

Strategic Positioning and Market Focus

The strategic differentiation among these platforms becomes clearer when examining their primary use cases and target markets.

BUIDL operates as a product in the truest sense: a tokenized investment vehicle designed to deliver yield to on-chain investors. By anchoring its offering in U.S. Treasuries and providing daily accruals, BlackRock has created a cash-equivalent token that bridges traditional finance and decentralized finance. The choice of Ethereum as the underlying blockchain signals confidence in public infrastructure and positions BUIDL to integrate with the broader DeFi ecosystem.

GS DAP functions as a platform, providing

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

OWNING THE PROMISE: HOW MANAGEENGINE IS BUILDING A SOVEREIGN CLOUD FUTURE IN THE UAE

In a world that rents convenience, a software company chooses to build trust one data center, one policy, one principled decision at a time.

The room is barely settled when Rajesh Ganesan leans into an answer that explains a very unusual move: a software company ManageEngine has invested in building its own data center in the UAE.

Most firms in his position would choose the convenient path. They'd sign with AWS, Azure, or Google Cloud, deploy their SaaS in-region, and move on. Instead, Rajesh is quietly defiant.

"We don't see it as inviting trouble," he says. "We're a technology company. If we deliver cloud software, we should know how to build and manage the cloud infrastructure."

The sentence is simple. The implications are not. For ManageEngine, whose products power IT operations across enterprises enterprise service management, endpoint management, identity and access management, and more this is a principled stand: the delivery mechanism must reflect the promise the company makes to customers. And the promise is clear: your data is yours; your trust is ours to earn.

The Long Road—By Design

The story begins long before the UAE data center. Back in 2003, when SaaS was still emerging, ManageEngine made a decision: it would not grow by "reselling" hyperscale infrastructure.

"If you're a startup today, it's easy," Rajesh says. "You rent compute and storage from AWS or Azure, build on top, and ship. But then what are you? A software trader reselling someone else's cloud?"

ManageEngine chose a different identity. It embraced the long road:

- Own the stack: from custom hardware selection to custom operating system choices and custom database layers.
- Orchestrate with its own software: run and manage the platform using ManageEngine's own tools, so real-world learnings feed directly back into product design.
- Stand behind the promise: ensure the company can honor its privacy and data commitments not by relying on another provider's changing policies, but by owning the infrastructure decisions end-to-end.

"We can't give a privacy promise and then depend on a third party that might change policies six months later," Rajesh says. "We want to control the promise we make."

Why the UAE? Sovereignty Is Not a Buzzword

For years, ManageEngine served UAE customers from data centers in the United States. It worked until the region's strategy matured.

Government policies evolved, enterprise procurement tightened, and cloud sovereignty moved from talking point to mandate. Where data is stored, who controls it, and how it can be accessed became fundamental.

RAJESH GANESAN
CEO, MANAGEENGINE

"We are a technology company. **We don't want to rent** technology—we want to build it."

"Many of our customers here are large enterprises and government agencies," Rajesh says. "We can no longer tell them their data will live in the US. That era is over."

At that moment, the company faced two paths:

- Host on AWS UAE or another hyperscaler region.
- Build in the UAE and own the responsibility that comes with it.

The first path was quick and affordable, but carried an uncomfortable contradiction: ManageEngine would be making promises with someone else's infrastructure.

The second path space, power, cooling from Equinix, and everything else designed, deployed, and governed by ManageEngine was harder. It was also the only one that aligned with the company's character.

"We use the colocation for the basics," Rajesh explains. "Everything else is ours the hardware, the operating system, the database, the orchestration, the monitoring and we manage it with our own software."

This isn't just an operational choice; it's a statement: sovereignty is delivered, not just declared.

The Cost Myth

When a software company builds a data center, the reflexive question follows: Will this increase costs for customers? Rajesh refuses the premise. "Cost is not the first factor," he says. "Commitment is."

He elaborates: Good leadership doesn't optimize purely for short-term price; it optimizes for privacy, security, compliance, and continuity. Cheap SaaS today can become an expensive incident tomorrow if the governance is weak.

But what about the bill? Here, Manage Engine's internal operating model is telling:

- The company allocates 60% of spend to R\&D.
- It caps marketing at 18%.
- It resists a strategy of acquisitive growth.
- And it deliberately builds region-specific, right-sized infrastructure far from hyperscaler billions, close to $10 million to start.

The message to customers: we won't pass DC costs to you. The model is built to absorb the investment without punishing the buyer. "We prefer investing in technology over field sales muscle and heavy marketing," Rajesh says. "Our customers shouldn't pay for our philosophy."

Not Monopoly—But Loyalty

A bracing question follows in the interview: Is this sovereign DC strategy a path to monopolistic control locking customers into an entire ManageEngine world?

Rajesh answers with disarming candor. "Not monopoly. But yes ambition," he says. "We want customers to buy our products and stay with us for as long as possible."

But he frames the ambition in terms of trust and longevity, not market force. For customers that have been with ManageEngine for five years and more, the company's trajectory is visible: deeper product features, responsible support, and now sovereign infrastructure that signals permanence. Trust, not pricing bundles. Credibility, not coercion. "We will do what our customers need from us end to end," he says. "That's the philosophy."

Supply Chains, Choices, and Pragmatism

Building and operating a data center is not romantic. It's procurement, compliance, supply chains, and the math of efficiency.

ManageEngine buys hardware from distributors rather than fabricating it. "Supply chain matters," Rajesh says. "You buy where it's most cost-effective and reliable. If you buy everything in-region, it might become much more expensive." They'll explore policy frameworks like production-linked incentives when it makes sense; they won't claim purity points.

This isn't about building everything, it's about owning what matters: the design, the control plane, the data handling, and the promise.

AI: The Accelerator and the Alarm Bell

Sooner or later, the conversation turns to AI because these days it always does. Rajesh's view balances optimism and vigilance. "AI is an enabler," he says. "Security is the foundation."

The hardest part of the modern CIO's job might be this: How do I ensure the AI my enterprise uses is responsible? There is no universal answer. Enterprises will choose among OpenAI, Gemini, Meta Llama, DeepSeek, and others. ManageEngine itself has a purpose-built model for IT management tasks anomaly detection, predictions, summarization, content generation designed with bias checks and responsibility in mind.

But when customers use external models, the control shifts. That's where ManageEngine positions itself.

"We sit in between," Rajesh says. "We monitor what data leaves your organization, how it's masked, who is sending it, and whether it aligns with policy."

In other words: ManageEngine guards the enterprise boundary before data touches external AI. It can't regulate OpenAI's ethics. It can regulate your governance.

A Region That Moves Fast

The UAE is not just a location; it's a signal. Sovereign cloud is becoming a regional norm, and leaders are moving fast. ManageEngine's presence inside an Equinix facility taking only space, power, and cooling, and building everything else aligns with how the region wants to grow:

"Identity, endpoint, network, and infrastructure—that's the security foundation. AI is an enabler on top."

NIRMAL KUMAR MANOHARAN
VP – SALES, MANAGEENGINE (ZOHO CORPORATION)

"Customers wanted their data local. **For us, investing in the UAE** was not optional—it was necessary."

sovereign, secure, modern, and self-respecting. Customers here are not waiting for global templates. They're setting their own.

The Last Word

Before the interview wraps, Rajesh leaves two lines that could double as a north star for any organization caught between speed and substance: AI will change everything. Security will define everything.

That balance ambitious and anchoredis exactly where ManageEngine has staked its future. Not by shouting the loudest, but by building the quietest, hardest parts of the promise.

In an industry that often confuses renting with owning, ManageEngine has chosen ownership. In a world that outsources the inconvenient, it is insourcing responsibility. And in a region that is accelerating its digital sovereignty agenda, the company is making a bet that principles will compound.

It may not be the easiest path. But for customers who measure partners by what they stand behind, not just what they ship, it might be the most trustworthy one.

Managing Trust in the Cloud: Inside ManageEngine's UAE Data Center Push

How a bold regional investment is reshaping cloud strategy, customer value, and competitive positioning across the Middle East.

When ManageEngine announced the launch of its new UAE data center, it was more than a technical expansion it was a strategic shift shaped by two decades of customer demand, regulatory evolution, and the company's deepening commitment to cloud delivery. Sitting down with Nirmal Kumar Manoharan, Vice President of Sales, the rationale behind the investment becomes unmistakably clear.

For years, ManageEngine's cloud customers in the UAE were served from the US or Europe. This model worked in the early stages of adoption, but as sectors like BFSI, government, aviation, and large enterprises matured, data sovereignty became non-negotiable. "Customers have been asking us for years," Nirmal says. "They wanted their cloud workloads hosted locally, and the region was ready for it." Cloud is now ManageEngine's primary delivery path, and hosting workloads closer to the customer is central to that vision.

Nirmal expects the UAE data center to have a direct impact on revenue. The company has consistently delivered around 20% annual growth in the region, but with local hosting now available, that number is projected to rise to 25%. As enterprises move away from managing their own servers, local cloud services become both a necessity and a competitive advantage. "Cloud adoption is accelerating everywhere," he adds. "The UAE investment enables us to meet that demand confidently."

The broader GCC market naturally enters the conversation. Will customers in Qatar, Bahrain, or Oman also be served from the UAE? Not immediately, Nirmal explains. Both the UAE and Saudi data centers are newly operational, and ManageEngine's first priority is to strengthen and stabilize these two hubs. Once fully established, the company will evaluate whether the UAE should expand to serve other GCC states. For now, customers in smaller markets continue to be hosted from the US or Europe.

One distinguishing element of ManageEngine's strategy is its complete independence from hyperscalers. The company has never run its cloud services on AWS, Azure, or GCP. "We've always operated our own infrastructure," Nirmal emphasizes. "This gives us full control over data handling, compliance, and security something our customers value, especially in regulated sectors." Earlier, most of the company's cloud operations were managed from Chennai; with new data centers in the Middle East, operations now blend regional presence with global expertise.

The UAE data center is expected to immediately benefit three key sectors: financial institutions, which require strict data controls; government agencies, which follow sovereignty mandates; and large enterprises, which demand localized performance. "These sectors will feel the impact first," Nirmal notes. "The combination of compliance, speed, and reliability is exactly what they've been waiting for."

A project of this scale naturally requires people. ManageEngine plans to triple its Middle East headcount over the next one to two years, with extensive hiring across the UAE, Saudi Arabia, and Jordan. This includes engineering, support, Arabic-language teams, and customer success roles—aligning with regional expectations of responsiveness and cultural proximity.

When asked about competition, Nirmal is realistic but confident. ManageEngine has built a significant customer base over the past 20 years, including major government bodies and enterprise brands. The new data center, combined with local hiring and Arabic support, positions the company strongly against global vendors. "We're ready for a more aggressive phase," he says.

Looking ahead, innovation remains at the core. Rather than focusing on a single new product or niche, ManageEngine evolves continuously updating features, adding modules, and expanding capabilities across its portfolio. "Our products from two years ago are not the same today," Nirmal explains. "Continuous improvement is who we are." As the conversation wraps, Sanjay asks whether Nirmal is satisfied with the company's achievements. He smiles: "Happy? Yes. Content? Never." For 2026, his targets are clear 25% revenue growth and around 10% new customer logos in the UAE, a mature market where the focus is increasingly on value expansion rather than pure acquisition.

ManageEngine's UAE data center is not simply an infrastructure milestone it is a strategic anchor for the company's future in the Middle East. With deeper cloud capability, regional hiring, and longstanding customer trust, the company is poised to strengthen its leadership in one of its most important global markets. ENT

SCALING THE AI ECONOMY: WHY SUBSCRIPTION PLATFORMS ARE BECOMING FOUNDATIONAL TO ENTERPRISE AI

To scale AI sustainably, enterprises must evolve beyond pilots and into a governed, subscription-driven operating model—one that links usage to economics, policy, and performance. Subscription platforms are emerging as the core infrastructure that transforms AI from experimental projects into durable enterprise capabilities. The organizations that master this model will unlock predictable growth, controlled risk, and measurable AI ROI.

Enterprise leaders are discovering a hard truth: AI adoption is easy. AI sustainability is hard.

It's easy to roll out a copilot, run pilots on a foundation model, and get early wins. It's much harder to scale AI across hundreds of products, thousands of users, and regulated data—without turning AI into an unpredictable cost center or a governance nightmare.

The constraint isn't only model quality. It's the economics and operating model behind the AI stack.

Over the last decade, subscription platforms transformed how enterprises consume cloud, software, and infrastructure—making elastic growth possible through metering, entitlements, forecasting, and governance. Now the same shift is happening in AI. Subscription platforms are becoming foundational to the AI economy because they provide the mechanism enterprises need to scale responsibly: they convert upfront risk into governed consumption, make unit economics visible, and embed controls without slowing innovation.

This article introduces a practical framework for enterprise AI scale: a five-layer AI stack, and the "AI Monetization Plane" that enables it.

1) The AI economy is a five-layer stack

A useful way to understand AI industrialization is as a five-layer ecosystem:

- Energy — electricity, grid capacity, cooling
- Chips — GPUs/accelerators, high-performance networking
- Infrastructure — data centers/cloud, storage, orchestration, observability
- Models — foundation models, fine-tunes, embeddings, safety systems
- Applications — copilots, workflows, vertical AI, agents

Most organizations focus on layers 4 and 5 because that's where value is visible. But scaling failures typically originate in layers 1–3 where constraints are physical and financial—then compound upward into governance, reliability, and customer trust.

When AI is small, costs are "absorbed." When AI scales, three realities show up fast:

- AI costs are multi-dimensional (tokens, GPU time, retrieval, network, safety).
- Demand is spiky and uncertain (today's experiment becomes tomorrow's enterprise dependency).
- Governance becomes non-negotiable (privacy, residency, audit trails, policy enforcement).

This is why the next wave of enterprise AI won't be won by the best demo. It will be won by the best operating model for scale.

2) The sustainability problem: AI value is real, but the cost curve is slippery

AI pilots often look inexpensive until they hit production complexity:

- The model call isn't the only cost; retrieval pipelines, vector stores, observability, and safety layers add up.
- Latency and uptime expectations rise once workflows become business critical.
- Security and compliance controls must be consistent across teams, vendors, and regions.
- Shadow AI emerges when approved paths are slow or unclear.

As AI adoption grows, leadership needs consistent answers to five questions:

- What does it cost to deliver this AI capability (fully loaded)?
- Who is consuming it, and at what rate?
- What guardrails limit risk and runaway spend?
- How do we fund growth without big upfront bets?
- How do we tie spend to business outcomes?

If those questions can't be answered, AI becomes fragile—politically and financially—even when it's technically effective.

3) Why subscriptions matter: converting AI risk into AI throughput

PIYUSH ANANDANI
Director of Innovation – Enterprise Monetization & Subscription Platforms, Hewlett Packard Enterprise

"The next frontier in AI won't be defined by bigger models—it will be **defined by the operating models that make them sustainable.** Subscriptions are the bridge between innovation and enterprise-scale reality."

Subscriptions are not "billing." In enterprise AI, they are the mechanism that turns experimental capability into a scalable service. They bring three essential properties.

3.1 Optionality: capex-style commitments become opex-style control

AI demand curves are uncertain. Subscriptions and consumption-based models allow organizations to scale based on validated consumption and outcomes, rather than locking into capacity too early. Optionality is critical because models evolve quickly, and workloads shift as agents, retrieval, and multimodal patterns mature.

3.2 Unit economics: visibility enables optimization

At scale, "AI spend" cannot remain a shared overhead. Subscriptions introduce metering and attribution so you can measure:

- cost per contract summarized
- cost per invoice processed
- cost per developer feature shipped

Once unit economics exist, optimization becomes systematic: routing requests to smaller models, caching responses, batching inference, reducing retrieval calls, improving prompts, enforcing quotas, and targeting premium tiers where ROI is proven.

3.3 Governance at speed: controls without slowing innovation

Enterprises often swing between two extremes: lock down AI and stall adoption, or open access and suffer compliance/cost fallout. Subscription platforms enable the middle path through policy-aware entitlements—who can use what model, what data class, what limits, and what residency rules.

4) The "AI Monetization Plane": the missing enterprise layer

To scale AI like an enterprise capability, you need a layer that connects usage to governance and economics. I call this the AI Monetization Plane—the control plane that makes AI measurable, governable, and financially scalable.

Diagram 1 (conceptual): AI Stack Monetization Framework

Consider adding horizontal layers of identity and entitlements, metering, rating, pricing, billing and AI FI-ops. This is what makes AI behave like a product and not a science project.

5) How subscriptions scale each of the five layers (practical patterns)

Layer 1: Energy — treat power like a governed utility, not invisible overhead

AI growth turns energy into a first-class constraint. Subscription thinking here means moving from static assumptions to consumption-aligned planning:

- power-aware scheduling for non-urgent workloads
- internal incentives that reward teams to reduce waste
- operational "budgets" tied to energy/cooling constraints

Mini-vignette: A team scaling batch inference sees cost spikes at peak hours. By shifting non-urgent processing to lower-demand windows and enforcing workload quotas, they reduce spend volatility without reducing output.

Layer 2: Chips — make GPU capacity a product, not a political bottleneck

GPU scarcity becomes a governance and prioritization issue as much as a technical one. Subscription patterns include:

- reserved capacity tiers for predictable workloads
- burst pools for peaks and experimentation
- metered GPU-hours with show back/chargeback
- premium SLAs for latency-sensitive business flows

Mini-vignette: Engineering and data science compete for the same GPU cluster. With metered GPU-hours and tenant quotas, teams align to utilization goals. Waste becomes visible, and priority flows are protected by policy.

Layer 3: Infrastructure — build an AI platform that behaves like cloud

The cloud scaled because it standardized consumption, metering, and controls. AI platforms need the same:

- tenant model (apps/teams as tenants)
- dev/test/prod tiers with policies
- standardized usage events across pipelines
- AI FinOps dashboards for forecasting and anomaly detection

Mini-vignette: A company launches multiple copilots. Without standard telemetry, costs are blamed on "the platform." With common usage events and cost attribution by tenant, leaders can invest rationally—scaling winners and retiring low-ROI experiments.

Layer 4: Models — productize models with measurable throughput and trust

Token-based pricing is only the beginning. Enterprises need richer dimensions:

- latency tiering (real-time vs batch)
- context size and retrieval costs
- safety controls and audit requirements

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

CLOUDSEK UNCOVERS RAMADAN-THEMED MALWARE CAMPAIGN TARGETING MIDDLE EAST RETAIL SHOPPERS

Attackers Use Fake Festive Coupons to Deliver Stealthy Multi-Stage Remote Access Trojan That Exfiltrates Data Through AWS S3

AYUSH PANWAR
THREAT INTELLIGENCE RESEARCHER, CLOUDSEK

"Threat actors no longer need advanced exploits seasonal **trust, familiar brands and stealthy malware** chains are enough to cause real damage."

Cybersecurity intelligence firm CloudSEK has uncovered a sophisticated Ramadan-themed malware campaign targeting retail shoppers across the Middle East. Designed to exploit one of the region's busiest shopping periods, the attack uses convincing fake coupon offers from well-known retail brands to deliver a stealthy multi-stage Remote Access Trojan (RAT) capable of data theft, remote command execution, and long-term system compromise.

According to CloudSEK, the campaign impersonates a Ramadan promotion from AlCoupon and references popular retailers including Hyper One, Carrefour, Saudi, and Metro. Victims are enticed with a fake Ramadan basket worth 2,000 EGP and festive discounts. Once the malicious document is opened and macros are enabled, a hidden infection chain begins crafted specifically to evade modern security tools.

Living-off-the-Land Techniques Increase Stealth

What sets this campaign apart is its use of legitimate Microsoft utilities to execute malware. Instead of dropping a typical malicious file, attackers write obfuscated C# code directly onto the victim's machine and compile it using trusted system binaries such as:

- csc.exe
- MsBuild.exe
- ilasm.exe
- rundll32.exe

By abusing trusted tools that already exist on Windows systems, the malware blends seamlessly into routine processes making detection significantly harder for traditional antivirus and endpoint solutions.

CloudSEK reports that the final payload is a full-featured RAT capable of stealing files, capturing screenshots, executing shell commands, and maintaining persistent access. In an additional evasion technique, stolen data is uploaded via AWS S3 presigned URLs, rather than attacker-controlled servers, helping the activity blend into normal cloud traffic.

Tailored for Middle Eastern Victims

CloudSEK's analysis shows that the campaign is intentionally designed for Middle Eastern users. The lure is written in Arabic, references local brands, and uses the promo code RAMADAN25 to appear authentic. The seasonal timing increases the likelihood of victims opening unsolicited documents, especially during a busy retail period.

"This campaign shows how threat actors are adapting their tactics to local behaviour and seasonal consumer habits," said Ayush Panwar, Threat Intelligence Researcher at CloudSEK. "The risk lies not just in the lure, but in the way the malware abuses legitimate tools and trusted cloud infrastructure to avoid detection."

How the Attack Works

The infection chain begins once a victim opens the malicious Word document:

- A hidden VBA macro creates a staging folder.
- The macro writes 180+ KB of obfuscated C# code line-by-line.
- Native .NET compilers produce an executable that runs silently.
- A second-stage loader retrieves an MSIL payload, converts it to a DLL, and executes it using rundll32.exe.
- The malware identifies system details such as username, OS version, RAM, CPU, uptime and privilege level.
- Temporary files and staging artifacts are deleted to erase forensic evidence.

CloudSEK also flagged several detection indicators, including unusual process chains (e.g., WINWORD.exe spawning csc.exe), suspicious files (quanta.exe, msid.txt), abnormal rundll32 execution paths, and traffic associated with article-learning[.]com and article-learning[.]xyz.

A Growing Trend in Cybercrime

CloudSEK warns that this campaign reflects a broader shift in global cybercrime,

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

AUSTRALIA HIT BY HIGHEST VOLUME OF CYBERWARFARE ATTACKS WORLDWIDE, ARMIS RESEARCH WARNS

New data shows rising nation-state threats, AI-driven cyberattacks, and widening readiness gaps across Australian organisations

NADIR IZRAEL
CTO & CO-FOUNDER, ARMIS

"Cyberwarfare is now a constant condition **organisations must urgently shift from reactive** security to proactive defence."

Australia is experiencing the highest volume of cyberwarfare attacks of any country globally, according to new research from Armis, the cyber exposure management and security company. The findings, published in the fourth annual Armis Labs Cyberwarfare Report, reveal a rapidly escalating threat environment driven by geopolitical tensions, AI-enabled attackers, and critical gaps in security preparedness across the country.

Armis reports that 72% of Australian organisations were forced to report an act of cyberwarfare to authorities in the past year up from 56% in 2025 and the highest rate among all countries surveyed. The rise comes amid growing national concern, with 81% of Australian IT decision-makers worried about the use of AI by nation-state actors to create more targeted and sophisticated attacks.

"Geopolitical tensions, AI acceleration, and unresolved security gaps are colliding, bringing the state of cyberwarfare to a boiling point," said Nadir Izrael, CTO and Co-Founder of Armis. "Attackers are operating at machine speed, while too many organisations still rely on outdated assumptions and reactive structures. Leaders must immediately strengthen proactive cybersecurity operations before it's too late."

Rising fears of full-scale cyber conflict

The report depicts a rapidly intensifying global threat landscape, with Australia positioned as one of the most critically impacted nations. According to the study:

- 84% of Australian IT leaders fear that nation-state cyber capabilities could trigger a full-scale cyberwar capable of crippling global infrastructure.
- 73% believe emerging technologies such as AI and quantum computing will dramatically escalate cyber conflict.
- 77% say GenAI is reshaping the geopolitical balance by enabling smaller nations to act as near-peer cyber adversaries.

Despite these escalating risks, Australian organisations show uneven readiness. While 84% say they have strengthened their cyberwarfare posture in the past three years, many continue to struggle with core vulnerabilities.

High breach rates, budget strain and defensive blind spots

Nearly 73% of Australian organisations reported one to two cybersecurity breaches last year, while 59% admit they have still not fully secured their environment following an attack. The issue is compounded by the fact that 45% of businesses respond to major cyber incidents only during or after an attack highlighting persistent reactive practices.

The financial burden is also rising sharply. Australian organisations reported an average ransomware payout of US$15.39M in 2025, up from $8.61M the previous year. Alarmingly, 66% say their typical ransomware payout exceeds their entire annual cybersecurity budget.

"Traditional security approaches that are reactive, fragmented, and blind to the full attack surface are obsolete," said Zak Menegazzi, Cybersecurity Specialist ANZ, Armis. "Australia remains critically under-prepared for the threats we face today. Organisations must urgently adopt proactive, intelligence-driven measures to build resilience against AI-powered cyberwarfare."

Key findings from Australia

- 62% delayed or halted digital transformation due to cyberwarfare concerns.
- 70% experienced an AI-generated or AI-led attack in the past 12 months highest globally.
- 95% are concerned about the overall impact of cyberwarfare on their organisation.
- 86% say nation-state threats increasingly target unmanaged or supply-chain assets invisible to traditional tools.
- 70% express strong confidence in the Australian government's ability to defend citizens and enterprises.

The findings are based on responses from 1,900+ IT decision-makers, including 200 from Australia, combined with Armis Labs' proprietary threat intelligence. ENT

THE TOKENIZATION RACE: HOW WALL STREET'S BIG THREE ARE RESHAPING DIGITAL ASSET INFRASTRUCTURE

How BlackRock, Goldman Sachs, and J.P. Morgan Are Taking Divergent Paths to Dominate the Next Era of On-Chain Finance

In the rapidly evolving landscape of digital finance, three major financial institutions have emerged with fundamentally different approaches to asset tokenization. BlackRock's BUIDL, Goldman Sachs' GS DAP, and J.P. Morgan's Kinexys represent divergent strategic visions for the future of on-chain finance, each targeting distinct segments of the institutional market with purpose-built infrastructure.

While all three initiatives share the common goal of modernizing financial markets through blockchain technology, their architectures, asset classes, and strategic objectives reveal sharply different philosophies about how tokenization will reshape the industry.

Three Platforms, Three Philosophies

BlackRock's BUIDL (USD Institutional Digital Liquidity Fund) has taken the bold step of launching on Ethereum's public blockchain, positioning itself as a tokenized money market fund that provides investors with daily dividend accruals in USD. Launched in partnership with Securitize Markets, BUIDL focuses on tokenized U.S. Treasuries, offering institutional investors on-chain yield with enhanced liquidity and transparency. The platform represents BlackRock's bet that public blockchains can deliver both the transparency and the institutional-grade reliability that traditional investors demand.

Goldman Sachs has charted a different course with its Digital Asset Platform (GS DAP), building on Digital Asset's Canton Network, a permissioned distributed ledger technology. Rather than creating a single product, Goldman has constructed a comprehensive institutional infrastructure designed for issuing, registering, and settling digital assets including securities and bonds. The platform's collaboration with BNY on tokenized money market fund settlement demonstrates its focus on accelerating settlement times and reducing operational costs across the institutional ecosystem.

J.P. Morgan's Kinexys (formerly Onyx Digital Assets) has prioritized speed and scale, developing a private, permissioned blockchain system optimized for instant payment settlements and tokenized collateral management. With over $1.5 trillion in tokenized transactions processed by mid-2025, Kinexys has achieved remarkable adoption through its flagship products: JPM Coin for payment rails and the Tokenized Collateral Network (TCN). The platform's 24/7 programmable payments and instant settlement of intraday repos address critical pain points in institutional treasury management.

Strategic Positioning and Market Focus

The strategic differentiation among these platforms becomes clearer when examining their primary use cases and target markets.

BUIDL operates as a product in the truest sense: a tokenized investment vehicle designed to deliver yield to on-chain investors. By anchoring its offering in U.S. Treasuries and providing daily accruals, BlackRock has created a cash-equivalent token that bridges traditional finance and decentralized finance. The choice of Ethereum as the underlying blockchain signals confidence in public infrastructure and positions BUIDL to integrate with the broader DeFi ecosystem.

GS DAP functions as a platform, providing the essential plumbing for digital asset issuance and lifecycle management. Goldman Sachs has positioned itself not as a product provider but as an infrastructure enabler, allowing institutions to issue tokenized bonds, funds, and other securities with significantly reduced settlement times. This platform approach reflects Goldman's traditional role as a market maker and facilitator rather than a direct asset manager.

Kinexys represents a network play, focusing on the movement of cash and collateral rather than static asset ownership. J.P. Morgan's emphasis on instant settlement and programmable payments addresses immediate operational needs in treasury and liquidity management. The platform's impressive transaction volume demonstrates market validation of its core value proposition: speed and reliability in institutional cash movement.

Technical Architecture and Blockchain Strategy

VIJETH SHIVAPPA
REGIONAL TEAM LEAD – SOLUTIONS CONSULTANT / TECHNICAL SALES, HITACHI VANTARA

"Tokenization is no longer an experiment it's the new **battleground where Wall Street is quietly rebuilding** the plumbing of global finance."

The choice of blockchain infrastructure reveals fundamental differences in how these institutions view the trade-offs between transparency, control, and interoperability.

BlackRock's embrace of Ethereum places BUIDL in the public blockchain camp, accepting the challenges of public infrastructure in exchange for composability and transparency. Investors can verify holdings on-chain, and the fund can potentially interact with other

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

INDIA'S OWN
IT NETWORKING CHOICE

DIGISOL®

TRUTHFULLY INDIAN

BY BIRTH. BY WORK. BY VISION.

30+ YEARS OF IT NETWORKING EXPERTISE

MADE IN INDIA PRODUCT PORTFOLIO

SOLUTIONS COMMITTED TO INDIA'S PROGRESS

STRUCTURED CABLING SOLUTIONS

COLLAPSIBLE DOOR KEYSTONE

FACE PLATE

CAT6 UTP PATCH CORD

CAT6 UTP 24 PORT 180 DEGREE PATCH PANEL

CAT5e RJ45 CONNECTOR

FTTH SOLUTIONS

DUAL BAND ONU

GEPON OLT

GEPON OLT TRANSCEIVER

GPON OLT

WIRELESS SOLUTIONS

HIGH GAIN WIRELESS DUAL-BAND USB ADAPTERS

ENTERPRISE Wi-Fi 6 ACCESS POINT

INDDOR CEILING MOUNT Wi-Fi 6 ACCESS POINT

IN-WALL CEILING MOUNT Wi-Fi 6 WIRELESS AP

ENTERPRISE ACCESS POINT CONTROLLER

SWITCHING SOLUTIONS

SMART MANAGED SWITCH

WEB MANAGED SWITCH

FULLY MANAGED SWITCH

UNMANAGED SWITCH

East: 9748834333 | South: 9566099681 | North/West: 9987090414

www.digisol.com | 1800 209 3444

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

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

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

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

sales@prostarm.com

www.prostarm.com