GALAXY
Integrating Technology | Driving Growth

TECH TALK

Issue 157 July 2025

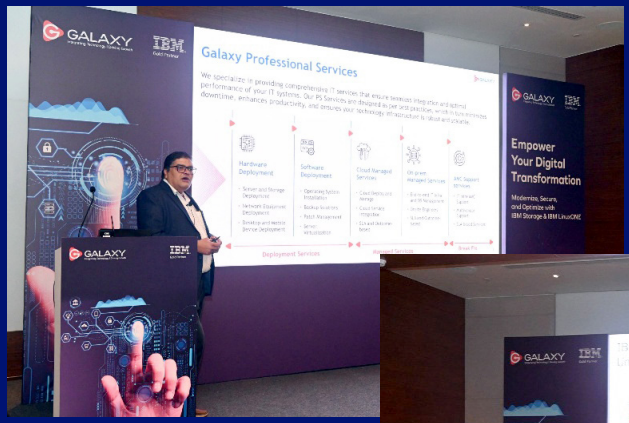
Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.

Galaxy and IBM hosted an exclusive **Digital Transformation Networking Session,** spotlighting the future of modern IT infrastructure with secure, efficient, and AI-powered solutions.

Attendees explored how **IBM Storage** and I**BM LinuxONE** are driving enterprise resilience through innovation, cybersecurity, and trusted AI. The event featured real-world insights, expert discussions, and bold strategies to modernize, secure, and optimize digital ecosystems.



Foreword

Dear Readers,

The recent events in the Middle East have reinforced our belief that the use of AI in military settings is more than just a technological upgrade; it signifies a major change in how military plans are made, executed, and assessed. AI-powered systems provide incredible new abilities in handling data, identifying threats, and planning strategies, allowing military units to respond quickly and accurately to new dangers.

Artificial intelligence includes a range of technologies such as machine learning, neural networks, natural language processing, computer vision, and robotics. In military use, these technologies help improve efficiency, support better decision-making, and lower the risks faced by humans.

AI plays a big role in military applications like autonomous weapons, target recognition, surveillance and reconnaissance, cybersecurity and defence, improving military logistics and transportation, combat training and simulation, and many others.

Although AI provides significant benefits for military use, it also introduces ethical issues and potential risks. The deployment of autonomous weapons raises concerns about accountability, transparency, and compliance with international humanitarian laws. Maintaining human oversight and ethical judgment is essential to prevent unintended harm.

The future of AI in military operations promises continued innovation and integration across various domains. Emerging technologies, such as quantum computing and advanced neural networks, will further enhance AI capabilities, enabling more sophisticated and effective military applications. As AI technologies evolve, military forces must adapt and develop comprehensive strategies to leverage AI effectively and responsibly.

I can only hope and pray that the use of AI in such military applications will reduce the collateral damage caused to innocent civilians and civilian infrastructure.

Galaxy has developed a range of non-military, AI-driven, outcome-based solutions for a number of industries. Do reach out to us with your pain points or challenges, and our experts can explore developing a solution to those.

Happy reading!

Anoop Pai Dhungat
Chairman & Managing Director

Future is now!

Vision Redefined:
How Nanotech Contact Lenses Could Transform Human Perception and Workplace Technology.

Humans can now see in the dark—and even with their eyes closed—using nanotechnology contact lenses that turn invisible infrared light into visible images, according to a new study published in the journal Cell.

After first testing in mice, scientists from China and the University of Massachusetts Chan Medical School created contact lenses for humans infused with specialized "nanoparticles", thousands of times smaller than a grain of sand, that let people see in the dark and in foggy conditions.

These nanoparticles are scattered throughout the soft lens material, where they absorb infrared light and convert it into images the human eye normally can't see.

Gang Han, the study's lead author and a Ph.D.-level nanoparticle researcher at UMass Chan Medical School, told ABC News the lenses enhance how someone sees colour.

"When wearing them, you still see everything normally," Hans said. "The lenses simply add the ability to see infrared images on top of what we already normally see."

Wearing the lenses, participants were able to recognize coded flashes of infrared light—similar to Morse code—identify basic shapes and patterns, and even distinguish colours in the infrared range, effectively adding a new dimension to human vision, Han explained.

They could even perceive the images with their eyes closed, thanks to the ability of infrared light to pass through eyelids, he said.

Humans can naturally see only visible light, a small slice of the full light spectrum that includes invisible wavelengths like ultraviolet and infrared. Night vision goggles can detect infrared light, but they're bulky, often need a power source, and usually show images in green or black and white, Han said.

"What's special about our contact lenses is that they let you see infrared light in colour—like red, green, and blue—so you can tell different things apart more easily," Han emphasized.

So far, the lenses have only been tested on a small group of individuals in China, all with normal vision.

Han said the researchers now need to test them in a more diverse population, including people with different vision capabilities.

"While we haven't specifically studied these lenses for people with vision impairments or eye diseases, this is an important area we hope to explore in the future," he said, adding that there needs to be further assessment to test their safety and spot any long-term effects on the eye.

Advances in nanotechnology could bring everyday benefits, especially for first responders.

"Our lenses help rescuers see clearly and navigate safely in dangerous environments like fires or dense fog," he said.

Doctors already use infrared technology to highlight tumors treated with special dyes visible to infrared cameras. Han noted that the new lenses could enhance this approach by allowing surgeons to see near-infrared signals directly in their line of sight, without needing to glance at separate monitors.

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, analyze, 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 analyzes 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 responses 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.

Routine maintenance and preparation

To maximize the effectiveness of security tools and measures in place, the SOC performs preventive maintenance such as applying software patches and upgrades and continually updating firewalls, allow lists and blocklists, and security policies and procedures. The SOC can also create system backups—or assist in creating backup policies or procedures—to ensure business continuity in the event of a data breach, ransomware attack, or other cybersecurity incident.

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 →

SPECIAL FOCUS

Guarding the Gateways: Why API Security Matters More Than Ever

APIs (Application Programming Interfaces) are critical components of modern applications, enabling seamless integration between services, applications, and platforms. However, they also present significant security challenges, making API security a top priority for organizations. API security solutions protect APIs from threats such as unauthorized access, data breaches, and malicious attacks.

Key Features

Authentication and Authorization

- Enforces strong authentication mechanisms (OAuth 2.0, JWT, API keys).
- Implements role-based and attribute-based access control (RBAC & ABAC).
- Integrates with Identity and Access Management (IAM) solutions.

Threat Detection and Mitigation

- Identifies and blocks API-specific attacks such as injections, denial-of-service (DoS), and credential stuffing.
- Detects anomalous behaviour using AI-driven analytics.
- Prevents abuse through rate limiting and throttling.

Secure Data Transmission

- Encrypts API traffic using TLS 1.2/1.3.
- Prevents data leakage through payload inspection.
- Ensures compliance with data protection regulations (GDPR, HIPAA, PCI-DSS).

API Gateway and Firewall Protection

- Provides centralized control and monitoring for API traffic.
- Filters and blocks malicious requests before they reach backend services.
- Supports WAF (Web Application Firewall) integration.

Visibility and Monitoring

- Offers real-time API traffic analysis and logging.
- Provides centralized dashboards for security insights.
- Supports integration with SIEM (Security Information and Event Management) platforms.

Zero Trust API Security

- Enforces continuous validation of API requests.
- Restrict access based on dynamic risk assessments.
- Implement micro-segmentation for API endpoints.

Security Testing and Compliance

- Conducts automated API security testing.
- Identifies vulnerabilities through penetration testing and fuzzing.
- Ensures compliance with Open API and other industry standards.

Business Benefits

Enhanced Protection

Prevents unauthorized access and data breaches.

Regulatory Compliance

Helps meet security and privacy regulations.

Improved API Performance

Reduces attack impact through rate limiting and filtering.

Operational Efficiency

Automates security enforcement and monitoring.

Scalability

Adapts to dynamic API traffic and business growth.

Increased Trust and Reliability

Ensures secure API interactions, enhancing user confidence.

Reduced Costs

Lowers incident response and recovery expenses by preventing security breaches.

We at Galaxy specialize in implementing API security solutions that enable enterprise customers to become compliance-ready in a cost-effective and secure manner.

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

TECH NEWS

Tech Trend Alert: **Gartner Predicts Major Setback for Agentic AI Projects**

A new report from Gartner has stated that more than 40% of agentic AI projects will be cancelled by the end of 2027 due to growing costs, elusive business value, and insufficient security. The survey conducted in January 2025 polled 3,412 webinar attendees.

The study also revealed that 19% of the organizations had made significant investments in agentic AI, 42% had made conservative investments, 8% had no investments, while the remaining 31% were taking a wait-and-see approach or were on the fence.

"Most agentic AI projects right now are early-stage experiments or proofs of concept that are mostly driven by hype and are often misapplied," said Anushree Verma, Senior Director Analyst, Gartner. "This can blind organizations to the real cost and complexity of deploying AI agents at scale, stalling projects from moving into production. They need to cut through the hype to make careful, strategic decisions about where and how they apply this emerging technology."

Most vendors were party to what the report called "agent washing," which was to market their existing products like AI assistants or robotic process automation (RPA) tools and chatbots as AI agents. The report estimated that around 130 of the thousands of agentic AI vendors were of substance.

Read more →

TECH NEWS

Meet Gemini: **Google's On-Device AI Model That Brings Robots to Life**

Google's DeepMind division released a new large language model called Gemini Robotics On-Device that runs locally on robotic devices. In a blog post, Google says that the new AI model has been optimized to efficiently run on the robot and shows "strong general-purpose dexterity and task generalization."

The new offline AI model builds on the company's Gemini Robotics model, which the tech giant unveiled earlier this year in March. The Gemini Robotics On-Device model can control a robot's movement and, like ChatGPT, can understand natural language prompts. Since it works without an active internet connection, Google says it is really useful for latency-sensitive applications or in areas where there is zero connectivity.

Designed for robots with two arms, Google explains that Gemini Robotics On-Device is engineered in such a way that it requires "minimal computational resources" and can complete highly dexterous tasks like folding clothes and unzipping bags, to name a few.

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