GALAXY
Integrating Technology | Driving Growth

TECH TALK

Issue 167
May 2026

Pioneering Tech Leadership with a Legacy of Excellence.

AIM

Galaxy Office Automation Pvt. Ltd.

Galaxy hosted an exclusive technology session in collaboration with Dell Technologies for our valued customers.

The session featured insightful discussions on private cloud, cyber resilience, and AI infrastructure, focusing on building future-ready enterprise IT environments.

It was a great platform to exchange ideas, understand evolving business needs, and explore scalable, secure, and intelligent technology solutions.

Thank you to everyone who joined us and made the session engaging and impactful.

Looking forward to driving more value through strong partnerships and customer-centric innovation.

Foreword

Dear Readers,

As we step into the second quarter of 2026, one of our boldest predictions from January is already proving itself. Hyperautomation is reshaping enterprises faster than most anticipated, and the organisations that leaned in early are already pulling ahead. Hyperautomation accelerates complex work by automating end-to-end processes, reducing labor productivity costs by up to 70% in some cases. In fact, Gartner predicts that through the combination of hyperautomation technologies and redesigned operational processes, enterprises will cut operational expenses by at least 30%.

At the start of this year, we predicted that Hyperautomation would extend well beyond the back office to span IT operations, security, and governance. Four months in, that prediction has become a reality for our most forward-thinking clients. Today, we want to go deeper into what Hyperautomation actually looks like when it lands inside a real enterprise.

The first wave of automation gave us scripts and schedulers. The second gave us RPA bots that mimicked human keystrokes. Hyperautomation is the third wave and it is categorically different. It is the orchestration of AI, machine learning, process mining, and intelligent agents working in concert, not in silos. The distinguishing feature is self-awareness: Hyperautomation systems do not just execute tasks. They discover, prioritise, and continuously improve the processes they run.

In practical terms, this means AI-driven runbooks that self-execute when anomalies are detected, compliance evidence that is collected and catalogued without a single human touchpoint, and cloud remediation that fires before a ticket is even raised.

Across our client engagements this year, three domains are seeing transformational outcomes:

IT Operations : Mean time to resolution is collapsing. Intelligent event correlation is eliminating alert storms, and automated runbooks are handling L1 and L2 incidents end-to-end. Human engineers are being freed to focus on architecture and innovation rather than firefighting.

Foreword

Security and Compliance : Governance teams are under enormous pressure from regulators and boards alike. Hyperautomation is stepping in to handle continuous control monitoring, automated audit trail generation, and real-time policy enforcement. Compliance is transformed from a quarterly scramble into a continuous, ambient capability.

Network and Cloud Operations : Event-driven remediation is becoming the new baseline. Self-healing infrastructure, auto-scaling with cost guardrails, and policy-as-code pipelines are no longer aspirational. They are in production.

At Galaxy, we have used our vast experience and expertise in IT, Security, Network and Cloud operations and AI capabilities to develop two proprietary platforms based on Hyperautomation.

Auxhealium is an AI-powered L1 and L2 incident handling platform, drastically reducing mean time to detect and resolve.

Protaigo layers intelligent agent orchestration on top of your existing stack enabling hyperautomated security operations, compliance workflows, and governance pipelines without ripping and replacing what you have built.

We are not just advising on Hyperautomation. We are building it, integrating it, and assuring it.

The organisations that will define their industries in 2027 and beyond are making their Hyperautomation commitments today. The technology is mature, the use cases are proven, and the competitive gap between leaders and laggards is widening with every quarter.

We invite you to reach out to our experts and evangelists for a focused conversation on where Hyperautomation can deliver the most value for your business and how Galaxy can get you there, faster and with confidence.

Happy reading!

Anoop Pai Dhungat
Chairman & Managing Director

AI Hallucination Risks Drive Demand for New Insurance Solutions

Insurers at Lloyd's of London have introduced a new insurance product designed to protect businesses from financial losses arising from artificial intelligence system failures, according to a report by The Financial Times. The insurance, developed by Y Combinator-backed start-up Armilla, provides coverage for legal claims against companies when AI tools generate inaccurate outputs.

The policy offers financial protection against potential legal consequences, including court-awarded damages and associated legal expenses. It responds to rising concerns over AI's tendency to produce unreliable or misleading information—commonly referred to as "hallucinations" in AI terminology.

As companies increasingly integrate AI tools to enhance efficiency, they also face growing risks from errors caused by flaws in AI models that lead to hallucinations or fabricated information. Last year, a tribunal ruled that Air Canada must honour a discount its customer service chatbot had wrongly offered.

What is an AI hallucination?

An AI hallucination occurs when an algorithm generates information that appears credible but is actually false or misleading. Computer scientists use the term to describe such errors, which have been seen in various AI tools.

These hallucinations can cause significant problems when AI is used in sensitive areas. While some errors are relatively harmless—such as a chatbot giving a wrong answer—others can have serious consequences. In high-stakes settings like legal cases or health insurance decisions, inaccuracies can severely impact people's lives.

Unlike systems that follow strict, human-defined rules, AI models operate based on statistical patterns and probabilities, which makes occasional errors inevitable. Though minor mistakes may not pose a big problem for most users, hallucinations become critical when dealing with legal, medical, or confidential business matters.

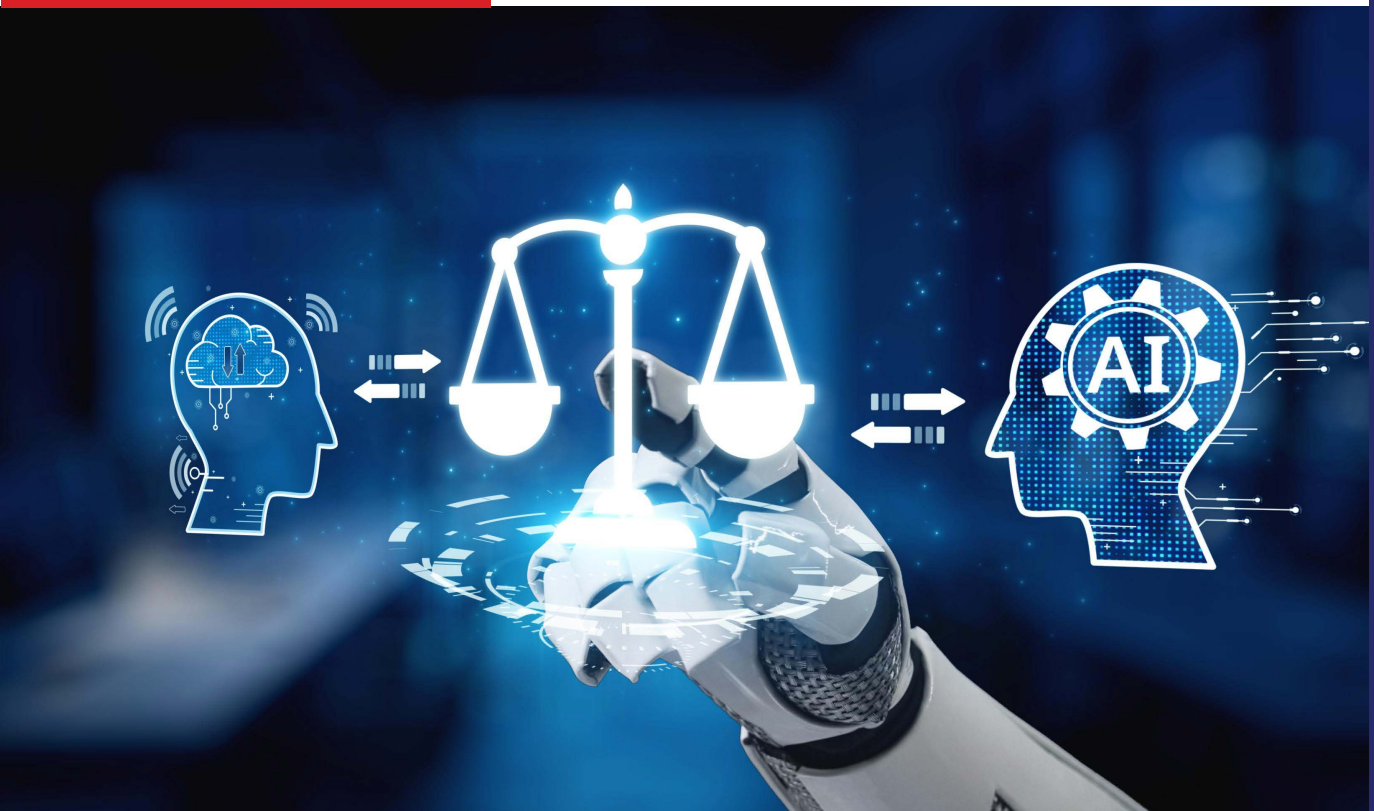
Karthik Ramakrishnan, Armilla's chief executive, said the new product could encourage more companies to adopt AI by addressing fears that tools like chatbots might break down or make errors.

Hallucinations getting worse despite AI advances

Despite improvements by companies like OpenAI and Google in reducing hallucination rates, the problem has worsened with the introduction of newer reasoning models. OpenAI's internal assessments found that its latest models hallucinate more often than earlier versions.

Specifically, OpenAI reported that its most advanced model, o3, produced hallucinations 33 per cent of the time on the PersonQA benchmark, which tests the ability to answer questions about public figures—more than double the rate of its earlier model.

Read more →



TECHNOLOGY FOCUS

Understanding Cloud Native DevOps: The Future of Software Delivery

Based on its name, cloud-native DevOps may seem to be the practice of running containerized applications in the cloud, but this definition is misleading. Instead, cloud-native DevOps is a method to structure your teams to take advantage of the automation and scalability that cloud-native technologies, such as containers and Kubernetes, offer—so you can increase the velocity of your business.

Understanding CNAs and DevOps

To properly define or explain cloud native DevOps, we must first understand cloud native apps (CNAs) and DevOps.

- CNAs are applications built for resiliency, agility, operability, and observability in mind.
- DevOps is a practice of operations and dev engineers working together throughout the entire lifecycle.

Based on both explanations, we can see that nothing is related to the cloud; they are simply principles and methodologies followed while working on a set of services or applications.Therefore, we can define cloud native DevOps as a set of practices that involves continuous improvement, automation, cross-functional teams, and better alignment with business needs, with customer expectations in mind. These principles apply to people, tools, culture, and process, not where the actual application lives (cloud or on-prem).

At its core, Cloud Native DevOps is a way to increase the velocity of your business and a method to structure your teams to take advantage of the automation and scalability that cloud native technologies like containers and Kubernetes offer. By nature, these cloud native technologies are designed to be:

- **Resilient.** Embracing failures instead of trying to prevent them, taking advantage of the dynamic nature of running on a platform.
- **Agile.** Allowing for fast deployments and quick iterations.
- **Operable.** Adding control of application life cycles from inside the application instead of relying on external processes and monitors.
- **Observable.** Providing information to answer questions about the application state

Changes needed to implement cloud native DevOps

To properly implement cloud native DevOps, changes must happen in three key areas:

1. **Cultural change from silos to proper DevOps.** As mentioned above, it is not necessary to run applications in the cloud in order to be cloud native, but DevOps is a must in order to practice cloud native. The goal of DevOps is to align everyone with the same tools and a common set of priorities.
2. **Organizational change involving buy-in from everyone to work in collaboration to achieve the same goal.** The idea is to encourage a faster feedback loop between developers and end users, which in turn speeds up application development and provides action items for the business.
3. **Technical change which relates to the way the application is built.** For example, moving from monolith to microservices.

Ways to implement cloud native DevOps

Implementing CNAs is not as straightforward as deploying into the cloud. To be considered cloud native, a CNA needs to meet certain characteristics:

- Aligning with the microservices patterns. Monolithic apps should be broken into small services that can be developed independently. As long as each service adheres to a strong contract, it can be iterated on. All these services comprise the application.
- Using containerization. Code can be packaged without worrying about the underlying system.
- Following declarative communication pattern. CNAs must trust that the network will deliver the message and that it will return either a success or a failure. This helps standardize a communication model, moving the functional implementation of how something achieves a desired state away from the application to a remote API or service endpoint.
- Deploying container orchestration. Perhaps the biggest orchestration platform out is Kubernetes, and for good reason. The biggest benefit of k8s is the fact that it abstracts away the details of underlying compute, storage, and networking resources.
- Writing code according to 12-factor application principles. This ensures clean, declarative contracts for cloud platform deployments.
- Increasing automation in CI/CD pipelines. Continuous integration and deployment are nothing new to cloud native, but the added complexity they bring means there must be extra automation in place to deal with the complexity of the pipelines.
- Exposing health check. This is great for knowing what is going on with the application. The application is telling the platform it is running on which state it is in, which in turn makes monitoring easier.
- Collecting telemetry data. Things like latency, requests per minute, etc., are information that is needed to determine whether you are meeting service level objectives (SLO). Telemetry data can and should be alerted on to consider your application cloud native.

Of course, cloud native DevOps is no silver bullet—it's just as important to be aware of the drawbacks as the benefits. Still, for companies looking to speed up automation and customize production to better serve customers, cloud native DevOps may be a useful tool.

Read more →

At Galaxy, we see Cloud Native DevOps as more than a tech shift—it's a strategy to boost agility, accelerate innovation, and empower teams through automation and scalable cloud-native technologies.

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

SPECIAL FOCUS

Beyond Protection: Rethinking Security with DSPM

Data Security Posture Management (DSPM) is an emerging cybersecurity approach designed to enhance the visibility, security, and governance of data across cloud and on-premise environments. With the increasing adoption of cloud computing and the proliferation of sensitive data, organizations face significant challenges in securing their data assets. DSPM provides a proactive and automated solution to mitigate data security risks.

Why DSPM is Required

1. **Growing Data Complexity:** Organizations store vast amounts of data across multiple environments, making manual security management inefficient.
2. **Regulatory Compliance:** Compliance standards such as GDPR, CCPA, HIPAA, and PCI-DSS require organizations to have robust data security measures in place.
3. **Cloud Security Gaps:** Cloud environments introduce new risks, such as misconfigurations, unauthorized access, and unintentional data exposure.
4. **Insider Threats:** Employees, contractors, or partners may have unintended or malicious access to sensitive data.
5. **Data Breaches:** Organizations need to proactively monitor, detect, and prevent data breaches before they occur.

Advantages and Benefits of DSPM

- **Automated Data Discovery & Classification:** DSPM solutions automatically identify and classify sensitive data across various storage locations, ensuring full visibility.
- **Risk Assessment & Continuous Monitoring:** Helps organizations detect vulnerabilities, misconfigurations, and unauthorized access attempts in real time.
- **Data Access Governance:** Ensures that only authorized users have access to sensitive data, reducing the risk of data leaks.
- **Incident Response & Remediation:** Provides actionable insights and automated remediation steps to mitigate security threats quickly.
- **Compliance & Audit Readiness:** Simplifies compliance reporting by continuously tracking security controls and generating audit logs.
- **Cost Savings & Efficiency:** Reduces the need for manual security assessments, lowering operational costs and improving efficiency.
- **Visibility in Highly Regulated Environments:** DSPM's ability to operate in air-gapped and on-premises environments ensures that sensitive data in highly regulated sectors is adequately protected.
- **Unified Policy Enforcement:** DSPM approaches simplified protection across all digital channels – including endpoints, cloud SaaS apps, web and email – in a single UI. This reduces complexity, minimizes management overhead and ensures consistent enforcement, providing comprehensive visibility and control oversensitive data, no matter where it resides.

Advantages and Benefits of DSPM

1. Cloud Data Security: Protecting sensitive data stored in AWS, Azure, and Google Cloud from misconfigurations and breaches. By leveraging automation, AI-driven risk detection, and continuous compliance monitoring, DSPM enables businesses to secure their cloud assets proactively and reduce cyber threats.
2. Regulatory Compliance Management: Ensuring organizations meet legal and industry compliance requirements effortlessly.
3. Shadow IT & Unstructured Data Management: Identifying and securing unauthorized or forgotten data repositories. Identifies sensitive data stored in unapproved applications, personal drives, or external servers.
4. Insider Threat Prevention: Monitoring and restricting excessive or unusual access to sensitive information. Insider threats are difficult to detect but DSPM provides a proactive security approach by continuously monitoring, analysing, and enforcing access controls, behavioral analytics, and automated incident response. By integrating DSPM into security strategies, organizations can reduce the risk of insider data breaches, ensure compliance, and safeguard sensitive information.
5. Data Loss Prevention (DLP): Preventing unauthorized data transfers and ensuring critical data remains within secure environments.
6. Third-Party Risk Management: Assessing and managing the risks associated with vendors and external collaborators accessing sensitive data. Data Security Posture Management (DSPM) helps organizations mitigate various security risks by providing visibility, automation, and proactive threat detection.

DSPM is a crucial component of modern cybersecurity strategies, helping organizations protect their data assets, ensure compliance, and mitigate evolving cyber threats.

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

TECH NEWS

Just a day after OpenAI made changes to its relationship with Microsoft, Amazon moves in; AWS CEO Matt Garman calls it

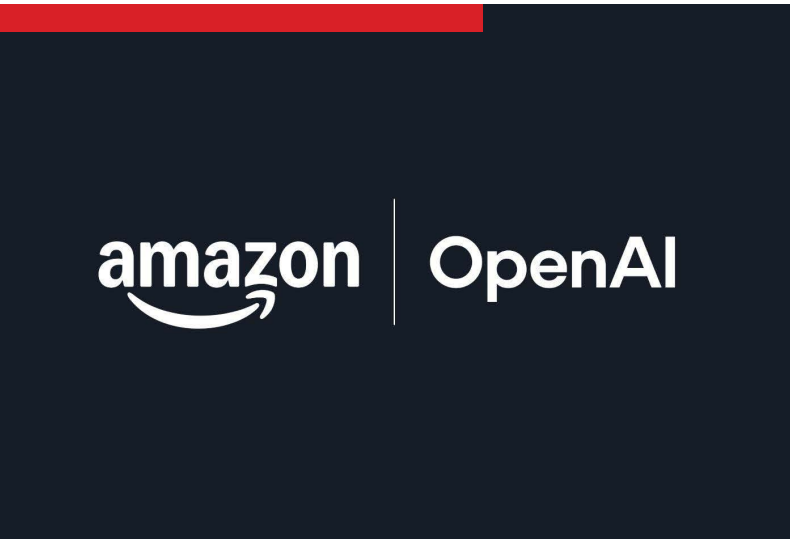
It almost took less than 24 hours, as in just one day, Amazon moved to capitalize on OpenAI's new relationship status with Microsoft. The Amazon Web Services (AWS) company launched a preview of OpenAI's models on its Bedrock platform. The announcement came just hours after the ChatGPT maker ended its exclusive cloud arrangement with Microsoft, one of its oldest and biggest partnerships. The companies reportedly described this as meeting years of customer demand.

According to a report in Geekwire, AWS CEO Matt Garman said at an event in San Francisco, "Their production applications run in AWS. Their data is in AWS. They trust the security of AWS, and we've forced them for the last couple of years, to get great OpenAI models, to go to other places."

OpenAI CEO Sam Altman too joined the event via recorded video, said, "The opportunity ahead of us is enormous, and the most exciting part is that this is not something in the future — it's starting right now."

Altman said that the collaboration with Amazon Web Services would involve co-developing a new platform for AI agents that can do computer-based work on people's behalf.

Amazon and OpenAI struck a $50 billion investment and cloud deal in February, with OpenAI committing to run workloads on Amazon's custom Trainium chips and the two companies agreeing to co-build what they called a "Stateful Runtime Environment" on Amazon's Bedrock platform. The cloud agreement alone is worth more than $100 billion over eight years.



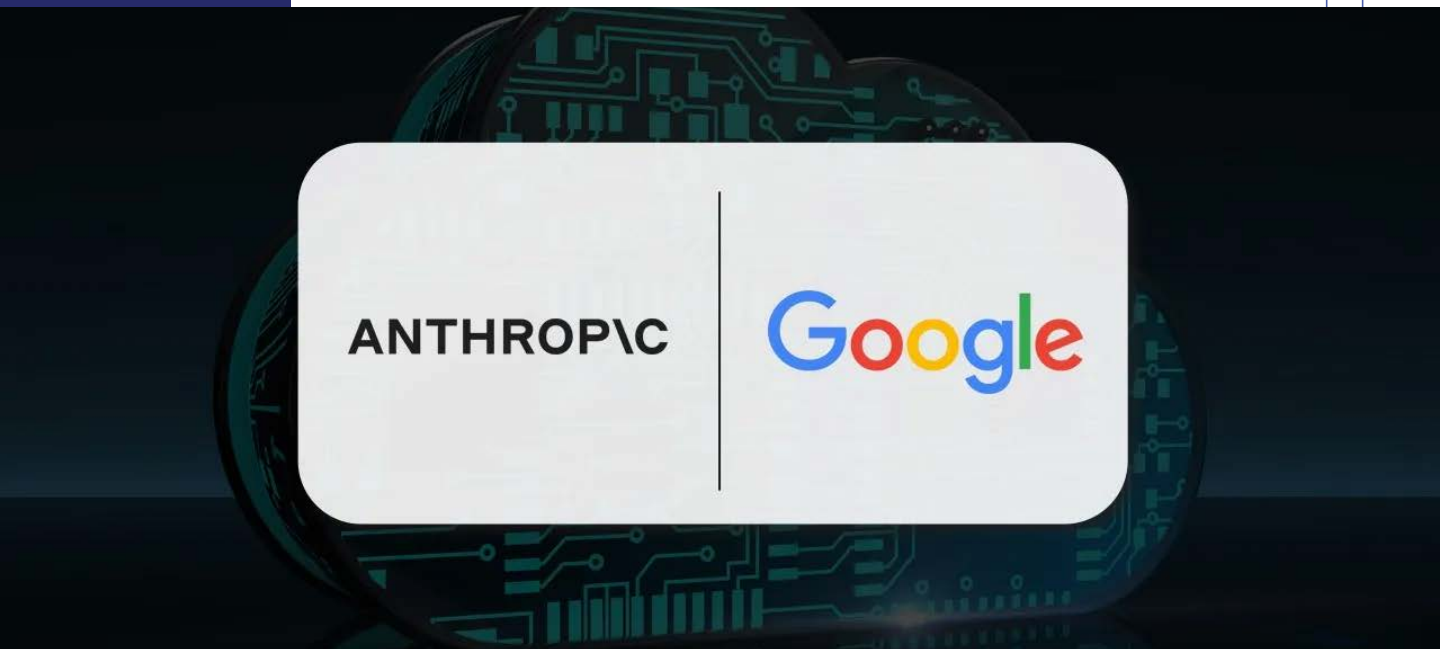
Read more →

TECH NEWS

Google to invest up to $40 billion in AI rival Anthropic

April 24 (Reuters) - Google-parent Alphabet (GOOGL.O) will invest up to $40 billion in Anthropic, as the tech giant deepens its partnership with the artificial intelligence startup that is also its rival in the global AI race. Anthropic said on Friday that Google has committed $10 billion now in cash at a valuation of $350 billion to help support a major expansion of its computing capacity, and will invest $30 billion more if the Claude maker meets performance targets. The investment comes just days after e-commerce giant Amazon (AMZN.O) said it will invest up to $25 billion in the startup, which has managed to stand out in the crowded AI industry
The startup raised $30 billion in a funding round in February that valued it at $380 billion post-money amid massive investor interest, and has drawn offers from venture capital firms valuing it at as much as $800 billion, according to media reports.

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