GALAXY
Integrating Technology | Driving Growth

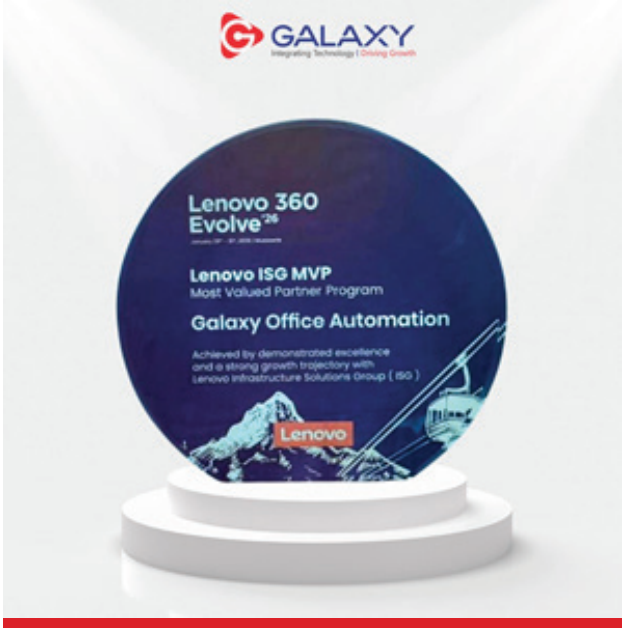
TECH TALK

Issue 166
April 2026

Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.



We are proud to share that we have been recognized as a Lenovo ISG MVP – Most Valued Partner at Lenovo 360 Evolve ’26. This prestigious recognition is a testament to our unwavering commitment to excellence, consistent growth, and delivering impactful, future-ready infrastructure solutions.

A heartfelt thank you to Lenovo ISG for this honour, to our Incredible team for their dedication, and to our valued partners and clients for their continued trust and collaboration.

Here’s to driving innovation together and building resilient, future-ready enterprises!

Foreword

Dear Readers,

At the beginning of the year, I had predicted that Confidential AI would move from niche to norm in 2026. This month, I will dive deeper into what Confidential AI actually means, why it matters now more than ever, and how it is quietly becoming the cornerstone of trustworthy enterprise AI.

Organisations are racing to build proprietary AI models trained on sensitive business data like customer records, financial transactions, clinical datasets, and intellectual property. The gives rise to a fundamental question - Who can actually see your data when it is being processed in the cloud? The uncomfortable answer, until recently, was that cloud providers' hypervisors and infrastructure administrators could, in principle, access data in use. Encryption at rest and in transit addressed two thirds of the problem. Confidential AI addresses the third and most vulnerable leg: data in use, during active computation.

Confidential computing achieves this through hardware-based Trusted Execution Environments (TEE) , which are isolated, encrypted memory regions within the processor itself. Inside a TEE, code and data are shielded from the host operating system, the hypervisor, and even the cloud provider's own administrators. When applied to AI workloads, this means that model training runs, inference pipelines, and fine-tuning jobs can execute in a cryptographically verified enclave. The training data, the gradients, and the resulting model weights remain invisible to anyone outside that boundary.

This is not a theoretical future. Major cloud providers are already rolling out Confidential AI Training Clusters, purpose-built environments that combine TEE-enabled GPU instances with hardware attestation frameworks. Attestation is the mechanism by which an organization can prove, cryptographically, that a given computation ran inside a genuine, unmodified enclave and not on a compromised or tampered host. This creates an auditable chain of trust from raw data to deployed model, something regulators and enterprise procurement teams are increasingly demanding as a baseline.

Foreword

The business implications are significant. Industries like banking, healthcare, defence, and legal services that operate under strict data sovereignty and privacy regulations have historically been the most cautious adopters of cloud-based AI. Confidential AI removes a structural barrier that has kept sensitive workloads on-premises or out of AI pipelines entirely. Multi-party scenarios also become viable: two organizations can collaborate on a jointly trained model without either party exposing their underlying data to the other, with the TEE acting as a neutral, verifiable intermediary.

The complexity of implementing Confidential AI includes spanning TEE-enabled hardware selection, attestation frameworks, secure enclaves for inference, and integration with existing zero-trust and data governance policies. This is precisely where expertise matters. At Galaxy, we serve as your AI Systems Integrator, bringing together the hardware, security, and software disciplines required to build Confidential AI pipelines that are not just technically sound but operationally sustainable. Our NOC & Managed Services, leverage AI and hyperautomation to continuously monitor and assure these environments, ensuring that the integrity of your confidential workloads is maintained well beyond initial deployment.

The era of trusting your cloud provider's assurances on faith alone is giving way to an era of verifiable trust where security guarantees are physical, not contractual. Confidential AI is the infrastructure layer that makes that possible.

Reach out to our experts and evangelists to explore how Confidential AI can protect your most sensitive workloads and unlock AI initiatives that once seemed too risky to pursue.

Happy reading!

Anoop Pai Dhungat
Chairman & Managing Director

This magnet-powered micro-robot could soon swim through your bloodstream

Scientists have developed a microrobot that can deliver medicine exactly where it's needed using magnets, according to a recent study from ETH Zurich, a Swiss university.

This new technology could enable doctors to dissolve blockages that cause strokes, treat infections with antibiotics, and deliver anti-cancer medication directly to tumours, without side effects elsewhere in the body.

The robot consists of a tiny spherical capsule, made of a dissolvable gel and iron oxide nanoparticles, which are added to make it magnetic. The scientists can track the robot using X-ray tech.

"Because the vessels in the human brain are so small, there is a limit to how big the capsule can be," said lead author Dr Fabian Landers, a postdoctoral researcher at the Multi-Scale Robotics Lab at ETH Zurich.

"The technical challenge is to ensure that a capsule this small also has sufficient magnetic properties."

The next challenge was to drive the robot through the maze of blood vessels, navigating twists, junctions, and fast-flowing blood.
"It's remarkable how much blood flows through our vessels and at such high speed," said Landers.

"Our navigation system must be able to withstand all of that."

So, they developed three ways to drive the microrobot with electromagnets. Depending on the type of magnetic force they used, the scientists were able to roll the robot against the vessel wall or pull it in a certain direction.

With these techniques, the microrobot could travel with or against the current and travel at speeds up to 4mm per second (or one inch every six seconds).

"Magnetic fields and gradients are ideal for minimally invasive procedures because they penetrate deep into the body and – at least at the strengths and frequencies we use – have no detrimental effects on the body," said last author Prof Bradley Nelson, a microrobot researcher at ETH Zurich.

Once the microrobot reached its target, the scientists could use a high-frequency magnetic field to heat the microrobot, dissolving its shell and releasing the medicine inside.

This invention was tested using silicone models that replicated the blood vessels of humans and animals, as well as in several pigs and the brain of a sheep.

The scientists' next goal is to begin human clinical trials, so this technology can soon be used in hospital operating theatres.

Read more →

TECHNOLOGY FOCUS

What is High Availability? A Simple Guide for Growing Businesses

High availability (HA) is a term that refers to a system's ability to be accessible and reliable close to 100% of the time. Highly available systems must be able to withstand outages, including scheduled downtime and site-wide disasters. Typically, HA systems meet two characteristics: They must be available for use close to 100% of the time. They must be able to meet a certain set of predetermined user expectations.

With the growth of digital transformation initiatives and the subsequent move of many services to the cloud, high availability solutions are now offered by many tech and software as a service (SaaS) companies, including Microsoft, Amazon (AWS), IBM, Red Hat, and more. High availability of IT systems is particularly important in industries where critical applications rely on having little or no system downtime. For example, in hospitals and data centers, users depend on high availability solutions to perform many routine, daily functions. If users can't access a system for any reason, it is deemed 'unavailable.' The period of time that a system is unavailable to users is known as downtime. HA versus Disaster Recovery (DR) Disaster recovery (DR) consists of IT infrastructure technologies and best practices designed to prevent or minimize data loss and business continuity disruption resulting from catastrophic events. High availability (HA), on the other hand, typically concerns smaller failures or faults that might impact a systems' availability. Even though they are different, DR and HA both share the goal of minimizing disruption to IT systems, and both typically employ redundant components and redundant systems as part of an overall strategy. Also, both DR and HA use data backups to make data available in case of a wide range of problems, including hardware failures, software failures and power outages. HA versus fault tolerance Fault tolerance is a system's ability to operate continuously after one or more of its critical components fail. Like HA, fault tolerance can help make a system available during or after a disruptive event.

However, where fault tolerance and HA differ is in the way they treat downtime. While HA seeks to have as little downtime as possible, the goal of fault tolerance is zero downtime, a goal it can only achieve through redundancy, having a backup or secondary copy of every single component in the infrastructure.

Benefits of high availability

With enterprises relying more than ever on online services and cloud and hybrid cloud architectures to deliver critical applications and services, infrastructure demands are rising, making high availability a priority.

Here are some of the most common enterprise benefits of highly available systems.

Increased flexibility

With digital transformation a key objective for most companies, high availability of systems is critical to giving employees and customers unlimited access to critical applications.

Secure data with a high availability architecture, organizations' most important data is always available, accessible, and protected from unauthorized breaches

Improved brand reputation. System failures that cause hours or even minutes of downtime can cause public relations nightmares for enterprises across a broad range of industries, including SaaS, aviation, and mobile technology. High availability infrastructure ensures a brand's reputation doesn't suffer due to an outage or unexpected downtime.

Better customer service, Managed Service Providers (MSPs) must deliver high availability of networks or risk not fulfilling their service level agreements (SLAs). HA systems help MSPs deliver networks that their most valuable clients can depend on, like one that helps autonomous vehicles drive safely or a healthcare facility manage patient records.

Read more →

Galaxy enables organizations to achieve high availability by building resilient, always-on IT systems that minimize downtime and ensure seamless business continuity. Our approach leverages robust infrastructure design, redundancy, and proactive monitoring to keep critical applications accessible, secure, and reliable—helping businesses enhance customer experience, protect data, and maintain operational excellence in a digital-first world.

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

SPECIAL FOCUS

Ransomware Evolution : How to Stay Protected in Modern Cybersecurity

Ransomware has emerged as one of the most disruptive and financially damaging cyber threats in the modern digital landscape. It is a type of malicious software (malware) designed to block access to systems, data, or networks until a ransom is paid. Over the past decade, ransomware has evolved from simple, opportunistic attacks into highly sophisticated, targeted campaigns run by organized cybercriminal groups.

With businesses increasingly relying on digital infrastructure, ransomware attacks now pose a serious risk to operational continuity, financial stability, and brand reputation. Understanding its evolution is critical to building effective cybersecurity defences

2. Evolution of Ransomware

2.1 Early Stage: Basic Encryption Attacks

The first known ransomware attack, the AIDS Trojan (1989), was distributed via floppy disks and demanded payment via postal mail. Early ransomware variants were relatively unsophisticated:

2.2 Crypto-Ransomware Emergence

With advancements in cryptography and the rise of digital payments, ransomware became more dangerous.

2.3 Ransomware-as-a-Service (RaaS)

Ransomware evolved into a service-based model where developers created ransomware kits and leased them to affiliates.

2.4 Targeted and Enterprise Attacks

Attackers shifted from mass attacks to targeted, high-value organizations such as enterprises, hospitals, and government bodies.

Common Ransomware Attack Vectors
Understanding how ransomware enters an organization is essential for prevention:

1. Phishing Emails
2. Remote Desktop Protocol (RDP) Exploits
3. Software Vulnerabilities
4. Supply Chain Attacks
5. Insider Threats. Impact of Ransomware

Ransomware can have severe consequences

5.1 Preventive Measures

a. Email Security
b. Endpoint Protection
c. Patch Management
d. Network Segmentation (Micro segmentation)
e. Secure Remote Access

5.2 Detection and Response

a. Security Monitoring
b. Threat Intelligence
c. Incident Response Plan

5.3 Data Protection and Recovery

a. Regular Backups

b. Disaster Recovery Planning

5.4 Advanced Security Approaches

a. Zero Trust Architecture

b. Secure Access Service Edge (SASE)

c. Data Loss Prevention (DLP)

d. Extended Detection and Response (XDR)

6. Best Practices for Organizations

- **Conduct regular security awareness training for employees**
- **Perform vulnerability assessments and penetration testing**
- **Align with frameworks like NIST, ISO 27001, and CIS Controls**
- **Partner with Managed Security Service Providers (MSSP)**

GALAXY helps you prevent, detect, respond to, and recover from ransomware through a fully integrated, 24x7 cybersecurity ecosystem.

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

TECH NEWS

OpenAI's U.S. ad pilot exceeds $100 million in annualised revenue in six weeks

OpenAI's ChatGPT ads pilot in the United States has crossed the $100 million annualised revenue mark within six weeks of launch, a company spokesperson said on Thursday, pointing to robust early demand for the AI startup's nascent advertising business.

Sam Altman-led OpenAI had said in January that it would start showing ads in ChatGPT to some U.S. users, ramping up efforts to generate revenue from the AI chatbot to fund the high costs of developing the technology. The ads were to be tested with users on the company's free tier and the lower-priced Go plan.

The ads are separate from the answers generated by ChatGPT and do not influence its outputs. User conversations are not shared with marketers, the company said at the time.

While roughly 85% of users are currently eligible to see ads, fewer than 20% are shown ads daily,

with considerable room to grow ad monetization within the existing user pool, the spokesperson said.

"We're seeing no impact on consumer trust metrics, low dismissal rates of ads, and ongoing improvements in the relevance of ads as we learn from feedback," OpenAI said.

The company plans to expand the test globally in additional countries in the coming weeks, including in Australia, New Zealand, and Canada.

OpenAI has now expanded to over 600 advertisers, with nearly 80% of small- and medium-sized businesses signalling interest in ChatGPT ads, the spokesperson said.

The ChatGPT maker is set to launch self-serve advertiser capabilities in April to broaden access and drive further growth.

David Dugan, a former Meta ads executive, was named to lead OpenAI's global advertising solutions team earlier this week.

Analysts said that ads could unlock a significant revenue stream from millions of ChatGPT users, but the move could irk some customers and hurt trust in the product.

Read more →

TECH NEWS

Meta Invests $10 Billion in Texas to Power Its AI Future

Meta said on Thursday it is increasing investment in its El Paso, Texas AI data center to $10 billion, a more than sixfold jump, as it aims to hit 1-gigawatt capacity ahead of the facility's projected opening in 2028.

The social media giant in October had committed an investment of $1.5 billion in the El Paso data centre, its 29th such facility globally and third in Texas.
Big Tech firms such as Meta, Amazon, Alphabet, and Microsoft have been racing to build AI infrastructure and are projected to spend over $630 billion on AI infrastructure this year.

The El Paso facility will lead to the creation of 300 new jobs once operational, with over 3,000 construction workers expected on-site at peak construction, Meta said in a blog.
Meta also said it has projects under contract that are adding more than 5,000 megawatts of clean energy to the grid in Texas and will ease the water burden by working with specialized nonprofits to bring fresh water to the area.

The company laid off a few hundred people across multiple teams on Wednesday, following an earlier Reuters report about Meta planning sweeping layoffs that could affect 20% or more of its workforce.
Its shares dropped on Thursday after two verdicts holding it liable for harm to young users sparked fears Meta may have to overhaul the design practices that have underpinned its sprawling advertising business.

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