Integrating Technology, Driving Growth

# TechTalk

GALAXY Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD.

Issue No. 127, January 2023

## Galaxy is honoured to receive Dell Technologies "Storage Hero Award 2022"

for top performance in storage sales at the Dell Technologies Partner Heroes event in Mumbai on 14th Dec 2022.


MD SPEAKS

***Anoop Pai Dhungat***
Chairman & Managing Director

*Dear Readers,*

*On behalf of all of us at Galaxy, I wish you a very happy, healthy and successful 2023. After almost 3 years of disruptions due to Covid, we have finally have accept the reality that we will just have to live normally and treat it like any other infectious disease. Let us just hope that with the vaccinations, the severity will continue to reduce.*

*As usual, we at Galaxy try and predict the technologies that will see widespread adaption during the year. Our top two picks for the year are Artificial Intelligence & Multi Cloud Management. Artificial Intelligence is poised to cross the rubicon between hype and adoption. We believe that in 2023, AI will be widely used by Governments, enterprises and even smaller businesses. This will happen through easily configurable low code tools to incorporate AI in various business processes and devices. Towards the end of last year ChatGPT has already given us a glimpse of what we can expect. In fact, I won't be surprised to see an AI marketplace where readymade AI models can be integrated with existing systems to make them smarter.*

*Businesses are now understanding the advantages of diversifying their services across a number of cloud providers. This multi-cloud approach, offers a number of advantages, including improved flexibility, redundancy and security. The growing popularity of containerized applications means that in the event of changes to service levels, or more cost-efficient solutions becoming available from different providers, applications can be quickly ported across to new platforms. I expect a number of solutions that facilitate & simplify the multi-cloud approach to emerge as winners in 2023.*

*Stay safe and happy reading.*

# Future Is Now

## Rise of Metaverse in Global Pharma Industry

The ways in which Metaverse will change life sciences industry is not yet fully understood, but significant research and development is underway to utilize the Metaverse and its associated technologies for a wide variety of life science applications. But by combining AI, VR, AR, metaverse can play a huge role in transforming drug development process and Pharma companies can also leverage faster time to market, better learning and development experience.

**Why is there sudden rise in Metaverse in Global Pharma Industry?**

In this ever-changing environment, more and more demand for complex drug development is increasing and COVID-19 is an experience that will be etched with pharma companies for decades, in terms of research, drug discovery, development and faster supply chain.

With the increase in innovative, advanced and complex drug development, the efforts to strengthen the manufacturing process across the industry has become more important than ever. Virtual reality shall offer multifold benefits to pharma industry from improved efficiency and scaling up of drug manufacturing leading to faster time to market.

This shall also help curtail current challenges posed to pharma companies helping in reduced costs, errors in production, reduced wastages, faster and efficient supply chain management leading to reduce data integrity challenges

**How can Metaverse benefit Pharma Industry?**

The multifold benefits metaverse offers shall not only benefit pharma companies but also the end user. Pharma companies spend a lot of money in Research and Development, and Metaverse introduces amazing possibility of using digital twins to starkly reduce the cost and time required for R&D.

Faster supply chain shall help digitalise retail pharmacy in virtual world, with drug delivery happening at doorstep in no time. Once the industry comes to speed with taking manufacturing to the next level, there will be an increased demand to train the resources necessary to achieve business outcome.

VR shall not only allow for faster employee training but also more effective step-by-step experiential training also making Pharma companies save a few bucks with reduced training cost in comparison to traditional classroom or online training methodologies..

https://bit.ly/3VF3MPk

# Technology Focus

## What is Enterprise Mobility Management (EMM)?

Enterprise Mobility Management (EMM) is the process of securing an organization's data on employee mobile devices, whether employee owned or corporate issued. EMM solutions typically include a broad suite of services designed to keep an organization's intellectual property and customer personally identifiable information (PII) safe and secure while integrating with other enterprise IT systems and applications to deliver a broad range of business functionality.

EMM solutions vary widely from organization to organization. Some are focused on securing specific applications; others attempt to completely secure or lock down employee devices, limiting applications that can be installed and erasing data and applications if a device is lost or stolen. EMM has evolved over the past several years from a strictly mobile device focus to enabling mobility in a broader sense, including Windows and MacOS laptops and tablets, access management, and improving the user experience (UX) for mobile applications and devices.

### What are Benefits of Enterprise Mobility Management?

Enterprise Mobility Management provides a single platform for enterprise mobility management, featuring a centralized console to manage mobile devices, email, applications, content, browsing, and more, offering a flexible approach to manage the devices or a secure workspace on devices to address the different use cases and needs organization-wide.

**Some common benefits of EMM systems include simplified and unified management and security by:**

- Support for a broad range of devices, mobile and stationary, so as many devices as possible can be managed by a common platform.
- The ability to protect all data on devices, whether corporate or personal data, by protecting all information with passwords and multifactor authentication, and with the ability to selectively erase corporate data without affecting personal employee information.
- Ensure security software is current by pushing updates as they become available to help prevent zero-day attacks.
- Utilize app stores to speed deployment of business applications in a secure manner and limit which applications can be installed on corporate devices.
- Enforce compliance by ensuring devices used remotely are utilizing secure infrastructure before access is granted to protected information or intellectual property.
- Provide usage data, analytics, and reporting to help uncover patterns that can improve utilization or that might indicate possible breaches or exfiltration of data.
- Applying a policy engine that can set and implement policies, modify them as need be, and tailor them for geography, department, job function, or other factor.

### What Are the Technologies Used in Enterprise Mobility Management (EMM)?

There are many components and technologies used in EMM, and they are constantly evolving. Here are the most common elements of an EMM system:

**Mobile Device Management (MDM).**

MDM is used to manage mobile devices via the use of profiles installed on each device. This enables remote control, encryption, policy enforcement, and the ability to wipe a device of select applications and data should it be lost, stolen, or when an employee leaves the organization.

**Mobile Content Management (MCM).**

MCM is responsible for managing content on mobile devices, including content access, security, pushing content to devices and protection of content at the file level. Many MCM tools work directly with popular cloud storage products to authorize access and data for each user.

**Mobile Identity Management (MIM).**

MIM is concerned with authentication and sign-on, including certificates, code signatures, authentication, and single sign-on to ensure that only authorized users and trusted devices can access corporate resources.

# Technology Focus

**Mobile Application Management (MAM).**

MAM focuses on deploying, managing, and updating the applications that run on an organization's mobile devices. MAM tools include pushing updates, license management, and application security, enabling specific applications to be protected, managed, and deleted if they are retired. MAM is gaining in popularity as it is a way to apply policies and security protocols to specific applications and their data without the need to wipe the entire phone.

**Mobile Information Management (MIM).**

MIM, which is usually part of MDM or MAM services, is responsible for remote access of databases from the mobile devices, and often integrates with the many public cloud storage and collaboration services such as Dropbox.

**Mobile Expense Management (MEM).**

MEM tracks mobile communication expenses, delivering insights to the organization regarding device usage, services consumed, and policies such as BYOD reimbursements. Data collected by MEM can also be used for chargebacks or audits of mobile device usage.

**What is the Difference Between MDM and EMM?**

EMM manages the entire mobile device, while MDM is focused on specific device features. While EMM includes security and policy compliance, application tailoring, and integration with enterprise network directory services, MDM is used to manage mobile devices via the use of profiles installed on each device. This enables remote control, encryption, policy enforcement, and the ability to wipe a device of select applications and data should it be lost, stolen, or when an employee leaves the organization.

MDM's device focus also provides insight into specifics such as OS being used, provisioning status, and what types of device are in use where, by whom, and in which department or business unit.

As organization demand a more holistic approach and view of mobility, many are expanding from a simple MDM approach to an EMM approach that offers a single view of all endpoint user devices and incorporates security from the ground up. As a result, many organizations now utilize a cloud enterprise mobility management platform, opting to store device data in the cloud rather than on a specific device for ease of access and to enhance analysis capabilities.

https://bit.ly/3Ig9SSX

# Special Focus

## How5G will change the way organisations manage their networks and security

Wireless networks are turning into dynamic, life-changing passageways to previously unheard-of levels of bandwidth and throughput speed thanks to 5G networks, which are revolutionizing the world. Providing every person on the planet with highspeed, broadband connectivity is just the beginning.

The earliest iterations of 5G technology are currently being seen. It has a wide range of characteristics that make it a top platform for the digital age. One of the advantages of 4G networks was their strong security, and the same is anticipated from 5G.

We'll demonstrate how two various objectives can be secured by 5G technology. Securing 5G is the first objective. Own platform. The second, at least equally crucial objective is to offer resources for securing the numerous services that are constructed over the 5G network.

Key parties including as operators, interconnection providers, equipment suppliers, application providers, standards bodies, governments, and regulators— each with specific roles to play—share responsibility for 5G cyber security. When carried out properly, these obligations can facilitate the secure deployment and operation of 5G equipment.

Security issues will be raised by new 5G architectures, services, and technologies In general, most threats and challenges faced by 5G security are the same as those faced by 4G security. However, the additional security challenges brought by new architectures, services, and technologies to 5G networks must be considered.

**New Architectures**

With the deployment of the 5G network, new boundaries are introduced when the User Plane Function (UPF) on the core network is shifted from the central equipment room to the Mobile Edge Computing (MEC). Additionally, the fusion of connections and computing raises new security issues.

**Build and operate secure and resilient networks:**
After the 5G effect Users must consider and develop a comprehensive 5G network protection solution through security strategy, design and deployment.

**Management plane protection:**
Customers construct a standalone management plane network, block it off from the Internet, divide the security zone, and install security safeguards like firewalls, intrusion detection, and data leak prevention. Access control for O&M is controlled using the bastion host, multi-factor authentication, and zero trust technologies, and all O&M operations are logged and audited.

**Signalling plane protection:**
To protect the signalling plane between networks, customers use devices such as the SEPP and signalling firewall to screen and monitor incoming and outgoing signalling. To protect intranetwork signalling, they plan security zones on the signalling plane, provide inter-domain protection and slice signalling protection, and protect the APIs for network capability openness

**User plane protection:**
Customers protect the security of 5G user-plane NFs, such as the MEC and UPF, and provide network-layer encryption and integrity protection to safeguard user data transmission.

**Cloud infrastructure protection:**
Customers utilize cloud features, such as cloud services and quick iteration and evolution, to strengthen security protection capabilities and safeguard the cloud platform, cloud-based virtual resources, virtual networks, and container environments. Customers build the security operations platform and system for efficient and intelligent operations.

**Build a security situational awareness and security operations centre:**
In order to improve the automation and intelligence of security operations, operators develop comprehensive security situational awareness for 5G networks, employ big data, cloud, AI, and machine learning technologies, and accelerate risk discovery, identification, and closedloop management.

**Enhance data security protection:**
In order to address the security requirements of vertical industries, operators construct a network security capability openness platform to open security features including authentication, network encryption, and anti-DDoS. To handle new potential security concerns brought on by the development of new services and the open Internet, network security must constantly change.

A great practice for enabling mobile networks is to encourage internal or external security audits, or both (not limited to 5G only). Operators must be vigilant and constantly one step ahead of any potential security concerns.

Don't let networking and security complexity delay your journey! Galaxy can help your organization extend a consistent solution. To talk to our experts, email us at marketing@goapl.com


# Tech News

## Airtel launches 'Always On' IoT solution for vehicle tracking

Bharti Airtel on Friday launched its 'Always On' Internet of Things (IoT) connectivity solution in India, which comprises a dual profile M2M eSIM, allowing an IoT device to stay connected to the networks of two telecom operators. Airtel in a statement said that the solution complies with the Automotive Research Association of India (ARAI)'s AIS-140 standard implemented by the Ministry of Road Transport and Highways (MoRTH).

It added that the solution is "best suited" for vehicle tracking providers, auto manufacturers, and any use-cases where equipment work in remote locations requires ubiquitous connectivity.

The statement said that Airtel's AIS-140 solution has already been tested and adopted by leading companies such as telematics provider Lumax ITuran, fleettech company Loconav, and vehicle tracking solutions provider e-Trans.

The AIS-140 standard lays down mandatory requirements related to connectivity and GPS tracking capabilities for devices in all passenger-carrying buses, private fleets and other public transport vehicles for tracking, safety and security purposes.

Airtel added that with the GSMA-compliant platform, API-based eSIM lifecycle management, and Airtel IoT Hub, along with compliance with the Department of Telecommunications (DoT)'s M2M guidelines, it is looking to acquire market leadership in this segment in the next few years.

"We are delighted to bring Always on connectivity solution to our customers. We believe this is the next big opportunity in the IoT segment. Our strengths in the network, modern and GSMA compliant platform offering real-time access to data and flexibility to integrate the solution with custom APIs will make Airtel Business stand out in the market," said Ajay Chitkara, Director and CEO, of Airtel Business.

https://bit.ly/3Q9ODUQ

## Cyber attacks against Indian government agencies doubled in 2022: CloudSEK report

The number of cyber attacks against Indian government agencies doubled in 2022, making it the most targeted country in this sector, according to CloudSEK XVigil research. "This expansion is the result of the hacktivist group Dragon Force Malaysia's #OpIndia and #OpsPatuk campaigns. Numerous hacktivist groups joined and supported these campaigns, which laid the path for subsequent ones. Government agencies in India have become popular targets of extensive phishing campaigns," the report said.

India, along with China, USA and Indonesia, continued to be the most targeted countries in the last two years accounting for 40% of the total incidents reported in the government sector. The report said that globally, the number of attacks targeting the government sector has increased by 95% in the second half of 2022, as compared to the same period in 2021.

One reason for this has been the rapid digitisation in this sector, brought about as a result of the Covid-19 pandemic. This has increased the attack surface for threat actors, as well as made it easier for hostile governments and state-sponsored actors to use cyber warfare to target other nations. The motivation for carrying out cyber attacks has moved on from purely financial gains to making a social or political point with hacktivist activity accounting for 9% of the recorded incidents in the government sector.

Ransomware groups were also very active in this industry accounting for 6% of the total incidents reported, with LockBIT as the most prominent ransomware operator, it said. The long-drawn war between Russia and Ukraine has also led to an increase in cyber threats against state-owned entities.

The report said that this is the era of cyber warfare, which involves weaponizing hacking to both initiate attacks and prevent cyber attacks. "Cyber warfare can sabotage the electric and physical assets of a nation, and cause physical-world disruptions, along with economic damage," it said.

https://bit.ly/3X67LoT