Integrating Technology, Driving Growth

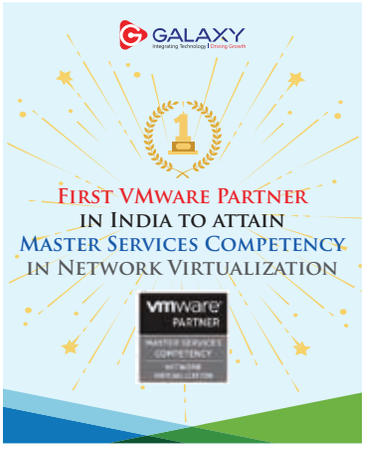
TechTalk

GALAXY
Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 98, August 2020

'Another First'- Galaxy becomes the First VMware Partner in India to attain Master Services Competency in 'Network Virtualization', after being the first to achieve MSC in Data Center Virtualization!

We are very proud to announce to be the First Partner in India to complete all the requirements to attain 'Master Services Competency' in Network Virtualization.



Achieving this competency designates expertise in the delivery of VMware NSX environments and services. Also validates deployment and optimization of NSX environment capabilities for our customers.

Galaxy along with Dell Technologies organizes a Masterclass on the new PowerStore products

To meet evolving application demands and infrastructure challenges, organizations are seeking efficiency and flexibility in the way they solve for today and tomorrow's primary storage challenges. Next generation media types and access methods provide exciting new capabilities. At the same time, new architectures are required to fully harness their potential and break though legacy restrictions and bottlenecks. Addressing these challenges requires asking the right questions about new solutions:

- How can we take full advantage of next generation media types and access methods while still maintaining our required data services and availability?
- Can we start small and scale as additional capacity and performance are required?
- How can I integrate my storage infrastructure with my virtualized, containerized, and devops infrastructures?

Built from the ground-up for next generation NVMe flash and Storage Class Memory, PowerStore enables organizations to easily meet these challenges. The webinar included overview about the mid-range storage and live demo about PowerT Management, Apps On overview, Vcenter Plugin and CloudIQ.

MD SPEAKS

Anoop Pai Dhungat
Chairman & MD

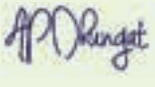
Dear Readers,

Unfortunately, the lockdown in most places in India has had to be extended - albeit with some relaxations. I call this unfortunate because despite a near total lockdown for 75 days, which should have been enough to control the spread to near zero, we find that the count of new cases just kept on increasing. We are still not out of the woods, and all of us should take the basic precautions needed to control the spread.

All this has come at a huge cost to the economy and a lot of businesses are finding it difficult to even survive. At Galaxy, we have put together a host of services that enable businesses of all sizes to enable remote work and carry out most of their tasks as before. This decreases the risk of catching and spreading the virus during the commute and at the same time doesn't disrupt their functions.

Lastly, I am proud to announce that after being the first system integrator in India to attain the Master Services Competency in Data Centre Virtualisation, we are again the first in India to attain the same in Network Virtualisation. Clearly, this reinforces our leadership in the virtualisation space and our 'Masters' will be happy to lead you on this journey in the most efficient manner. Do reach out to us to learn more about this.

Stay safe & happy reading



Future Is Now

Elon Musk Claims His Neuralink Chip Will Allow You to Stream Music Directly to Your Brain

Elon Musk's mysterious Neuralink start-up is working on a brain-computer interface that will allow wearers to stream music directly to their brain, the technology entrepreneur has claimed.

Mr Musk, who also heads SpaceX and Tesla, is set to reveal new information about the mysterious start-up next month but has been slowly releasing details over Twitter in recent days. Responding to computer scientist Austin Howard, Mr Musk confirmed that Neuralink's technology would allow people to "listen to music directly from our chips."

He also said that Neuralink "could help control hormone levels and use them to our advantage (enhanced abilities and reasoning, anxiety relief, etc.)." Since its founding in 2016, Neuralink has only held one major public presentation about how the technology will work.

Speaking at the 2019 event, Mr Musk said the firm was working on a "sewing machine-like" device that would provide a direct connection between a computer and a chip inserted within the brain.

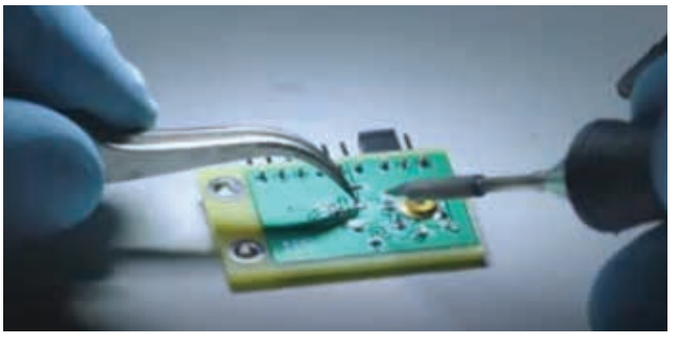
The technology could first be used to help people suffering from brain diseases like Parkinson's, but the ultimate aim of Neuralink is to allow humans to compete with advanced artificial intelligence, he said.

The process of having the chip fitted will be similar to Lasik laser eye surgery, according to Mr Musk. One part of it will involve a neurosurgical robot, which fits flexible "threads" into the brain connected to a tiny implantable computer chip.

A research paper detailing the device claims that a single USB-C cable will provide "full-bandwidth data streaming" to the brain. Neuralink has 11 job postings listed on its website, offering roles for a mechanical engineer, a robotics software engineer, and a "histology technician".

Over the weekend, Mr Musk made a request for people with specific expertise in wearables. "If you've solved hard problems with phones/ wearables (sealing, signal processing, inductive charging, power management, etc.), please consider working at [Neuralink]," he tweeted.

Earlier this month, Mr Musk hinted that Neuralink's chip will be able to cure depression and addiction by "retraining" the parts of the brain responsible for these afflictions. Trials have already been carried out on animals and human trials were originally scheduled to take place this year, though details are yet to be made public.



https://bit.ly/3f6KSLJ

Technology Focus

How cloud is turning to be an effective tool for healthcare industry during Covid-19

Healthcare in the digital age has become a place where a tremendous amount of data is generated on a daily basis. Patients' medical and financial details, as well as any research, are just some of the data that is generated, and maintaining a quick and secure database is of utmost importance.

With the coronavirus outbreak, hospitals and clinics are being overwhelmed with patients. The amount of data that needs to be generated or shared and the speed at which it needs to occur puts a lot of pressure on healthcare professionals. Luckily for them, cloud computing could provide a quick, secure, and cost-effective solution.

Cloud computing comes with a unique set of benefits that can greatly benefit the healthcare sector.

Management of servers

The advantage of cloud-based systems for healthcare is that managing data is not the job of the healthcare provider. With talented IT professionals keeping a watch and managing the system, healthcare providers are able to focus on other important facets of healthcare.

Cost benefits

With cloud computing, it is easier to oversee the services you pay for and take decisions that are cost-effective. By making a custom plan to fit your needs, you can negotiate a deal that is a lot more cost-effective than setting up your own systems.

Designed to manage a tremendous amount of data

As stated earlier, Healthcare and its related sectors generate a lot of data. For example, medical images like scans are extremely detailed and generate high-resolution images, utilizing a lot of data. A lot of this data needs to be stored for the patient's entire lifetime, not to mention – be kept secure. Physical storage is inconvenient and cloud computing provides an easier alternative.

Fast speeds

With patient numbers increasing, speed is of utmost importance. Accessibility to faster cloud servers makes it easy to upload, share, and recover data at a quick pace. It also gives us the ability to make changes faster. Exchange of data and communication between healthcare workers, hospitals, research centers, and funding services like medical crowdfunding creates a better healthcare environment. Time is of the essence in healthcare and with cloud, we can now be a lot more time efficient.

Security and protection

Cloud computing has come a long way when it comes to addressing security concerns. The use of private and hybrid cloud systems has ensured that the medical and financial details of a patient remain secure. For example, if a hospital has a patient that needs to raise funds using a crowdfunding platform, there can be a secure exchange of data between the platform and the hospital using cloud systems. Moreover, the remote servers keep it more protected from any on-location hazard and also reduces any hassles during data recovery.

The opportunities that Cloud computing gives to the Healthcare systems:

Scalability

The needs of the healthcare service provider may change with time. Scaling the cloud services according to their requirements is easy. Cloud allows you to scale up or down quickly, allowing you to meet your current needs or prevent unnecessary expenditure, and also allow for future growth.

Ability to update

Technology is in a constant state of change and innovation. As systems upgrade, data will need to be changed/updated. Whenever these changes do occur, updating data using cloud will be much easier and quicker. Having a cloud-based system will enable you to update your data, applications, and systems as quickly as possible.

Allowing easier collaborations

During the digital age, the sharing of resources is important to create better opportunities for patients. For eg. collaborating with other healthcare providers can provide better services while collaborating with crowdfunding and other alternative funding options enables patients to afford them. Collaborations like these create a better healthcare system for everyone.

Using cloud data in telemedical practices

During this pandemic, doctors and patients alike are at risk of contracting the virus in hospitals. During this critical time, telemedical practices can help healthcare workers continue to provide safe healthcare remotely. These modern medical systems need to transfer the patient data back and forth at high speeds, something that cloud can be used easily, while also maintaining the doctor-patient privacy. By involving cloud computing in telemedical systems, we can now have a safe system, both physically and digitally.

From all that we can assimilate from the advantages that cloud-based systems have, we can conclude that such systems can drastically reduce the number of resources that would be required from the healthcare systems to manage data. It saves time, money, and other important resources. The availability of these resources allows healthcare service providers to concentrate on providing better services, which should be their primary focus.

The early adopters of cloud services have been able to reap the benefits of it for some time now. This has only proved that cloud computing is not only viable, but essential to healthcare, and needs to be adopted now more than ever before.

Galaxy offers solutions for cloud, multi-cloud and hybrid cloud that helps customers to enable greater operational efficiency, resiliency and scalability throughout the entire cloud infrastructure. Get in touch with our experts by emailing us at marketing@goapl.com

https://bit.ly/2CTQb4e

Special Focus

Why Choose Forcepoint DLP?

Forcepoint will enable Organisations to discover and secure critical information whether it resides on premise, in the cloud or in an off-network endpoint device. We will enable Organisations to extend the Forcepoint DLP solution across its high-risk data loss channels, as well as stopping data loss and theft by malicious insiders, outsiders and broken business processes. Key Features and

Benefits

- ForcePoint's unique PreciseID Fingerprinting detects even a partial fingerprint of structured (database records) or unstructured data (documents) on Mac and Windows endpoints – whether an employee is working in the office or on the road.
- Quickly identify incidents for immediate remediation action from statistical data modeling and behavioural baselining .
- Instantly prioritize cases from high-to-low risk levels with customizable risk score thresholds delivered in an Incident Risk Ranking report stack
- Know which cases exceed the risk score threshold in the designated time period that you've selected.

Other Key Features

- Optical Character Recognition (OCR) – See Text within an image with OCR integrated OCR identifies sensitive data within images such as CAD designs, scanned documents, MRI's and screen shots
- Drip DLP - considers cumulative data transmission activity over time to identify small amounts of data leakage
- Data Encryption automatically encrypt data being transferred onto removable storage devices to enable secure data sharing with partners
- Email-Based Incident Workflow makes it easy to distribute an incident for review and remediation to data owners and business stakeholders without needing to provide access to the DLP management system
- Integrated Solution – TRITION unified architecture: Integrated DLP Policies transfer to Enterprise DLP
- Detect and prevent sensitive data being sent out of the organization via email, web uploads, IM and cloud service clients - includes Native SSL decryption for both network traffic and on the endpoint.

Business Value to Organisations

- Protect critical data wherever it resides
- Business enablement – Cloud Services/Cloud apps/collaboration
- Business enablement – Use the technology you want to use
- Enable IT – Ease the burden while preventing the exfiltration of data

Forcepoint Capabilities

- Embrace innovation with confidence
- Ease the burden of deployment and management
- Complete data protection with the industry's most advanced technologies

The Power behind Forcepoint

ACE (ADVANCED CLASSIFICATION ENGINE)

Forcepoint ACE provides real-time, inline contextual defenses for Web, email, data and mobile security by using composite risk scoring and predictive analytics to deliver the most effective security available. It also provides containment by analysing inbound and outbound traffic with data-aware defenses for industry-leading data theft protection.

FORCEPOINT THREATSEEKER INTELLIGENCE

The Forcepoint ThreatSeeker Intelligence, managed by Forcepoint Security Labs, provides the core collective security intelligence for all Forcepoint security products. It unites more than 900 million endpoints, including inputs from Facebook, and with Forcepoint ACE security defenses, analyse up to 5 billion requests per day. This expansive awareness of security threats enables the Forcepoint ThreatSeeker Intelligence to offer real-time security updates that block advanced threats, malware, phishing attacks, lures and scams, plus provides the latest web ratings. The Forcepoint ThreatSeeker Intelligence is unmatched in size and in its use of ACE real-time defenses to analyse collective inputs.

TRITON ARCHITECTURE

With best-in-class security and a unified architecture, TRITON Architecture offers point-of-click protection with real-time, inline defenses from Forcepoint ACE. The unmatched real-time defenses of ACE are backed by Forcepoint ThreatSeeker Intelligence and the expertise of Forcepoint Security Labs researchers. The powerful result is a single, unified architecture with one unified user interface and unified security intelligence.

To talk to our experts or for a free consultation, please write to us at marketing@goapl.com

Tech News

More AI adoption may lead to 2.5% hike in India's GDP: Report

One unit increase in Artificial Intelligence (AI) intensity by Indian firms can result in a 2.5 per cent increase in the country's gross domestic product (GDP) in the immediate term, a study by Google, IT industry body Nasscom and think tank ICRIER revealed.

AI intensity is measured as the ratio of AI to total sales of the firm, said the report titled "Implications of AI on the Indian Economy". In the absence of a direct measure of AI at the firm level, the model uses investments in software, databases and computer machinery as a proxy for AI.

"This is a seminal report, estimating a 2.5 per cnet growth in India's GDP if India adopts AI in a sustained way," Sanjay Gupta, Country Head and Vice President, Google India, said in a statement. The research, however, found that the current rate of growth in AI investments is unlikely to increase the levels of AI intensity adequately.

In order to trigger a positive growth shock, AI intensities should be sharply increased, it added. "India is in the midst of a once-in-a-generation disruption driven by AI. AI has become a strategic lever for economic growth across nations and will continue to be one of the most crucial technologies of the future," said Amitabh Kant, CEO, NITI Aayog, in a special address. "By integrating new technologies like AI and ML into various sectors, we can radically leapfrog and catch up with advanced economies."

The suggested policy measures required to support AI's wider adoption in India include identifying a nodal agency for the development and diffusion of AI; building collaborative frameworks for engagement between governments, industry and academia; building an all-encompassing data strategy for India; addressing India's skill gap in AI; and promoting the development of AI safety standards.

"In hopes to accelerate growth and pave a path towards innovation, AI has a definite role to play in empowering industries, infrastructure and the society at large," said Debjani Ghosh, President, Nasscom.

"With sheer enthusiasm we are now fostering investments in the new generation of digital natives to elevate industry growth trajectory and further boost productivity levels."

https://bit.ly/30WagP9

SonicWall Highlights 65% Drop Malware Drop in India, Ransomware Jumps 20% Worldwide

The SonicWall Capture Labs threat research team today published the mid-year update to the 2020 SonicWall Cyber Threat Report, highlighting increases in ransomware, IoT malware attacks, opportunistic use of COVID-19 pandemic, systemic weaknesses and growing reliance on Microsoft Office files by cybercriminals.

The analysis shows India, along with a few other countries, have experienced a decrease in malware volume. Interestingly, India experienced 64% reduced malware volume. However, this does not imply that it is a safer world. India's malware rates plummeted in April, but by June had nearly reached Q1 levels. The report analyzes threat intelligence data gathered from 1.1 million sensors in over 215 countries and territories. Few salient features of the mid-year update to the 2020 SonicWall Cyber Threat Report are:

- 24% drop in malware attacks worldwide
- 50% rise of IoT malware attacks
- 7% of phishing attacks capitalized on COVID-19 pandemic
- 176% increase in malicious Microsoft Office file types

Commenting on the cyber threat landscape, Debasish Mukherjee, SonicWall Vice President of Regional Sales, APAC, said, "With more people working from home during the COVID-19 pandemic, the abrupt shift to remote working has sparked an unprecedented increase in cyber threats as opportunistic hackers take advantage of the boundary-less ecosystem.

"Exploiting the new raft of vulnerabilities in less secure

situations and preying on fear, cyberspace has seen a significant jump in phishing during global shelter-in-place orders in March and ransomware through the first half of 2020. Cybercriminals are also increasingly using non-standard ports to evade detection and deploy malware, despite a continuation of a downward trend in malware volume since November 2019 and a 32% decline in encrypted threats."

Changing Landscape Leads to Waning Malware Volume

During the first half of 2020, global malware attacks fell from 4.8 billion to 3.2 billion (-24%) over 2019's mid-year total. This drop is the continuation of a downward trend that began last November.

There are regional differences in both the amount of malware and the percentage change year over year, highlighting shifting cybercriminal focus. For example, the United States (-24%), United Kingdom (-27%), Germany (-60%) and India (-64%) all experienced reduced malware volume.

IoT Continues to Serve Threats

Work-from-home (WFH) employees or remote workforces can introduce many new risks, including Internet of Things (IoT) devices like refrigerators, baby cameras, doorbells or gaming consoles. IT departments are besieged with countless devices swarming networks and endpoints as the footprint of their corporate expands beyond the traditional perimeter.

Researchers at SonicWall found a 50% increase in IoT malware attacks, a number that mirrors the number of additional devices that are connected online as individuals and enterprise alike function from home. Unchecked IoT devices can provide cybercriminals an open door into what may otherwise be a well-secured organization.

Malware-laden COVID-19 Emails

The combination of the global pandemic and social-engineered cyberattacks has proven to be an effective mix for cybercriminals utilizing phishing and other email scams. Dating as far back as Feb. 4, SonicWall researchers detected a flurry of increased attacks, scams and exploits specifically based around COVID-19 and noted a 7% increase in COVID-related phishing attempts during the first two quarters.

As expected, COVID-19 phishing began rising in March, and saw its most significant peaks on March 24, April 3 and June 19. This contrasts with phishing as a whole, which started strong in January and was down slightly globally (-15%) by the time the pandemic phishing attempts began to pick up steam.

Office Lures Remain a Staple

Microsoft Office is a necessity with millions of employees now more remote and dependent on the business productivity suite of applications. Cybercriminals were quick to leverage this shift, as SonicWall threat researchers found a 176% increase in new malware attacks disguised as trusted Microsoft Office file types.

Leveraging SonicWall Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection (RTDMI) technology, SonicWall discovered that 22% of Microsoft Office files and 11% of PDF files made up 33% of all newly identified malware in 2020. The patent-pending RTDMI™ technology identified a record 120,910 'never-before-seen' malware variants during that time — a 63% increase over the first six months of 2019.

Don't let your organization be vulnerable! Galaxy offers various cybersecurity solutions to keep your company safe, especially when you are working from home

https://bit.ly/2DhdQLB

GALAXY
Integrating Technology | Driving Growth

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