GALAXY
Integrating Technology | Driving Growth

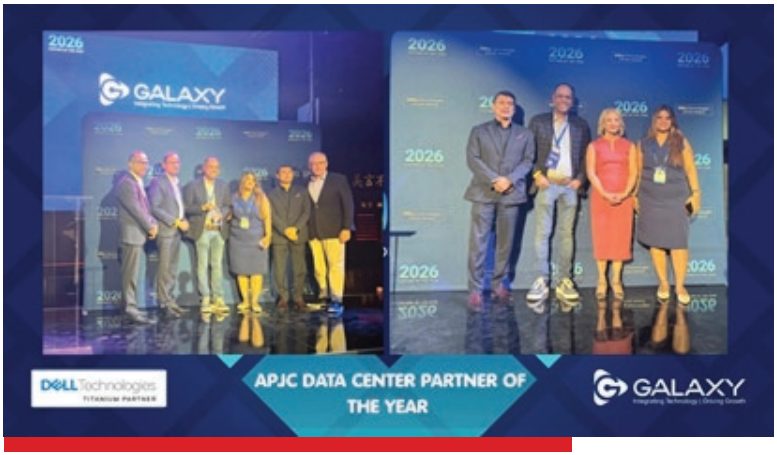
TECH TALK

Issue 168
June 2026

Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.



We are proud to announce that Galaxy has been honoured with the Dell Technologies – APJC Data Center Partner of the Year Award at Dell Technologies World 2026.

This achievement reflects our continued commitment to delivering innovative, reliable, and future-ready data center solutions that empower enterprises across industries to transform and grow with confidence.

The recognition reinforces our dedication to excellence, strong customer relationships, and our vision of driving digital transformation through advanced technology solutions.

We extend our sincere gratitude to Dell Technologies, our valued customers, partners, and the incredible Galaxy team for their continued trust and support in making this milestone possible.

Here's to achieving many more milestones together.

Foreword

Dear Readers,

As we move deeper into 2026, the conversation around enterprise AI is evolving rapidly. Last year, organisations were experimenting with copilots and generative AI assistants. Today, the leaders are moving beyond assistance toward autonomy. Agentic AI represents the next major transformation in how enterprises operate. Unlike traditional AI systems that wait for prompts or human direction, AI agents can independently analyse situations, make decisions, coordinate actions across systems, and continuously learn from outcomes. In practical terms, this means enterprises are beginning to deploy digital operators rather than digital tools.

At Galaxy, we see Agentic AI as the next evolution of intelligent enterprise operations and are already building AI agents to assist our SOC and NOC teams in the following areas:

IT and Service Operations: AI agents are beginning to act as autonomous operational coordinators. Incident triage, root cause analysis, escalation management, and remediation workflows are becoming increasingly self-directed.

Cybersecurity: Agentic AI is enabling continuous threat hunting, automated investigation chains, adaptive policy enforcement, and significantly faster response cycles. Security teams are gaining the ability to scale without proportionally increasing operational overhead.

Cloud and Governance: Intelligent governance agents continuously validate configurations, monitor compliance posture, enforce policy-as-code controls, and optimise cloud resource utilisation in real time. Governance is evolving from periodic assessment into an always-on operational discipline.

Through our AI, Security, Network, and Cloud expertise, we are helping organisations move beyond experimentation toward production-ready autonomous operations.

Foreword

It is important to note that Agentic AI introduces new challenges that enterprises cannot afford to ignore. A few examples are conflicting decision handling, audibility and agent sprawl. Addressing these challenges demands not just better models, but new frameworks for agent identity, inter-agent coordination, and continuous verification of agent behaviour against human-defined policies. Our focus is not simply on deploying AI models but on engineering governed, secure, enterprise-grade agent ecosystems that integrate seamlessly with existing operational environments.

The organisations that succeed will treat agentic autonomy as an engineering discipline, not just an AI feature, to operationalise autonomous intelligence across the core of their business.

I invite you to connect with our experts and evangelists for a focused discussion on how Agentic AI can accelerate operational resilience, strengthen governance, and unlock the next stage of enterprise transformation for your organisation.

Happy reading!

Anoop Pai Dhungat
Chairman & Managing Director

A chip the size of a palm that gives spacecraft a brain of their own

Small enough to fit in the palm of a hand, NASA's High Performance Spaceflight Computing processor packs the power of a full system-on-a-chip. This next-generation processor is made to survive deep space while delivering a massive leap in computational speed compared to current spacecraft technology.

NASA is developing a powerful new computer chip designed to dramatically increase the intelligence and performance of future spacecraft. Through a commercial partnership, the project is creating advanced processing technology capable of helping spacecraft operate more independently during missions far from Earth.

NASA's High Performance Spaceflight Computing project is focused on boosting the computing capabilities of spacecraft used in space exploration. Current missions rely on older processors because they are durable enough to survive the extreme conditions of space.

While those chips are dependable, they lack the performance needed for more advanced missions. The agency says newer and far more capable processors are essential for future autonomous spacecraft, faster onboard scientific analysis, and supporting astronauts during missions to the Moon and Mars.

"Building on the legacy of previous space processors, this new multicore system is fault-tolerant, flexible, and extremely high-performing," said Eugene Schwanbeck, program element manager in NASA's Game Changing Development program at the agency's Langley Research Center, in Hampton, Virginia. "NASA's commitment to advancing spaceflight computing is a triumph of technical achievement and collaboration."

Radiation Hardened Processor Faces Extreme Testing

At the center of the project is a new radiation-hardened processor built to deliver up to 100 times the computing power of today's spaceflight computers while surviving the harsh environment of space. Engineers at NASA's Jet Propulsion Laboratory (JPL) in Southern California are running a wide range of tests designed to simulate those conditions.

"We are putting these new chips through the wringer by carrying out radiation, thermal, and shock tests while also evaluating their performance through a rigorous functional test campaign," said Jim Butler, High Performance Space Computing project manager at JPL.

To qualify for spaceflight, the processor must withstand intense electromagnetic radiation and dramatic temperature fluctuations that can damage electronics. High-energy particles from the Sun and deep space can also trigger computer errors that force spacecraft into "safe mode," temporarily shutting down nonessential systems until engineers resolve the issue.

NASA is also testing how the chip handles the challenges of planetary landings.

"To simulate real-world performance, we are using high-fidelity landing scenarios from real NASA missions that would typically require power-intensive hardware to process huge volumes of landing-sensor data," said Butler. "This is an exciting time for us to be working on hardware that will enable NASA's next giant leaps."

Testing at JPL began in February and is expected to continue for several months. Early results have been highly encouraging. According to NASA, the processor is functioning as intended and has shown performance levels roughly 500 times greater than the radiation-hardened chips currently used in spacecraft. The team also marked the beginning of testing with a symbolic moment by sending an email titled "Hello Universe," referencing the famous introductory messages used during the early days of computer programming.

Read more →

TECHNOLOGY FOCUS

Inside the Security Operations Center (SOC): Your Frontline Defence Against Cyber Threats

A security operations center (SOC) improves an organization's threat detection, response, and prevention capabilities by unifying and coordinating all cybersecurity technologies and operations.

A SOC—usually pronounced "sock" and sometimes called an information security operations center, or ISOC—is an in-house or outsourced team of IT security professionals dedicated to monitoring an organization's entire IT infrastructure 24x7. Its mission is to detect, analyse, and respond to security incidents in real-time. This orchestration of cybersecurity functions allows the SOC team to maintain vigilance over the organization's networks, systems, and applications and ensures a proactive Defence posture against cyber threats.

The SOC also selects, operates, and maintains the organization's cybersecurity technologies and continually analyses threat data to find ways to improve the organization's security posture.

When not on premises, a SOC is often part of outsourced managed security services (MSS) offered by a managed security service provider (MSSP). The chief benefit of operating or outsourcing a SOC is that it unifies and coordinates an organization's security system, including its security tools, practices, and response to security incidents. This usually results in improved preventative measures and security policies, faster threat detection, and faster, more effective, and more cost-effective response to security threats. A SOC can also improve customer confidence and simplify and strengthen an organization's compliance with industry, national, and global privacy regulations.

What a security operations center (SOC) does

Preparation, planning, and prevention

Asset inventory: A SOC needs to maintain an exhaustive inventory of everything that needs to be protected, inside or outside the data center (for example applications, databases, servers, cloud services, endpoints, etc.) and all the tools used to protect them (firewalls, antivirus/anti-malware/anti-ransomware tools, monitoring software, etc.). Many SOCs will use an asset discovery solution for this task.

Incident response planning: The SOC is responsible for developing the organization's incident response plan, which defines activities, roles, and responsibilities in the event of a threat or incident, and the metrics by which the success of any incident response will be measured.

Regular testing: The SOC team performs vulnerability assessments—comprehensive assessments that identify each resource's vulnerability to potential or emerging threats and the associated costs. It also conducts penetration tests that simulate specific attacks on one or more systems. The team remediates or fine-tunes applications, security policies, best practices, and incident response plans based on the results of these tests.

Staying current: The SOC stays up to date on the latest security solutions and technologies, and on the latest threat intelligence—news and information about cyberattacks and the hackers who perpetrate them, gathered from social media, industry sources, and the dark web.

Read more →

We at Galaxy specialize in delivering Managed SOC Services that help enterprises stay secure and compliant through cost-effective, 24/7 threat monitoring and rapid incident response.

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

SPECIAL FOCUS

Strengthen Cybersecurity with Intelligent Network Detection & Response (NDR)

In today's rapidly evolving cybersecurity landscape, organizations are facing increasingly sophisticated cyber threats such as ransomware attacks, insider threats, zero-day vulnerabilities, Advanced Persistent Threats (APTs), and lateral movement within enterprise networks. Traditional security solutions such as Firewalls, Antivirus, and Intrusion Prevention Systems (IPS) are essential security components, but they are often limited in detecting advanced threats that operate inside the network after bypassing perimeter defences.

To address these challenges, organizations are adopting Network Detection & Response (NDR) solutions as an advanced security layer to provide deep network visibility, behavioural analytics, real-time threat detection, and automated incident response capabilities.

NDR Architecture and Working Principle

- **Traffic collection methods (SPAN, TAP, Cloud Sensors)**
- **Packet inspection and metadata analysis**
- **AI/ML-based analytics engine**
- **Threat intelligence integration**
- **Detection and response workflow**

Key Features OF NDR

- **Continuous Network Monitoring**
- **AI & Machine Learning-Based Detection**
- **Behavioural Analytics**
- **Real-Time Threat Detection**
- **East-West Traffic Visibility**
- **Encrypted Traffic Analysis**
- **Threat Intelligence Integration**

Benefits of NDR

- **Improved network visibility**
- **Faster threat detection and response**
- **Reduced Mean Time to Detect (MTTD)**
- **Reduced Mean Time to Respond (MTTR)**
- **AI-driven anomaly detection**
- **Enhanced SOC efficiency**

Use Cases of NDR

- **Ransomware Detection & Prevention**
- **Lateral Movement Detection**
- **Insider Threat Detection**
- **Zero-Day Threat Detection**
- **hreat Hunting & Incident Investigation**
- **Cloud & Hybrid Network Monitoring**
- **Remote User & VPN Monitoring**
- **Automated Threat Response & Containment**

Why NDR is required in a modern environment

NDR is needed in modern environments to provide complete network visibility and detect advanced cyber threats that traditional security solutions may miss. It helps organizations identify ransomware,

insider threats, lateral movement, and suspicious network behaviour in real time.

By using AI/ML-based analytics, NDR improves threat detection and accelerates incident response. It also supports cloud, hybrid, IoT, and remote work environments while enhancing overall SOC efficiency and cybersecurity posture.

Galaxy helps organizations strengthen their cybersecurity posture with advanced Network Detection & Response (NDR) solutions that provide real-time visibility, AI-powered threat detection, and faster incident response. Our solutions help detect ransomware, insider threats, malware communication, and suspicious network activities that traditional tools may miss. With seamless integration across Firewall, SIEM, SOC, and XDR platforms, Galaxy enables businesses to reduce cyber risk and secure their on-premises, cloud, and hybrid IT environments.

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

TECH NEWS

Meta eyes AI pendant as part of its ambitious new hardware strategy

Meta Platforms is preparing a broader push into AI-focused consumer hardware. A new internal memo reportedly outlines plans that include smart wearables, upgraded AI devices, and a possible artificial intelligence (AI)-powered pendant.

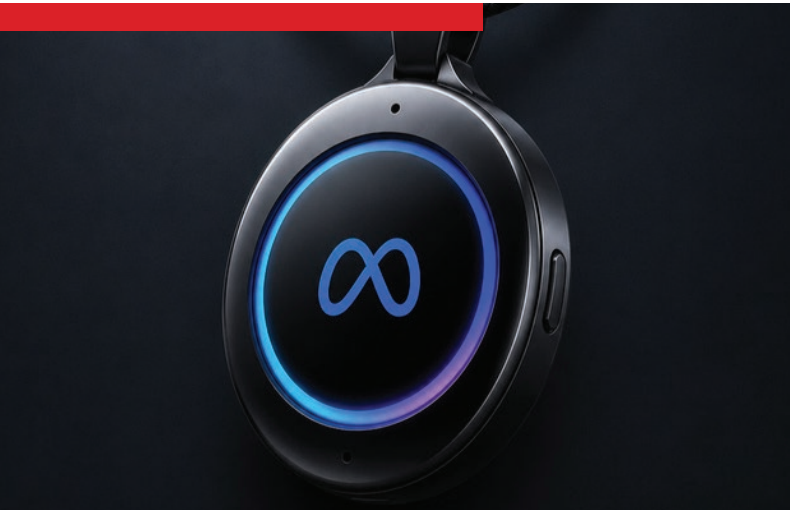
According to a report by The Information, the memo details Meta's long-term hardware strategy as the company seeks to position itself at the centre of the rapidly growing AI ecosystem. The plans suggest Meta is exploring more personalised and persistent AI experiences through its wearable devices.

One of the most notable products mentioned in the memo is an AI pendant, a wearable device that could function as a voice-based digital assistant worn around the neck. While technical details remain unclear, the report says the device is expected to focus on voice-based AI interactions. It remains unclear whether it will include cameras or other sensors.

The roadmap also aims to improve the performance of Meta's loss-making Reality Labs hardware division. The memo also reportedly mentions a business-focused initiative called 'Wearables for Work', aimed at enterprise customers. This development comes amid a growing industry trend in which tech giants are researching AI-based hardware beyond mobile phones. Screenless personal assistants, wearables with AI functionality, and AI-driven multimodal user interfaces are some trends the operating companies are exploring.

The company is also continuing to expand its AI infrastructure and assistant capabilities across its apps, smart glasses, and future devices as competition intensifies with rivals including OpenAI, Google, and Apple. While Meta has not officially commented on the report or announced a launch timeline for the reported AI pendant, the memo suggests the company is accelerating development of AI-centric hardware designed to make digital assistants more personal, portable, and continuously accessible.

Meta has a long history of investing in AI and wearable technology. For instance, Meta has developed Ray-Ban Meta glasses that use a camera, speaker, and voice functionality along with an AI assistant capability. Mark Zuckerberg has repeatedly highlighted AI-powered wearables, smart glasses, augmented reality (AR), and virtual reality (VR) as key parts of Meta's long-term computing strategy.



Read more →

TECH NEWS

NVIDIA says its forecast for the $200 billion CPU market includes China

Nvidia CEO Jensen Huang said on Saturday that his forecast of a $200 billion market for CPUs includes China, signalling Nvidia still sees significant long-term demand in the market amid ongoing U.S.-China technology tensions.
Central processing units have taken centre stage as companies and businesses gravitate towards agentic AI – systems that perform autonomous functions – broadening demand beyond graphics processing units, or GPUs, that are used to train large models.
Huang on Wednesday aimed to assure investors that the world's most valuable company can keep up its blockbuster growth with the help of a broad base of customers and that new products will help it beat the $1 trillion in sales it has forecast for its flagship AI chips.
During earnings call on Wednesday, Huang said Nvidia's new "Vera" central processors give it access to a new $200 billion market.
Speaking to reporters upon arrival in Taipei on Saturday and asked if that forecast included China, he said: "I would think so." H200 chips Nvidia has received licenses from the U.S. government to sell its H200 chips but has not received approval from Chinese officials who are fostering China's own chip suppliers.
U.S. President Donald Trump's talks with Chinese President Xi Jinping in Beijing this month produced no immediate breakthrough for Nvidia to sell H200 chips. Huang was also there as part of the U.S. delegation

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