GALAXY
Integrating Technology | Driving Growth

TECH TALK

Issue 165
March 2026

Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.

We are proud to announce that we are honoured to be recognised as **Strategic Partner of the Year – India** by **Commvault** at the **SHIFT India Partner Leadership Summit 2026.**

This milestone reflects our unwavering commitment to building trusted partnerships, driving innovation, and delivering measurable impact for our customers. It reinforces our dedication to excellence and our shared vision of enabling secure, resilient, and future-ready enterprises.

We are grateful for the collaboration, continued trust, and strong relationships that make such achievements possible.

Here's to many more milestones together.

Foreword

Dear Readers,

At the beginning of the year, I had predicted that Cognitive Zero-Trust Fabric will be poised for widespread adoption in 2026. This month, I will try and dive deeper into what Cognitive Zero-Trust Fabric actually is.

Traditional security models assumed that systems inside the corporate perimeter could be trusted. That assumption is no longer valid. Modern IT environments span multi-cloud infrastructures, distributed edge deployments, APIs, AI services, and hybrid workforces. The attack surface has expanded dramatically, and static rule-based security approaches struggle to keep pace with increasingly sophisticated threats.

Zero-Trust architectures addressed part of this challenge by enforcing the principle of "never trust, always verify. "However, the scale and complexity of digital ecosystems in 2026 require a more adaptive approach. This is where Cognitive Zero-Trust Fabric helps. By combining AI-driven analytics, behavioural identity intelligence, and continuous policy enforcement, this architecture enables security systems to dynamically evaluate trust across users, devices, applications, and data flows in real time.

Instead of relying solely on predefined rules, a cognitive security fabric continuously learns from network activity, user behaviour, and system interactions. It can detect anomalies, predict potential attack paths, and automatically adjust access policies before threats materialize. This adaptive security layer becomes especially critical as AI agents, automated workflows, and distributed edge systems begin making autonomous decisions within enterprise environments.

Foreword

Cybersecurity in the AI era cannot rely on rigid boundaries or static policies. It must be intelligent, adaptive, and deeply integrated into the fabric of digital infrastructure. Cognitive Zero-Trust Fabric represents a critical step toward a future where trust is continuously verified, intelligence is embedded into every layer, and security becomes a catalyst for innovation rather than a constraint.

Reach out to our experts and evangelists to explore how Cognitive Zero-Trust Fabric can strengthen your organization's AI-driven infrastructure.

Happy reading!

Anoop Pai Dhungat
Chairman & Managing Director

Scientists Unveil Nanobots That Target and Kill Cancer Cells

To begin with, the intelligentsia at the Karolinska Institute in Sweden made it possible to deliver only nanobots that specialize in destroying cancer cells. This approach to nanotechnology involves developing a nanobot. These robots move using the energy they get from a fly and can kill cancer cells, only with minor destruction to nearby healthy cells.

The nanobots are designed with strict safety guidelines. The initial approach introduces DNA origami switches that contain death receptors and cause cell death. These receptors are specific only in the acidic environment, where tumours are generally found, and their influence on healthy cells drops. In the experiments performed on mice with human breast cancer cells, the nanobots killed off the tumour cells by 70%, showing that they are both cancer-specific and practical.

This therapy has been a path-breaking event, and it has emerged as a possibility that nanotechnology can even become a part of the medical revolution. This picture indicates how nanotechnology can make treatments more successful and precise, hence lessening the side effects of the current therapies.

Moreover, it is a way out for cancer patients. Therapies are becoming available with less severe side effects. Thus, patients will have the chance to recover, and doctors are more likely to find a cure.

The Technology Behind the Nanobots

The principle of using molecular biology powers modern nanotechnology and the newly produced nanobots for cancer treatment. The general concept of these robots is DNA origami construction, which eventually takes the DNA molecule and architecturally folds it into a particular structure with the required functionality. The nature of these robots is that they cannot operate in the cell's neutral pH but can work under an acidic environment, as seen in tumour cells.

Then, the robots will stick to the cancer cells and kill them. Below is a treatment plan for the cancer cells using the nanobots: All these disciplines that have taken place to develop these nanobots indicate the knowledge interrelationship in the module.The nanobots that act as "death receptors" contain apoptosis that is otherwise laid out as a pharmaceutical rather than when the normal cells are left. These autonomous units of nanorobotics not only let the cell nano-sensors of the body's function report to the cloud over their location but also the cues the doctor must inject and the place to which the pharmaceuticals should go, e.g., apply to the tumour.

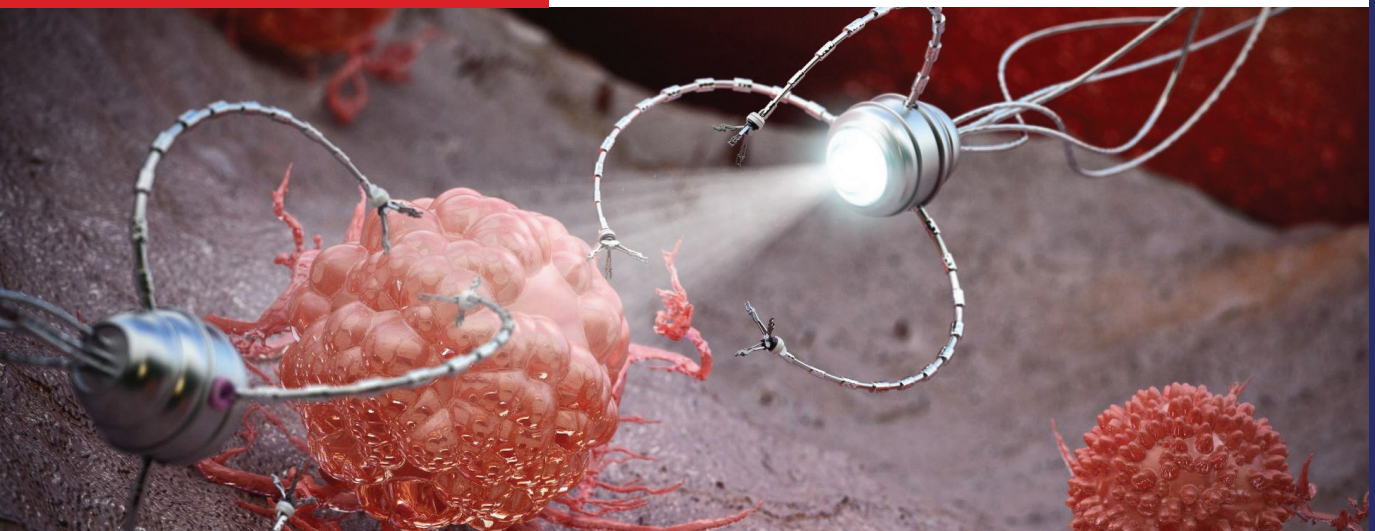
The best exploration is to give local low-dose therapy targeted to cancer to prevent the whole body from absorbing the drug and becoming toxic. The cooperation that has brought us these nanobots is the perfect scenario for using different approaches to solve problems simultaneously. This would be made possible by a new micro-robotic earth core drilling method, a strong candidate for geothermal energy and earth science applications.

Mechanism of Action

The nanobots are flexible and can be used well by the Swedes depending on their creation; they function only in a sick environment, for example, with a pH of 7.4, a typical number for healthy tissue. Still, the pH of cancer has a slight difference (6.5); it is a slightly acidic environment. This difference is necessary for the nanobots' function and will be further described. Every time a tumour is present, the nanobot works because it assimilates the acidic change in the body and, as a result, shifts its form into a new configuration. The exosome replenishment re-exposes HLA-option DR49 to the cells that acquire the tumour antigen and regain the apoptotic abilities thereof. With this tool, exosomal nanoparticles can reprogram the antigenic cargo of tumor cells by recycling apoptotic vesicles. After binding, the cancer cells are shocked by apoptosis and mutated or deactivated.

This focused approach is an essential improvement compared to the methods of the past, such as radio- or chemotherapy, treatments that bring damage to cancerous and healthy cells. Hence, the treatment becomes difficult to tolerate. It would be possible with targeted therapy for cancer with nanobots that the outcomes are positive, cancerous cells are attacked, and fewer healthy cells are affected, as the tumours' acid spaces are influenced and the proper tissues untouchable remains. This is the first step in developing the use of more precise and less toxic drugs against cancer.

Read more →



TECHNOLOGY FOCUS

What Is Quantum Cybersecurity?

The Future of Digital Protection Explained

Quantum cybersecurity is an emerging field that leverages the principles of quantum mechanics to enhance digital security. It is a response to the evolving threats posed by quantum computing to conventional cryptographic systems. Traditional cybersecurity methods rely on mathematical complexity to protect data, but quantum computers have the potential to break many of these encryption protocols, necessitating a shift toward quantum-resistant and quantum-enhanced security solutions.

Quantum cybersecurity encompasses two primary approaches: post-quantum cryptography (PQC) and quantum cryptography. PQC involves developing encryption methods that can withstand attacks from quantum computers while remaining compatible with classical systems. On the other hand, quantum cryptography utilizes quantum mechanics principles, such as quantum key distribution (QKD), to create theoretically unbreakable encryption techniques.

Organizations and governments worldwide are investing in quantum cybersecurity to future-proof their data and communications against potential cyber threats. This field is critical for securing sensitive information, financial transactions, and national security infrastructure.

How Quantum Computing Impacts Cybersecurity

Quantum computing represents both a challenge and an opportunity for cybersecurity. The main concern is that quantum computers can break widely used encryption algorithms, rendering many traditional security methods obsolete. Here's how quantum computing impacts cybersecurity:

1. The Threat to Classical Cryptography

Most modern encryption relies on complex mathematical problems that classical computers take an impractically long time to solve.

However, quantum computers, through algorithms such as Shor's algorithm, could in the future factor large numbers exponentially faster than classical computers,

compromising widely used encryption schemes like RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and Diffie-Hellman key exchange.

2. Quantum-Secure Cryptography

To counteract this threat, cryptographers are developing post-quantum cryptographic (PQC) algorithms,

designed to be secure against both classical and quantum attacks.

These algorithms rely on hard mathematical problems that quantum computers cannot efficiently solve.

3. Quantum Key Distribution (QKD)

To counteract this threat, cryptographers are developing post-quantum cryptographic (PQC) algorithms,

designed to be secure against both classical and quantum attacks.

These algorithms rely on hard mathematical problems that quantum computers cannot efficiently solve.

4. Quantum Random Number Generators (QRNGs)

Classical encryption often depends on pseudo-random number generators, which can sometimes be predictable. QRNGs use quantum mechanics to generate truly random numbers, ensuring unprecedented security for cryptographic keys.

While quantum computing poses risks to existing cybersecurity frameworks, it also presents new, highly secure methods for encryption and secure communications.

Key Features of Quantum Cybersecurity

Quantum cybersecurity is defined by several key features that distinguish it from classical security measures:

1. Unbreakable Encryption with Quantum Cryptography

Quantum cryptographic techniques, such as QKD, offer theoretically unbreakable encryption by leveraging quantum mechanics principles like superposition and entanglement.

2. Quantum-Resistant Algorithms

Post-quantum cryptography ensures data security even against powerful quantum computers. These algorithms rely on complex problems such as lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography.

3. Intrusion Detection via Quantum Mechanics

Quantum cybersecurity enables new ways to detect cyber threats. Since quantum states collapse upon measurement, any attempt to eavesdrop on a quantum-encrypted communication will be instantly detected.

4. True Randomness with QRNGs

Quantum random number generators use quantum fluctuations to produce genuine randomness, making cryptographic keys more secure compared to traditional pseudo-random generators.

5. Enhanced Authentication and Secure Communications

Quantum-secure authentication methods prevent identity theft and unauthorized access. Quantum-enhanced secure communication channels ensure tamper-proof data transfer, benefiting industries handling sensitive information.

Together, these features make quantum cybersecurity a powerful tool for securing digital systems in a world increasingly threatened by advanced cyberattacks.

Galaxy empowers organizations to stay ahead of emerging quantum-era threats by enabling future-ready cybersecurity through quantum-resistant cryptography, advanced key protection, true randomness, and governance-driven security frameworks. Our approach helps safeguard sensitive data, strengthen digital trust, and ensure long-term cyber resilience in an evolving threat landscape.

To connect with our experts, write to us at marketing@goapl.com

Read more →

SPECIAL FOCUS

How to Build a 90-Day DPDP Compliance Technology Roadmap

India's Digital Personal Data Protection (DPDP) Act has shifted privacy from a legal discussion to a technology execution mandate. Organizations are now expected to demonstrate visibility, control, and accountability over personal data - across hybrid infrastructure, legacy platforms, SaaS ecosystems, and partner networks.

The challenge?

Most enterprises don't fail at intent - they fail at operationalizing compliance inside IT systems.

This 90-day roadmap provides a structured, execution-focused approach to help organizations transition from policy readiness to technical enforcement.

Why a 90-Day Approach Works

DPDP compliance is not a one-time project. It's a transformation.

A 90-day roadmap helps organizations:

- Achieve rapid visibility into personal data risks
- Prioritize high-impact remediation instead of boiling the ocean
- Establish defensible safeguards aligned with regulatory expectations from Ministry of Electronics & Information Technology
- Build a scalable privacy-by-design foundation

The 90-Day DPDP Compliance Technology Roadmap

Phase 1 (Days 0-30): Data Visibility & Risk Baseline

Objective: Establish a comprehensive "Ground Truth" for personal data by uncovering its location, movement, and security status.

Automated Data Discovery

Deploy scans across the entire ecosystem, including cloud storage, legacy databases, and employee endpoints, to catalogue both structured and unstructured data.

Centralized Data Registry

Construct a master inventory that classifies data types and validates the legal justification for their retention.

Data Lineage Mapping

Visualize how data traverses internal systems and where it exits to third-party partners or international jurisdictions.

Vulnerability Assessment

Pinpoint "hot zones" such as unencrypted repositories, forgotten (Shadow IT) databases, and redundant data.

Phase 2 (Days 31-60): Control Implementation & Process Alignment

Objective: Transition from visibility to active enforcement by embedding DPDP-compliant controls into the tech stack.

- Consent Lifecycle Management: Deploy a robust architecture to capture, timestamp, and store granular consent. Ensure "Withdrawal Synchronization" so that if a user opts out, the preference propagates to all downstream systems.
- Automated Rights Fulfilment: Streamline Data Principal Rights (SRRs) by building automated workflows for data access, correction, and the "Right to Erasure," supported by secure identity verification.
- Privacy-by-Design Implementation: Enforce data minimization by stripping non-essential fields from UI/UX and backend schemas, ensuring collection is strictly tethered to a defined business purpose.
- Advanced Data Protection: Institutionalize "Security-by-Default" through end-to-end encryption, strict Role-Based Access Control (RBAC), and continuous audit logging of all PII access.

Phase 3 (Days 61-90): Automation, Monitoring & Governance Readiness

Objective: Institutionalize data protection through automation, ensuring the organization remains "compliant by default."

- Proactive Security Telemetry: Deploy User and Entity Behaviour Analytics (UEBA) to detect anomalous access to personal data. Maintain immutable, forensic-grade logs for real-time threat detection and post-incident analysis.
- Resilient Incident Response: Formalize a "Privacy-First" breach framework. This includes automated impact assessments and predefined workflows to meet strict regulatory notification timelines.
- DevSecPrivacy Integration: Embed data protection into the Software Development Life Cycle (SDLC). Implement automated data masking in staging environments and "Privacy Gates" within CI/CD pipelines.
- Executive Oversight Dashboards: Launch centralized reporting to track Key Performance Indicators (KPIs), such as Right-to-Erasure fulfilment speeds and overall data risk scores.

How Galaxy Helps Accelerate DPDP Compliance in 90 Days

- Galaxy enables organizations to translate DPDP obligations into deployable technology controls through a structured, outcome-driven approach.
- Rapid Discovery & Classification Instantly locate and categorize personal data across on-prem, multi-cloud, SaaS, and legacy systems to create a unified "Source of Truth."
- Consent & Lifecycle Engineering Systemically embed consent capture, validation, and withdrawal directly into your digital architecture to eliminate manual compliance gaps.
- Automated Data Flow Mapping: Visualize how data traverses applications, vendors, and borders to identify and close hidden exposure points.
- Data-Centric Security Safeguards Harden protection using Zero Trust principles, end-to-end encryption, and real-time monitoring of all sensitive data interactions.
- Automated Rights Fulfilment Deploy seamless workflows for Data Principal requests (Access, Correction, Erasure) without disrupting core business operations.
- Privacy-by-Design (DevOps) Integrate privacy engineering and data masking into CI/CD pipelines, ensuring every new release is compliant by default.
- Audit-Ready Governance Equip leadership with real-time dashboards tracking risk posture, consent metrics, and regulatory accountability.

With the right technology roadmap and execution partner, DPDP compliance can move from uncertainty to structured transformation—in just 90 days.

GALAXY helps organizations meet DPDP compliance by assessing data flows, implementing security controls, and deploying compliant tools for consent, access control, and breach management.

To talk to our experts, write to us at marketing@goapl.com

TECH NEWS

Perplexity CEO Aravind Srinivas reveals the ‘next big thing’ with Perplexity Computer

After nearly two months of silence, Perplexity AI is back in action. The AI start-up headed by Aravind Srinivas has announced Perplexity Computer, its latest flagship offering that redefines the functions of AI-powered assistants.

Perplexity AI began as an AI-powered answer engine, something like Google that summarises info into paragraphs with source citations. The AI search engine is capable of research, summarisation, and generation, and with its latest offering, Perplexity aims to go way further.

Following the roll-out of Perplexity Computer, co-founder and CEO Aravind Srinivas, who has been missing in action for weeks, took to his X profile to share what the company has been up to for the past two months.

What has Perplexity been up to last two months? We’ve silently been working on the next big thing: Perplexity Computer. Computer unifies every current capability of AI into a single system. Files, tools, memory, and models, orchestrated together, working for you,” he wrote.

Perplexity Computer brings AI capabilities that give more power to AI assistants. It does not merely answer questions or small bits of code and is being pitched as a general-purpose digital worker. Essentially, a virtual agent that can autonomously carry out an assortment of tasks on a user’s behalf, such as researching, coding, drafting, deploying, and managing workflows, and all of these with minimal human supervision.

Conceptually, when a user asks Perplexity Computer to do a task, it breaks it into subtasks, employs multiple specialised AI models to handle those tasks, and stitches together results into a finished product. The models may split research, coding, data extraction, design, and deployment tasks among themselves, and all of these are managed by the platform’s internal logic.

Read more →

TECH NEWS

DeepSeek withholds the latest AI model from US chipmakers, including Nvidia

DeepSeek, the Chinese artificial intelligence lab whose low-cost model rattled global markets last year, has not shown U.S. chipmakers its upcoming flagship model for performance optimization, two sources familiar with the matter said, breaking from standard industry practice ahead of a major model update.

Instead, the lab, which is expected to launch its next major update, V4, granted early access to domestic suppliers, including Huawei Technologies, the sources said. AI developers typically share pre-release versions of major models with leading chipmakers such as Nvidia and Advanced Micro

Devices to ensure their software performs efficiently on widely used hardware. DeepSeek has previously worked closely with Nvidia's technical staff.

NVIDIA, AMD Left out

For its forthcoming model, which was expected to be released around the Lunar New Year holiday, DeepSeek did not provide access to Nvidia and AMD and gave Chinese chipmakers, including Huawei, a head start of several weeks to optimize the software for their processors, the sources said.

NVIDIA and AMD declined to comment. DeepSeek and Huawei did not respond to requests for comment.

Reuters could not immediately determine the reason for the decision.

"The impact to Nvidia and AMD for general data accelerators is minimal – most enterprises are not running DeepSeek, which serves as a benchmarking model more than anything else," said Ben Bajarin, CEO of research firm Creative Strategies. He added that new AI coding tools are reducing the time it takes to make software run well on hardware, "from months to weeks."

The move is likely part of a broader strategy by the Chinese government "to try to keep U.S. hardware and models disadvantaged" in China, Bajarin said. The development comes as a senior Trump administration official told Reuters DeepSeek's latest AI model was trained on Nvidia's most advanced chip, Blackwell, using a cluster in mainland China, in a move that appears to violate U.S. export controls.

Read more →

GALAXY
Integrating Technology | Driving Growth

Galaxy Office Automation Pvt. Ltd. B-602,
Lotus Corporate Park, Graham Firth
Compound, Off. Western Express Highway,
Goregaon (E), Mumbai - 400 063.

+91 22 46108999

marketing@goapl.com

www.goapl.com

© 2026 Galaxy Office Automation Pvt Ltd . All Rights Reserved.
All product names, logos, brands, trademarks, and registered
trademarks are the property of their respective owners.