Integrating Technology, Driving Growth

TechTalk

GALAXY Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD.

Issue No. 133, July 2023

The CheckPoint and Galaxy networking event was a huge success with over 100 IT professionals from various industries attending. The event took place at Taj Lands End, Bandra and featured keynotes from Check Point and Galaxy experts.

Attendees enthusiastically shared their insights, challenges, and success stories with one another, The keynote speakers covered a range of topics, including the latest developments in network security, threat intelligence, and trends in the industry.

MD SPEAKS

Anoop Pai Dhungat
Chairman & Managing Director

Dear Readers,

A couple of disturbing events over the past month have really highlighted the importance of the human element in safety measures. The first one was the tragic train accident in India that killed almost 300 and injured more than a 1000. The second one, the implosion of the OceanGate submersible, was much less in terms of lives impacted but very high on media visibility - mainly due to the attempted rescue mission. As per the preliminary investigations, the root cause of both accidents was about some persons ignoring the numerous red flags that indicated something was going wrong. This is where the human element comes in. An alert person with the necessary education on safety would have been able to prevent both these tragedies. Moreover, these were not even attacks but natural events that caused them.

Cybersecurity has to continuously deal with attacks, and so the human element there is even more important in prevention. As the world gets more dependant on IoT, any attack designed to cause loss of lives will be much more disastrous than the ones I've mentioned. The human element in cyber security is less about the deliberate criminal actions of insiders than innocent mistakes made by people who fail to apply basic controls such as limiting permissions on cloud databases, or who fall prey to seemingly legitimate e-mails that fool them into clicking on malicious links. Education, audits, simulated attacks and investing in the right technologies are some ways to reduce the risk of cyberattacks. At Galaxy, our cybersecurity experts can help you implement robust technologies and strengthen the human element to increase your resiliency and protect your data.

Happy Reading

APDhungat

Future Is Now

What will the Internet look like by 2050?

The internet is an incredible thing, changing human existence over the past five decades and continuing to provide us with huge advancements each year. But what does the future hold for the internet, and how will it impact our lives?

Immersive VR, eye implants to view our social feeds, predictive algorithms, and green web hosting are just a few of the huge advancements to come over the next 30 years. Find out what's in store for the digital world in the list below:

Social Networks: An Eye Implant to View Our Social Media Feed

It's apparently only a matter of time before consumers seize control of their own data, brokered by AI agents through personal clouds. The next generation of social networkers will be impacted by the acceleration in digital innovation, including the development of hyper-augmented reality and brain-to-computer interfaces. By 2050 there will be implants placed over our eyes to access our digital world without the need for a display.

Virtual Reality and Artificial Intelligence: Brain Computer Interface Replaces Virtual Reality

Virtual Reality (VR) and Artificial Intelligence (AI) will pave the way for a more streamlined online experience, whether for ecommerce, entertainment, or business. Thanks to rapid developments in the field of brain-computer interface technology, by 2040 users will be able to send information and commands through mere brain signals.

By 2050 it's expected that consumers will be able to plug nanobots directly into the brain for full-immersion virtual reality that directly influences the nervous system. We'll soon see VR developments across a broader spectrum of senses, to simulate smell and taste as current technology does sight.

Data: Virtual Clouds Will Replace Hardware Data Storage

The cloud will be able to accommodate further personal assets that would otherwise have historically demanded local storage.

For increasing the capacity and capability of the cloud, green web hosting is set to be used universally by 2050. With this, companies will dramatically cut down on the size of their data centres in favour of cloud-based technology and reduce their environmental impact.

Design: 3D Printing Will Replace Old Ways of Shopping

The prominence of the 3D printer will continue rising significantly. By 2040 all homes will have access to a device, laying the foundations for the DIY economy. A trip to the hardware store will be a thing of the past, in favour of simply 'printing' your desired appliance.

Security: Improving AI Could Spell Disaster for Security

Cyber criminals are the third most significant threat to humanity, after natural accidents and pandemics. Access to increasingly sophisticated technology could spell disaster.

While extreme computing brings countless benefits, it could also trigger major concern; as we become ever-more connected, those who intend to break through encryption barriers could use super-fast machines to do so in an instant and take an immediate hold over the lives of millions.

Payment: A Cashless Society is Only Around the Corner

The demise of cash has been long coming, and a total reduction of physical money is predicted before the turn of the next decade, with 60% of UK adults expecting a completely cashless society by 2030.

Customer Service: Algorithms which Predict Our Needs

As the world shifts towards digital platforms, customer service will follow suit. In-person customer service will be a thing of the past, with digital advisors placed to address concerns and queries, unless a situation requires complex human involvement.

As early as the next 5-7 years, we'll begin to see a rise in digital agents. As these agents evolve, they'll begin to think for us, renew our insurance for us, and screen advertising messages for us.

https://tinyurl.com/2s46xjf3

Everything you need to know about perimeter security

The term “perimeter security” may sound familiar, but what does it really mean? No, it's got nothing to do with building a fence around your organization. At its most basic, perimeter security is a system, or a group of systems, designed to keep an area safe by preventing unauthorized physical intrusions.

Think of it as a digital fortress: high walls, a moat, maybe even a dragon or two. Except here, instead of stone and fire, advanced technology is employed. The goal remains the same – keep intruders out and protect the people and assets inside.

Why is this so important? In today's world, security threats are a reality that can't be ignored. Whether residential properties or businesses, perimeter security is the crucial first line of defense. It's akin to the goalkeeper in a football match, warding off potential threats before they can get close enough to score.

Technological innovations bolstering perimeter security

However, we're not talking about old-school methods like moats or drawbridges. The modern world calls for modern solutions, and that's where technological innovation comes into play. The advancements in technology have brought forth incredible tools to bolster perimeter security. From smart technologies and artificial intelligence (AI) to biometrics and drone surveillance, it feels like we're living in a sci-fi movie!

These technologies, alongside Internet of Things (IoT) devices, have significantly improved the effectiveness and efficiency of perimeter security. They offer the ability to monitor, react, and adapt like never before. With AI, patterns can be analyzed and potential breaches predicted. Biometrics allow for identity verification with incredible precision. Drones and IoT devices? They provide eyes and ears in places previously unreachable.

Yet, as impressive as all this technology is, it isn't without its challenges. False alarms, triggered by various factors such as wildlife movement, weather conditions, or system malfunctions, can lead to panic or unnecessary action. Conversely, frequent false alarms can result in complacency, slowing responses when a real threat emerges.

Managing authorized access in a system with many users can become complex, especially in larger establishments where numerous individuals require different access levels. Striking a balance between security and efficient operation requires careful planning and regular review.

Furthermore, the systems themselves require regular maintenance to stay effective. Like any other equipment, security systems can deteriorate or become outdated as technology advances. Regular maintenance checks and system updates are vital to ensure the system stays in top working condition and can defend against the latest threats.

So, how can these challenges be tackled? There are a few best practices that are particularly helpful. Regular system checks are essential to ensure everything is functioning as it should.

What is the role of a layered approach in perimeter security?

Another effective practice is integrating systems for better control. This enhances the efficiency of the security network, reduces blind spots, and enables faster responses to issues. Keeping informed about the latest technologies and threats is also vital. Remember, knowledge is power!

Finally, a layered approach to security should be considered. This means having multiple security measures in place so if one fails, others are there to back it up. It's like having a goalkeeper and an entire team working together to defend their goal.

In conclusion, a robust perimeter security system isn't just a luxury—it's a necessity in the modern world. While it really does seem like building a fence around the organization, it's integral to protecting properties, assets, and, most importantly, people from potential threats. The goal isn't just to respond to security breaches—it's to prevent them from happening in the first place. So, whether someone is protecting a home, a business, or even a castle (yes, some people still live in castles), they should think of perimeter security as their digital fortress.Just remember to go easy on the dragons, because then you'll need firewalls.

https://tinyurl.com/mtdzu5b4

Nutanix Unifies Data Services Across Hybrid Multicloud Environments

Nutanix (NASDAQ: NTNX), a leader in hybrid multicloud computing, announced new capabilities in the Nutanix Cloud Platform to enable customers to integrate data management of containerized and virtualized applications on-premises, on public cloud, and at the edge. This includes comprehensive data services for Kubernetes applications as well as cross-cloud data mobility.

According to IDC, by 2025 there will be 750 million new logical applications, more than the past 40 years of computing, all generating large amounts of data across clouds*. This means it will be paramount for organizations to integrate management of data for both containerized and virtualized applications as well as across multiple environments.

"According to the Enterprise Cloud Index, nearly all enterprises have started using Kubernetes for their containerized applications.

Now IT teams need to find a way to both enable their developers with self-service data services, while also ensuring governance and security policies are applied uniformly," said Thomas Cornely, SVP, Product Management at Nutanix. "With Nutanix Data Services for Kubernetes, the Nutanix Cloud Platform will extend storage provisioning, snapshots, and disaster recovery operations to Kubernetes applications to help accelerate containerized application development in the enterprise."

Data Services for Kubernetes

Currently, developers and administrators are faced with gaps and complexity for stateful Kubernetes® applications, necessitating multiple third-party tools or complex DIY projects to solve for the application and namespace layers. Nutanix Data Services for Kubernetes™ (NDK) will give customers control over cloud-native apps and data at scale.

Initially delivered as part of Nutanix Cloud Infrastructure (NCI), NDK will bring the full power of Nutanix's enterprise class storage, snapshots, and disaster recovery to Kubernetes. This will help accelerate containerized application development for stateful workloads by introducing storage provisioning, snapshots, and disaster recovery operations to Kubernetes pods and application namespaces. NDK will empower Kubernetes developers with self-service capabilities to manage storage and data services, while also enabling IT with visibility and governance over consumption. NDK is also designed for use with Red Hat OpenShift.

"Application modernization is a key aspect of our digital transformation journey to continually deliver a better experience for our customers," says Yongju Jo, Chief Manager, IDC Business Dept, Shinsegae. "We believe Nutanix Data Services for Kubernetes has a big potential to deliver simplified enterprise-grade storage provisioning, snapshots, and disaster recovery for our Kubernetes deployments."

Cross-Cloud Data Mobility

Nutanix also introduced the Multicloud Snapshot Technology™ (MST) capability to deliver cross-cloud data mobility. MST will extend Nutanix hybrid multicloud data services by enabling snapshots directly to cloud native object stores, starting with the AWS S3™ object storage service.

This will unlock hybrid multicloud data protection, recovery, and mobility use cases, such as the ability to seamlessly protect and migrate stateful Kubernetes applications and data across cloud infrastructures with NDK leveraging this technology.

MST will enable several use cases including disaster recovery and backup for both containerized and virtualized applications, the ability to create a snapshot and instantly recover it anywhere, cross-cloud data migration, the ability to share data for workflows like test/dev, long-term retention for compliance and more.

This will also help many customers manage costs of their primary infrastructure enabling them to easily store snapshots in a less expensive storage medium, and just as easily recover them, across any infrastructure —private or public cloud.

Special Focus

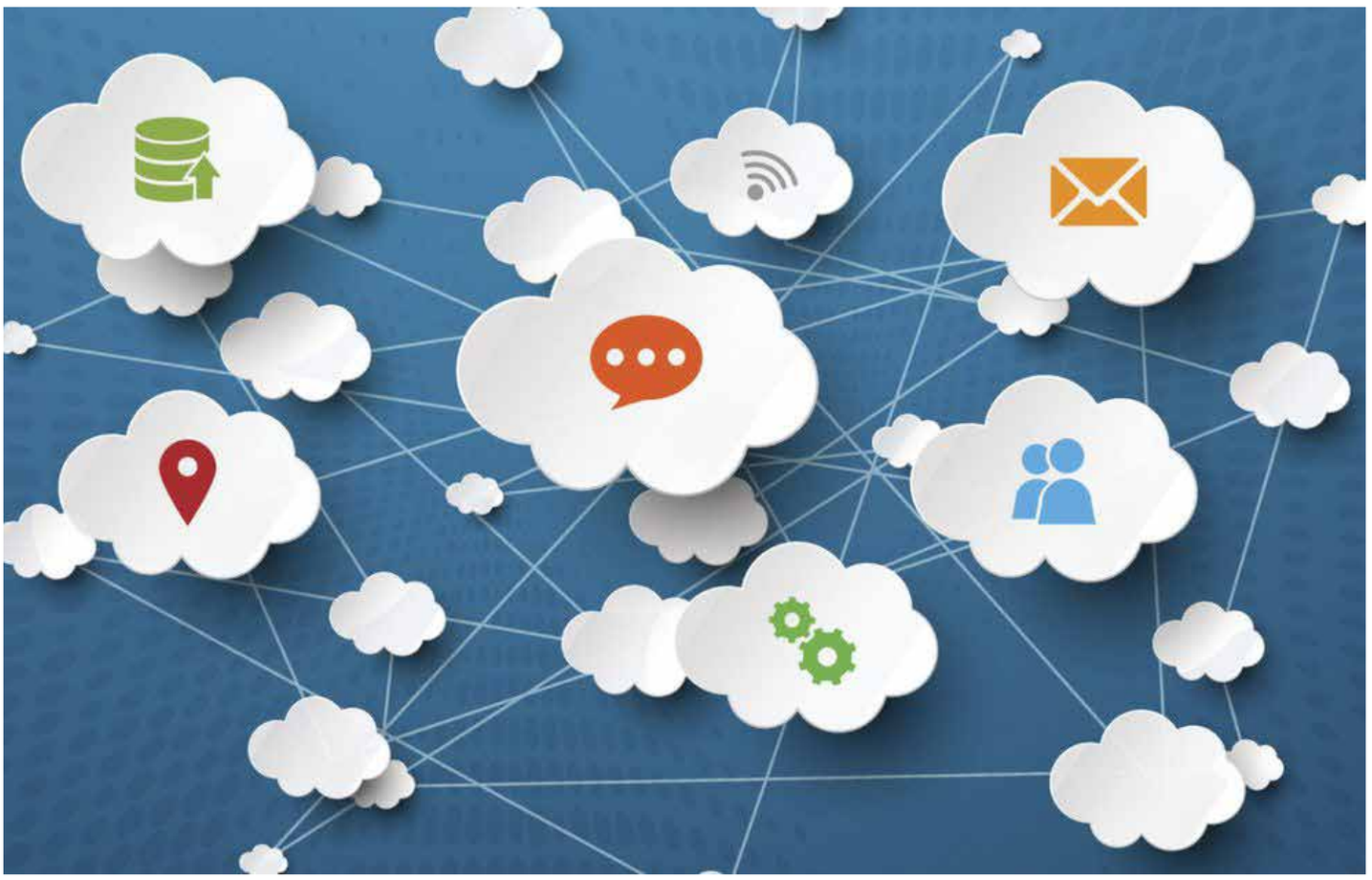
In addition to these new capabilities, the Nutanix Objects Storage™ solution now integrates with Snowflake, the Data Cloud company, to allow organizations to leverage the Snowflake Data Cloud to analyze data directly on Nutanix Objects. This can help to ensure data stays local, accelerates time to value, and delivers faster insights. Additionally, a single namespace in Nutanix Objects simplifies access to globally distributed data.

"Application data is often driving infrastructure decisions for many enterprises whether it's cost, governance or locality, but it's often a separate IT layer from the underlying infrastructure whether on public cloud or on-premises.

The Nutanix Cloud Platform delivers a universal cloud model with natively integrated data services for both containerized and virtualized applications enabling enterprises to easily extend their data governance policies to containerized applications as well as across clouds."

"For organizations looking to ride the next wave of digital transformation, the way forward is to allow workloads to run in the best suited optimal landing zone, underpinned by an open hybrid multi cloud platform with rich data services to run and manage any application, anywhere. Nutanix Cloud Platform and Wipro FullStride Cloud enables customers to make hybrid multicloud simpler to adopt and deliver simplified multicloud management with faster time to market and lower TCO."

With Galaxy and Nutanix, reduce complexity and simplify operations, to focus on business outcomes. We are trusted by companies to power hybrid multicloud environments consistently, simply, and cost-effectively. To talk to our experts, email us at **marketing@goapl.com**



Tech News

Email-based phishing attacks surge 464% in 1st half of 2023: Report

New Delhi, In the first half of 2023 alone, the number of email-based phishing attacks has surged 464 percent globally when compared to 2022, a new report said on Friday.

According to Swiss technology company Acronis, there has also been a 24 percent increase in attacks per organization over the same frame. In the first half of 2023, the report observed a 15 percent increase in the number of files and URLs per scanned email, plus cybercriminals have also tapped into the burgeoning large language model (LLM)-based AI market, using platforms to create, automate, scale, and improve new attacks through active learning.

"The volume of threats in 2023 has surged relative to last year, a sign that criminals are scaling and enhancing how they compromise systems and execute attacks," said Candid Wuest, Acronis VP of Research. Moreover, the report showed that phishing remained the most popular form of stealing credentials, making up 73 percent of all attacks, with business email compromise (BEC) scams making up 15 percent and malware comprising an additional 11 percent. The LockBit gang was responsible for major data breaches.

In Q1 2023, about 30.3 per cent of all received emails were spam and 1.3 per cent contained malware or phishing links. There were 809 publicly mentioned ransomware cases in Q1 2023, with a 62 percent spike in March over the monthly average of 270 cases, the report mentioned. "To address the dynamic threat landscape, organisations need agile, comprehensive, unified security solutions that provide the necessary visibility to understand attacks, simplify context, and provide efficient remediation of any threat, whether it may be malware, system vulnerability, and everything in between," said Wuest.

https://tinyurl.com/4pwpjyma

Tech cooperation defines India-US strategic alignment

The current set of agreements between India and the US on emerging technologies implies that technology will now be at the core of their ties

Prime Minister Narendra Modi's recent visit to the United States (US) has elevated the bilateral tech cooperation to the next level. While much of the focus of the visit was on the two headline-grabbing defence deals: the GE F414 engine co-production and procurement of General Atomics MQ-9Bs Sea Guardian drones, India and the US have also agreed to intensify cooperation in several other emerging and strategic technologies.

These are critical not just for both countries' economic development but will also help them tackle evolving international security challenges. By signing agreements focused on these technologies, New Delhi and Washington are establishing a robust foundation for advancing their 'global strategic partnership.'

The initiative on Critical and Emerging Technology (iCET) set the tone of this tech engagement a year ago. The agreements signed during Modi's visit represent the next stage of the iCET partnership. While the fulfilment of these agreements in the upcoming months will certainly depend on several factors, including the extent of tech transfer and application of US strategic export control regimes, the tone for deeper cooperation is set. India and the US are capitalising on the opportunity presented by the momentous geopolitical shifts in international politics and India's tech transformation.

This is a remarkable transformation of the bilateral relationship, where in the past, New Delhi often found itself at the receiving end of Washington's strategic export control or tech-denial regimes.

https://tinyurl.com/3dzfjmh7