Integrating Technology, Driving Growth

TechTalk

GALAXY Integrating Technology | Driving Growth

SPEED UP

GALAXY OFFICE AUTOMATION PVT. LTD.

Issue No. 136, October 2023

We are thrilled to share that
Galaxy has been honoured as the

APJ CHANNEL PARTNER OF THE YEAR

by Check Point

This recognition is a testament to the dedication and hard work of our entire team.

MD SPEAKS

Anoop Pai Dhungat
Chairman & Managing Director

Dear Readers,

As we enter a wonderful sporting phase for India, I would like to congratulate our participants at the ongoing Asian Games for their great performances and wish the Indian Cricket Team the best for the upcoming Cricket World Cup. As a sporting nation, we have indeed come a long way over the past 25 years and now compete for a place amongst the best in many disciplines. This trend is evident across many other areas where India has grown to assume a significant position in the world order.

In the last issue, I talked about App Modernisation and its benefits. Here, I would like to address some cybersecurity challenges that could arise and if not addressed properly could multiply manifold in no time. Legacy vulnerabilities (where outdated systems harbor unaddressed vulnerabilities, infiltrate the modernization process) and agile development gaps (where rapid development cycles may overlook security, inducing inadvertent weaknesses) can be addressed through Foundational Secure Coding and Robust User Identity Management. This entails elevating security from the outset through secure coding practices that eradicate vulnerabilities at the code level and establishing stringent user identity controls to ensure authorized access to sensitive data and functionalities. However, the most important of all is to undertaking Holistic Training Initiatives i.e. Equip your teams with up-to-date cybersecurity knowledge, nurturing a culture of collective vigilance. Our team of experts specializes in cybersecurity, allowing you to accelerate digital transformation with confidence. Do reach out to our experts for any help or assistance.

Happy Reading

APDhungat

Scientists have used mushrooms to make biodegradable computer chips

Foraging for fungi may not only mean mushrooms are on the menu. New research has shown that mushroom skins could provide a biodegradable alternative to some plastics used in batteries and computer chips, making them easier to recycle.

Researchers from the Johannes Kepler University in Austria were working on flexible and stretchable electronics, with a focus on sustainable materials to replace non-degradable materials, when they made their discovery, published in the journal Science Advances Friday.

"There was a fair share of serendipity involved," Martin Kaltenbrunner, head of the university's Division of Soft Matter Physics and co-author of the paper, told CNN.

At the time, a member of the team had been looking at using fungus-derived materials for use in other areas. This work led to the latest study, which shows how Ganoderma lucidum mushroom skin could work as a substitute for the substrate used in electrical circuit.

A substrate is the base of a circuit that insulates and cools the conductive metals sitting on top of it. Typically, they are made of non-degradable plastics, which are discarded after use.

The team, led by Doris Danninger and Roland Pruckner from the university's Institute for Experimental Physics, discovered that the mushroom – which typically grows on decaying hardwood trees in Europe and East Asia – forms a compact protective skin made of mycelium, a root-like network, to protect its growth medium (the wood).

"They do so in order to protect themselves from ingress of other fungi or bacteria," Kaltenbrunner said, explaining that the team were able to harvest this insulating protection by peeling away the skin and drying it out.

According to the research paper, the skin is slightly less insulating than plastic, but it still worked safely and successfully in the electrical circuits, with a thickness akin to paper and the ability to withstand temperatures exceeding 200° Celsius (392° Fahrenheit), making it a good substrate.

The skin has many properties that set it apart from other biodegradable materials, Kaltenbrunner said, "but most importantly, it can simply be grown from waste wood and does not need energy or cost intensive processing."

"Our mycelium is kind of in the sweet spot" because it can last a long time if kept dry, but in just a standard household compost, it would degrade entirely within two weeks or less, he added.

While the team's work is currently experimental and a long way from being put into mass production, they believe the biodegradable skins could be a sustainable alternative material for use in electronics that don't require long-lasting electrical circuits, such as wearable health monitors and near-field communication tags for electronic devices.

But they also envisage wider use if they are able to control the mycelium's growth so that it is uniform and reproduceable.

There are large amounts of waste wood, like wood chippings from industrial sawing, Kaltenbrunner told CNN, which is a lot of food for mushrooms.

http://tinyurl.com/4wv5wm9b

What is a software-defined Data Center?

Since the introduction of server virtualization years ago, organizations have recognized the value of pooling infrastructure resources. By abstracting compute resources from physical servers, server virtualization helps speed provisioning, improve system utilization and reduce hardware expenditures.

The SDDC results from years of evolution in server virtualization. It extends virtualization from compute to storage and networking resources, and it provides a single software toolset to manage those virtualized resources. Plus, the SDDC enables policy-driven automation of provisioning and management, which speeds delivery of resources and enhances efficiency.

Benefits

An SDDC can also help improve infrastructure performance. You can optimize compute, storage, and networking for each application and workload without having to undertake physical changes to the infrastructure.

In the long term, the SDDC helps control costs. Pooling resources improves utilization of infrastructure and enables you to avoid new infrastructure purchases. Better utilization also means that less infrastructure sits idle - consuming real estate, power, and cooling. If you decide to implement an SDDC using hybrid or public cloud infrastructure, you could shift from a CAPEX to an OPEX model, avoiding large up-front capital expenditures.

Adopting an SDDC approach also helps establish a path toward infrastructure and application modernization. Standardizing on a single management platform enables you to more easily integrate new technologies and migrate workloads to cloud environments.

Challenges

Before you implement an SDDC, be sure you understand the potential challenges that could jeopardize your return on investment.

The primary hurdle is gaining cross-functional agreement. Standardization across teams is crucial to adopting SDDC, but many traditional IT organizations are bound by siloed processes and policies that make standardization difficult. Getting procurement teams, development teams, IT analysts, system administrators and others aligned on new tooling and processes can take time. Nonetheless, the payoff in efficiency, innovation, and total cost of ownership can be immense when SDDC is fully adopted.

Once standardization has been accepted across your organization, there are technical challenges as well. For example, switching over to the new environment could result in some application downtime. Planning to implement components of the SDDC in phases could help minimize the risk of downtime. Using a cloud-based SDDC could also allow you to cost-effectively test new virtualization layers before bringing the entire environment into production.

Selecting a cloud provider

What should you look for in a cloud-based SDDC provider? The right provider will offer familiar management tools and interfaces, so your organization does not have to spend time and money learning new management software.

The right provider will also have the expertise you need for a seamless transition to the new environment. You can work with the provider to implement a hybrid environment quickly so you can start benefiting from the new architecture right away, while continuing to use your existing infrastructure.

The right provider will also have the flexibility to support a range of SDDC and hardware configurations. The provider should offer managed and unmanaged options, so you can choose whether to retain complete control of the environment or outsource administration. Ultimately, you should have the flexibility to implement an SDDC that meets your unique requirements.

http://tinyurl.com/mur4tjy8

Galaxy supports organisations to seamlessly transition from old to new environments effectively. To talk to our experts, email us at **marketing@goapl.com**

Microsegmentation

Microsegmentation is a network security technique that enhances the security of a network by dividing it into smaller, more isolated segments, or "microsegments." Each microsegment is typically a small, self-contained network segment that is isolated from other parts of the network. This isolation is achieved through the use of network security policies and controls.

The key principles and features of microsegmentation include:

- **Granular Access Control:**
  Microsegmentation allows organizations to apply highly granular access controls to network resources. Instead of relying on traditional perimeter-based security measures, such as firewalls at the network edge, access controls are applied at a much finer level, often down to the individual workload or application.

- **Zero Trust Security Model:**
  Microsegmentation aligns with the zero-trust security model, which assumes that no entity, whether inside or outside the network, should be trusted by default. Access to network resources is restricted based on the principle of "least privilege," meaning that users or systems are granted only the minimum access necessary to perform their tasks.

- **Isolation:**
  Microsegments are isolated from one another, which means that even if an attacker gains access to one segment, they will have a difficult time moving laterally within the network because the communication paths between segments are restricted. This containment helps limit the potential impact of a security breach.

- **Application-Centric:**
  Microsegmentation is often application-centric, focusing on securing individual applications or workloads rather than entire subnets or network segments. This approach allows organizations to tailor security policies to the specific requirements of each application.

- **Dynamic Policies:**
  Microsegmentation can be dynamic, meaning that security policies can be adjusted in real-time based on changing network conditions, user behavior, or threat intelligence. This adaptability is crucial in responding to evolving security threats.

- **Network Visibility and Monitoring:**
  To effectively implement microsegmentation, organizations need robust network visibility and monitoring tools. These tools help administrators understand network traffic patterns, detect anomalies, and enforce security policies effectively.

- **Automation:**
  Automation plays a significant role in micro-segmentation, as it can help manage and enforce policies at scale. Automation tools can respond to security events and policy changes rapidly.

Microsegmentation can be implemented using various technologies and tools, such as virtual firewalls, software-defined networking (SDN), and network access controls (NAC). It is commonly used in data centres and cloud environments to enhance security and prevent lateral movement by attackers. This approach to network security is especially valuable in modern, complex IT environments where traditional perimeter-based security measures may be insufficient to protect against advanced threats.

Advantages of microsegmentation

Microsegmentation offers several advantages for network security and is increasingly adopted by organizations to enhance their cybersecurity posture. Some of the key benefits of microsegmentation include:

- **Improved Security Posture:**
  Microsegmentation significantly enhances security by reducing the attack surface. It limits lateral movement within the network, making it more challenging for attackers to compromise multiple systems once they gain access to one segment. This containment helps prevent the spread of threats.

- **Zero Trust Security:**
  Microsegmentation aligns with the zero-trust security model, which means that trust is not assumed, and access is restricted by default. This proactive approach to security reduces the likelihood of unauthorized access and data breaches.

Special Focus

- **Granular Access Control:**
  With microsegmentation, organizations can implement highly granular access controls. They can specify who or what has access to specific resources or applications, providing a finer level of control compared to traditional perimeter-based security.

- **Tailored Security Policies:**
  Microsegmentation allows organizations to tailor security policies to individual applications or workloads. This customization ensures that security measures are appropriate for the specific needs and vulnerabilities of each asset.

- **Reduced Attack Surface:**
  By isolating segments from one another, microsegmentation minimizes the exposure of critical assets to potential threats. Even if one segment is compromised, it doesn't automatically grant access to other parts of the network.

- **Dynamic Adaptation:**
  Microsegmentation can dynamically adjust security policies in response to changing conditions, such as the detection of suspicious activities or emerging threats. This flexibility enables organizations to respond quickly to security events.

- **Compliance and Regulatory Benefits:**
  Microsegmentation can help organizations meet compliance and regulatory requirements more effectively. It allows for the enforcement of access controls and data protection measures, which are often mandated by industry-specific regulations.

- **Network Visibility:**
  To implement microsegmentation effectively, organizations typically invest in network visibility and monitoring tools. This enhanced visibility allows administrators to gain insights into network traffic patterns, detect anomalies, and make informed decisions to strengthen security.

- **Easier Incident Response:**
  In the event of a security incident, microsegmentation can aid in containment and isolation, limiting the scope of the breach and making it easier for security teams to investigate and respond.

- **Scalability:**
  Microsegmentation is scalable, making it suitable for environments with varying sizes and complexities. It can be applied to both on-premises data centers and cloud environments, allowing organizations to maintain consistent security measures across their infrastructure.

- **Automation:**
  Automation plays a significant role in micro - segmentation, helping manage and enforce policies at scale. Automated responses to security events or policy changes enhance overall security and operational efficiency.

- **Compliance:**
  - PCI DSS Compliance (Payment Card Industry Data Security Standard): Securing Payment Card Data: Organizations handling credit card transactions can use microsegmentation to isolate systems that store, process, or transmit cardholder data, helping meet PCI DSS requirements.

  - Healthcare and HIPAA Compliance (Health Insurance Portability and Accountability Act): Protecting Patient Data: Healthcare providers can implement microsegmentation to safeguard electronic protected health information (ePHI) and ensure compliance with HIPAA regulations.

While microsegmentation offers numerous advantages, it is important to note that its successful implementation requires careful planning, ongoing monitoring, and expertise in network security. Additionally, organizations must strike a balance between security and usability to ensure that microsegmentation doesn't hinder legitimate business operations.

Galaxy enables Microsegmentation technique that helps architects to logically divide the data center into distinct security segments down to the individual workload level.
To talk to our experts, email us at
marketing@goapl.com

Tech News

Global ransomware attacks at all-time high: Report

The global ransomware attacks are at an all-time high, and the US is the primary target, a new report has said.

The findings from the internet security firm Malwarebytes showed alarming trends in the global ransomware surge from July 2022 to June 2023, in which it noted 1,900 reported ransomware attacks collected, over 43 per cent originating in the US. Germany, France, and the UK all saw an increase in ransomware deployment but lower than the US.

A total of 48 separate ransomware groups attacked the US in the observed period, a 75 per cent increase in the average number of monthly attacks in the US between the first and second half of the last 12 months.

American companies, governmental organizations, healthcare and educational institutions were most attacked. For a year and a half, LockBit, which claims to have 100 affiliates, has been the most dominant form of "Ransomware-as-a-Service" (RaaS) in the US, averaging about 24 attacks per month.

On the other hand, the UK emerged as the second-largest ransomware target, enduring close to 200 ransomware attacks, according to the report.

About 32 separate ransomware groups attacked the UK, seven of which recorded more than ten known attacks. "More ransomware gangs are attacking targets multiple times a month, the number of groups carrying out more than one known attack per month in the UK has climbed steadily for a year, from just one in July 2022 to eight in June 2023," the report said.

https://tinyurl.com/9f63pczj

Global cellular IoT connections to cross 6 billion mark in 2030: Counterpoint

The widespread adoption of cellular connectivity will also contribute to a further reduction in prices for cellular-connected devices, making them more competitive against alternative non-cellular connectivity technologies like LoRa, Sigfox and Wi-SUN, Shah said.

Cellular Internet of Things (IoT) connections are expected to grow at a compound annual growth rate (CAGR) of 10.8% to reach an installed base of 6 billion by 2030, according to Counterpoint Research.

"The growth will be mainly driven by cellular connectivity adoption across various sectors such as utilities, automotive, industrial, retail and healthcare," said Counterpoint's Research Vice President Neil Shah in a statement.

Unlike the previous decade, where consumer devices like smartphones and PCs played a significant role in driving cellular connections, this decade will see a shift towards cellular connections being propelled by the digital transformation initiatives undertaken by enterprise IoT payers, Shah added.

https://tinyurl.com/mrxu2yes

A-23/24, Ambika Towers, Ground Floor,
Off. Jijamata Road, Nr, Pump House,
Andheri (E), Mumbai - 400 093, India.

91-22-42187777

marketing@goapl.com

www.goapl.com