Integrating Technology, Driving Growth

TechTalk

GALAXY Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 118, April 2022

GALAXY RECOGNISED AS DREAM COMPANIES TO WORK FOR.

We have been recognised by the World HRD Congress as one of the Dream Companies to work for under IT/ITES category. This is an important milestone for us and we will continue to invest our management time and focus on creating a highly committed workforce and delivering great value to our customers.

https://bit.ly/36KntBU

MD SPEAKS

Anoop Pai Dhungat
Chairman & Managing Director

Dear Readers,

As we begin a new fiscal year in India, I can only hope that this will be a normal year without any disruptions due to lockdowns or sanctions. My prayer are with all those impacted by the ongoing conflict in Ukraine and a speedy return to normalcy. The amount of destruction and misery will take a lot of rebuilding - not only the physical infrastructure but the mental health of all concerned. Clearly, wars have more losers than winners!

On the technology front, cybersecurity again has moved to the fore due to the cyberattacks that form part of modern warfare. Right from disrupting railway and power plants to hacking into information about the other sides plans and strategies are taking place in the cyberspace. It is clear that no single solution can prevent a cyberattack of such magnitude. What is required is a combination of solutions that provide a layered and complex defence that can detect an attack early enough to prevent or deflect it. At Galaxy, we have been providing such solutions to our customers to keep their activities secure and safe from espionage. Do call us for more information on this and many other solutions that can make your digital transformation journey safe and secure.

I am very proud and happy to announce that even during the past 2 years which affected a lot of businesses adversely, Galaxy has shown double digit growth in both those years. This has been only due to the extraordinary efforts put in by each and every member of our team. Another thing that warms my heart is that, this year, Galaxy has been recognised by World HRD Congress as one of the dream companies to work for. Kudos to all those who have made this happen.

Stay safe and happy reading.

APDhungat

Personal wearable air conditioner to cool the human body

MU engineers design on-skin electronic device providing a personal air conditioner without needing electricity.

An on-skin device designed by engineers at the University of Missouri can achieve around 11 degrees Fahrenheit of cooling to the human body. The device also includes numerous human health care applications such as the ability to monitor blood pressure, electrical activity of the heart and the level of skin hydration. Unlike similar products in use today or other related concepts, this breathable and waterproof device can deliver personal air conditioning to a human body through a process called passive cooling. Passive cooling does not utilize electricity, such as a fan or pump, which researchers believe allows for minimal discomfort to the user.

"Our device can reflect sunlight away from the human body to minimize heat absorption, while simultaneously allowing the body to dissipate body heat, thereby allowing us to achieve around 11 degrees Fahrenheit of cooling to the human body during the daytime hours," said corresponding author Zheng Yan, an assistant professor in the College of Engineering. "We believe this is one of the first demonstrations of this capability in the emerging field of on-skin electronics." Currently, the device is a small wired patch, and researchers say it will take one to two years to design a wireless version. They also hope to one day take their technology and apply it to 'smart' clothing.

"Eventually, we would like to take this technology and apply it to the development of smart textiles," Yan said. "That would allow for the device's cooling capabilities to be delivered across the whole body. Right now, the cooling is only concentrated in a specific area where the patch is located. We believe this could potentially help reduce electricity usage and also help with global warming." The study, "Multiscale porous elastomer substrates for multifunctional on-skin electronics with passive-cooling capabilities," was published in Proceedings of the National Academy of Sciences. Other authors include Yadong Xu, Bohan Sun, Yun Ling, Qihui Fei, Zanyu Chen, Xiaopeng Li, Shivam Goswami Yixuan Liao, Shinghua Ding, Qingsong Yu, Jian Lin and Guoliang Huang at MU; Peijun Guo and Nari Jeon at Argonne National Laboratory in Lemont, Illinois.

https://bit.ly/35mi9E2

Data architecture - A framework for managing data

Data architecture translates business needs into data and system requirements and seeks to manage data and its flow through the enterprise.

Data architecture definition

Data architecture describes the structure of an organization's logical and physical data assets and data management resources, according to The Open Group Architecture Framework (TOGAF). It is an offshoot of enterprise architecture that comprises the models, policies, rules, and standards that govern the collection, storage, arrangement, integration, and use of data in organizations. An organization's data architecture is the purview of data architects.

Data architecture principles

According to Joshua Klahr, vice president of product management, core products, at Splunk, and former vice president of product management at AtScale, six principles form the foundation of modern data architecture:

- Data is a shared asset. A modern data architecture needs to eliminate departmental data silos and give all stakeholders a complete view of the company.
- Users require adequate access to data. Beyond breaking down silos, modern data architectures need to provide interfaces that make it easy for users to consume data using tools fit for their jobs.
- Security is essential. Modern data architectures must be designed for security and they must support data policies and access controls directly on the raw data.
- Common vocabularies ensure common understanding. Shared data assets, such as product catalogs, fiscal calendar dimensions, and KPI definitions, require a common vocabulary to help avoid disputes during analysis.
- Data should be curated. Invest in core functions that perform data curation (modeling important relationships, cleansing raw data, and curating key dimensions and measures).
- Data flows should be optimized for agility. Reduce the number of times data must be moved to reduce cost, increase data freshness, and optimize enterprise agility.

Data architecture components

A modern data architecture consists of the following components, according to IT consulting firm BMC:

- Data pipelines. A data pipeline is the process in which data is collected, moved, and refined. It includes data collection, refinement, storage, analysis, and delivery.
- Cloud storage. Not all data architectures leverage cloud storage, but many modern data architectures use public, private, or hybrid clouds to provide agility.
- Cloud computing. In addition to using cloud for storage, many modern data architectures make use of cloud computing to analyze and manage data.
- Modern data architectures use APIs to make it easy to expose and share data.
- AI and ML models. AI and ML are used to automate systems for tasks such as data collection, labeling, etc. At the same time, modern data architectures can help organizations unlock the ability to leverage AI and ML at scale.
- Data streaming. Data streaming is flowing data continuously from a source to a destination for processing and analysis in real-time or near real-time.
- Container orchestration. A container orchestration system such as open-source Kubernetes is often used to automate software deployment, scaling, and management.
- Real-time analytics. The goal of many modern data architectures is to deliver real-time analytics, the ability to perform analytics on new data as it arrives in the environment.

https://bit.ly/3j1lTOB

Akamai DDOS

What is A DDoS Attack?

DDoS, or distributed denial of service, is a type of cyberattack that tries to make a website or network resource unavailable by flooding it with malicious traffic so that it is unable to operate.

How does a DDoS Attack Work?

DDoS attacks exploit networks of internet-connected devices to cut off users from a server or network resource, such as a website or application they may frequently access. To launch a DDoS attack, attackers use malware or take advantage of security vulnerabilities to maliciously infect and gain control over machines and devices. Each computer or infected device, called a "bot" or "zombie," becomes capable of spreading the malware further and participating in DDoS attacks.

These bots form bot armies called "botnets" that leverage their strength in numbers and amplify the size of an attack. And because the infection of IoT devices often goes unnoticed - just like that pesky B movie zombie that you didn't realize was infected - legitimate device owners become secondary victims or unknowing participants, while attackers remain hard to identify by the victimized organization.

Once an attacker has built a botnet, they are able to send remote instructions to each bot, directing a DDoS attack on the target system. When a botnet attacks a network or server, the attacker instructs individual bots to send requests to the victim's IP address. Just as we humans have one-of-a-kind fingerprints, our devices have a unique address that identifies them on the internet or local network. The result of overwhelming traffic leads to a denial of service, preventing normal traffic from accessing the website, web application, API, or network.

Sometimes botnets, with their networks of compromised devices, are rented out for other potential attacks through "attack-for-hire" services. This allows people with malicious intent but no training or experience to easily launch DDoS attacks on their own.

Edge Defense

Akamai architected its globally distributed intelligent edge platform as a reverse proxy to only accept traffic via ports 80 and 443. All network-layer DDoS attacks are instantly dropped at the edge with a zero-second SLA. That means that attackers launching network-layer DDoS attacks don't stand a chance. For application-layer DDoS attacks, including those launched via APIs, Kona Site Defender detects and mitigates the attacks, while simultaneously granting access to legitimate users.

DNS Defense

Akamai's authoritative DNS service, Edge DNS, also filters traffic at the edge. Unlike other DNS solutions, Akamai specifically architected Edge DNS for availability and resiliency against DDoS attacks. Edge DNS also delivers superior performance, with architectural redundancies at multiple levels, including name servers, points of presence, networks, and even segmented IP Anycast clouds.

Cloud Scrubbing Defense

Prolexic protects entire data centers and hybrid infrastructures from DDoS attacks, across all ports and protocols, with 20 global scrubbing centers and more than 10 Tbps of dedicated DDoS defense. This capacity is designed to keep internet-facing assets available — a cornerstone of any information security program. As a fully managed service, Prolexic can build both positive and negative security models. The service combines automated defenses with expert mitigation from Akamai's global team of 225+ frontline SOCC responders. Prolexic also offers an industry-leading zero-second mitigation SLA via proactive defensive controls to keep data center infrastructure and internet-based services protected and highly available.

Effective defense requires the combination of a proven platform, seasoned professionals, refined processes and techniques. With Galaxy technology experts we aim to provide the pro-active response for deploying the advance security solutions for securing the infrastructure. To talk to our experts, email us at marketing@goapl.com

How the Ukraine war impacts your IT operations

The increase in cyber attacks as a part of the larger war could have devastating effects on IT setups of companies across the world, irrespective of their leanings.

Last week, just a few hours before Russia marched into Ukrainian territory, several websites of Ukraine's banks and government agencies were disabled by a DDoS attack that many believe was launched by Russia. But this was just the beginning of the cyber war between the two countries. After the previous attack on Ukraine reported last month, a destructive wiper attack struck computer systems in Ukraine as well as in two neighbouring countries, Latvia and Lithuania. These attacks again started off as a DDoS attack as a diversionary tactic and deployed a destructive malware, dubbed HermeticaWiper. Like the previous infection, HermeticaWiper is designed to overwrite files on systems to render them inoperable.Various reports warn that future cyber attacks may target U.S. and Western European organizations in retaliation to increased sanctions or other political measures against the Russian government. According to a report, one in five Fortune 500 companies rely on Ukraine's IT outsourcing sector. Experts suggest that organizations might not be directly attacked by the hackers but could still feel the impact.

While the current attacks observed are targeted towards the Ukrainian Government, financial institutions, and Ukrainian websites, the current situation could spill out and affect many other regions globally, taking companies and infrastructures down as collateral damage. "For instance, given how interconnected and interdependent our technologies are, a large-scale attack on a hosting provider in Ukraine could impact businesses working with that hosting provider the world over, leading to a domino effect of system shutdowns, and more," said Vicky Ray, Principal Researcher, Unit 42 at Palo Alto Networks. Amid the war, the hacker group Anonymous also declared cyber war against Russia. The hacking collective posted on its social media account that they had taken down dozens of Russian websites.

Cloud and Data Center providers at risk?

As cloud becomes the default IT model for organizations by freeing them from the burden of owning and managing physical infrastructure, the trend of attacks on cloud services is growing. Cloud services have been the focus of attacks many times in the past (SolarWinds, Capital One) and these won't be the last ones either. According to experts, data in the cloud may just be more vulnerable than data stored on on- prem servers. These vulnerabilities are further compounded by failures across both cloud service providers and end-users.

https://bit.ly/3ISGgYp

Tech News

Govt wants to make India a data centre hub, plans Rs 12,000 crore sops

An ambitious incentive scheme worth up to Rs 12,000 crore is in the works to encourage companies to set up data centres in the country. The government is targeting an investment of Rs 3 lakh crore in the next five years as part of the hyperscale data centre scheme and is planning to provide between 3% and 4% of capital investment as incentive to companies, along with real estate support and faster clearances. Government officials said the vision is to "make India a global data centre hub" and termed the scheme's target as the largest so far in terms of expected investment in the country over a period of just five years. The policy is currently being circulated for inter-ministerial consultations and is expected to be sent for cabinet approval after it is finalised. The quantum of the incentive is still being discussed and could be in the range of Rs. 10,000 crore to Rs. 12,000 crore. "Our vision is to make India a global data centre hub. We have proposed that ease of doing business has to be improved and the bottlenecks have to be addressed," a senior government official told ET.

In the recent past, several multinational technology companies such as Microsoft, Amazon and Google have set up data centre regions in the country. Domestic firms such as Adani Enterprises and Hiranandani Group have also announced aggressive plans to set up data centres in Noida in the National Capital Region. "No other scheme has such ambition in such a short time, so this will be a major game changer for the high-tech industry in India. We want to invite Rs 3 lakh crore worth of investment in data centres in India in next five years," the official added.

The scheme, which is being spearheaded by the Ministry of Electronics and IT, will also look to promote domestic manufacturing of high-end servers. India is fast emerging as a location of choice for data centre majors. The new data centre policy, which is also being finalized by the government, will also play a big part in setting up a national framework aimed at attracting more investment through simplified rules and improved ease of doing business. Delhi, Noida, Gurugram, Mumbai, Chennai, Bengaluru and Hyderabad have already emerged as large data centre hubs due to the forward policies of their state governments which offer land to players, other concessions and faster approvals.

https://bit.ly/3DlqwfJ