TechTalk

Issue 76th, October 2018

Galaxy Participates in the Dell Tech Forum 2018

Dell Technologies Forum is a popular platform for delegates to experience the power of Dell's seven technology powerhouses – all in one place, as well as connect with peers and industry thought leaders. Dell EMC had organized the Dell Tech Forum on 7th September at the Grand Hyatt in Mumbai, for mid-senior level IT executives from across Dell EMC's list of customers in Western India.

Galaxy's partnership with EMC began in 2012. Since then, we have been partnering with EMC, and later with Dell, before they merged into a single entity.Post their merger, we have grown our relationship with Dell EMC over last two years, and are a Dell EMC Titanium partner today. Thus, we were invited to be part of Dell Tech Forum and had a dedicated presence in form of a booth where our Data Center Solutions team had put up a HCI [VxRail] demo for all visitors. We had 100+ visitors to our booth from various organizations and industries such as Manufacturing, BFSI, etc.

Galaxy was also invited to participate in a speaking session during the event, where Aditya Sakhavalkar from Galaxy's marketing team gave an overview on Galaxy's solutions and services, as well as our relationship with Dell EMC. This was followed by Mr. Suhas Ingale [Head IT - Bajaj Electricals] who spoke on XtremIO implementation by Galaxy in their office, and how it alleviated some of the earlier issues and challenges faced by their team.

We would hereby like to thank Galaxy's DCG team for their initiative in taking our message to customers, and Dell EMC team for their whole-hearted support and guidance in making this event a grand success.

IN THIS ISSUE

M.D. Speaks

"Dear Readers,

Recently there has been a lot of buzz around using artificial intelligence and machine learning for cybersecurity. With the rapidly increased number and type of attacks, the security industry was always a step behind the hackers. Couple this with a shortage of skilled workers in this space, and the need for using artificial intelligence was inevitable. However, it will be important to remember that in this case it could be a double edged sword. As with any AI or machine learning system, the system is only as good as the algorithm and training data set provided. In the rush to release products in the market, some vendors use training information that could be on the borderline of malware and clean content. The risk in this case is that some attacks may be missed. Another risk is that the hacker could actually target the training information to mark malware as clean. Or they may actually use their own AI algorithm to find out what code is being considered as malware and then work around that. Please note that I am not trying to be alarmist, but only alerting you to the fact that merely using buzzwords in a product does not make it bulletproof. Use the best security product, but please take adequate precautions to monitor and minimise the risks mentioned above.

I wish all of you a very happy upcoming festive season.

Happy reading."

The Future is Now

You Will Be Using Quantum Computers Sooner Than You Think

Today, Quantum computing is the single most important technology in development today. In the past year alone, tech giants like Google, Microsoft, Intel, and IBM made bold investments for their own quantum development.

Today, more than 70 real-world prototype applications run on D-Wave quantum computers. In September, the U.S. House passed the National Quantum Initiative Act, a bipartisan bill to accelerate education, research, and development; the Senate is now considering the bill. This manifests most obviously in some questions. It's no longer, "What is quantum computing?" and "Is it real?" Today, it's, "*When* will this be real?", "What will it look like?", and perhaps most often, "Who's going to win the quantum race?"

The future of quantum computing is hybrid. A diverse set of quantum technologies—combined with classical computing hardware—will work in tandem to serve our future needs. No one company is going to reach a discrete end point. Rather, we must test, collaborate, and share knowledge to reach a collective future. Just as many diverse members of the classical ecosystem figured out how to make computers the most important technology of the 20th century, a new diverse ecosystem will make quantum computing the most important technology of the 21st.

Often, people learning about quantum computing will point to their smartphone and ask, "So when will this run on quantum?" The answer is: "Possibly sooner than you think." But the quantum computer will not be in your handset. Instead of a replacement of our classical devices, the quantum future will be hybrid. QPUs (quantum processors) and classical processors will work together to tackle day-to-day computing as well as complex, enterprise-level problems across industries. So even if smartphones won't contain a quantum computer, they are likely to access quantum computers for certain applications via the cloud within the next few years.

A good comparison for the progression is that of Nvidia's graphics processor. Over time, its perception evolved from that of a hyper-specialized unit for niche, complex applications to that of a powerful technology with real-world applications in everything from scalable AI for autonomous vehicles to consumer drones. Nvidia's founding theory was similar to quantum computing's: processors capable of solving complex problems for graphics could also solve other problems faster than existing computing systems can. It's proved that its graphics processing units (GPU) can accelerate many computations, but is everyone using an Nvidia-powered laptop or phone? No—because such a unit is not needed for every type of daily computation. Plus, Nvidia's GPUs operate in hybrid systems alongside traditional central processing units (CPU).

The truth is that we all win. Quantum computing promises to expand computing power in a nearly limitless way, opening up new pathways to cure cancer, explore the universe, develop unimagined materials, and solve for known and unanticipated complexities of our human systems. There's likely to be more than one quantum computing technology that helps to solve these important problems over the long term.

A Technology to Reverse Climate Change

Last October, Swiss company Climeworks announced its participation in the CarbFix project in Iceland, where its DAC technology is capturing CO_2 to be mineralised and permanently stored underground. This October, project-planning phase for expanding the DACS capacity will begin.

The capture and long-term storage of atmospheric CO_2 will be necessary if we are to protect humanity against the consequences of global warming. All scenarios aim to achieve the 1.5°C goal require 'Carbon Dioxide Removal' – i.e. the removal of CO_2 from the atmosphere through long-term sequestration. The CarbFix consortium, including Icelandic utility Reykjavik Energy and Climeworks, has successfully tested the Direct Air Capture and Storage (DACS) technology in Iceland. This will give everyone the opportunity to have their emissions removed from the atmosphere via Direct Air Capture, for the first time in the world.

With Direct Air Capture being the latest disruptive Negative Emissions Technology, climate scientists needed a "proof of concept" for the promising DACS technology – a milestone that Climeworks and Reykjavik Energy, the pioneers in capturing CO_2 from air and storing it underground, have now achieved with its successful year-long demonstration within the CarbFix2 project. "Today, we have a clear message for climate science and the rest of the world: Direct Air Capture and Storage not only works, but it's safe, permanent and achievable on an industrial scale," said Christoph Gebald, co-founder of Climeworks. "From 2019, we will offer individuals, countries, businesses and institutions from all over the world the unique opportunity to reverse their past, present or future emissions permanently and safely with Direct Air Capture.". As the IPCC makes clear once more, it is now necessary to reduce worldwide emissions fast, whilst at the same time actively remove CO_2 from our atmosphere. The global potential of DACS technology for the permanent removal of atmospheric CO_2 is enormous. Not only is the land and water-use very low for DACS, but Climeworks plants can be implemented anywhere where basalt rock (or other CO_2storage possibilities) and renewable energy sources are available. More importantly, DACS plants do not require any fertile land for operation creating no strain on ecosystems.

The geological conditions for safe and permanent sequestration also exist outside of Iceland in regions of the world such as the USA, the Middle East and Africa. "The storage capacity is such that, in theory, basalts could permanently hold the entire bulk of CO_2emissions derived from burning all fossil fuel on Earth," says Dr. Sandra Snaebjornsdottir, a geologist working for CarbFix.

Technology Focus

How Does Micro Segmentation Help Security?

Micro-segmentation enables fine-grained security policies to be assigned to data center applications, down to workload level.

Data centers running business-critical workloads need proactive security solutions to protect from hidden and emerging threats. Enterprises invest in several high-capacity firewalls and intrusion detection systems, but constantly worry about Advanced Persistent Threats (APTs), malware and other security breaches that may be lurking undetected anywhere in the data center. Because micro-segmentation can assign security policy at the workload level, the security can persist no matter how or where the workload is moved – even if it moves across cloud domains. Using micro-segmentation, administrators can program a security policy based on where a workload might be used, what kind of data it will be accessing, and how important or sensitive the application is. Security policies can also be programmed to have an automated response, such as shutting down access if data is accessed in an inappropriate way.

Traditional methods of detecting and preventing APTs involve several challenges:

a. Segmenting using subnets – Creating multiple VLANs/ACLs is cumbersome and time-consuming
b. Segmenting using firewalls – Capital intensive and need to deal with thousands of firewall rules
c. Segmenting using VMs – Not platform agnostic and doesn't suit a multi-cloud environment
d. Enable zero-trust networks in your multi-vendor environment

ColorTokens secure micro-segmentation is a paradigm shift in data center security, as it focuses on the end-users and applications. This operational principle makes ColorTokens agnostic to firewalls, virtual machines, and private and public cloud infrastructure – capable of securing dynamic application workloads spread across bare-metal and cloud data centers. With ColorTokens, your data center security is future-proof and scalable, enabling protection against undetected lateral threats, malware and zero-day attacks

How Does ColorTokens Work?
ColorTokens has two main components – ColorMaster and Trust Agent. ColorMaster provides a single-pane of glass for your hybrid data center, and it is the main console that provides all administrative functions including cross-segment traffic visibility, analytics, and security policy simulations and enforcement. Trust Agent is a light-weight software agent that is deployed on resources to be protected. These agents are hardened, non-disruptive, and never come in the traffic path.

Get end-to-end visibility across on-premise and cloud data centers
ColorTokens Unified Threat Visibility and Analytics helps you visualize cross-segment traffic flows across servers, clouds, workloads and applications. ColorTokens centralized visibility helps you segment your data center, visualize the impact of the segmentation and ensure a uniform security posture across these segments. ColorTokens eliminates the operational overhead of using multiple visualization and monitoring tools in a multi-vendor environment, removes the need for point products and reduces security gaps in your data centers.

Automate security in minutes
User access to applications and communication between workloads, within and across segments, is facilitated using reusable and customizable security policy templates. With ColorTokens, you can quickly segment the network using abstractions, rather than by IP addresses or VLAN memberships, and apply security policies in minutes. ColorTokens secure micro-segmentation adapts to dynamic application environments and business requirements, providing unparalleled operational ease and security.

Secure Hybrid Deployments Using ColorTokens
ColorTokens Unified Security Platform enables enterprises gain granular visibility into multi-cloud environments, reducing the attack surface and improving the security posture of hybrid data center deployments. Enterprises scale-up their data center, cloud burst into a public cloud when demand peaks and enable disaster recovery using hybrid deployments. While doing hybrid deployments, the enterprise IT teams must ensure that the security policies and compliances remain unchanged across all applications and workloads – be it on their private cloud, or on several public clouds.
Maintaining a uniform security posture using traditional methods is a challenge for hybrid deployments:

a. No cross-cloud traffic visibility between private and public clouds – Risk of undetected data movement
b. Learn/unlearn software from multiple vendors – Operations overhead
c. Deal with IT personnel from multiple departments to achieve the desired security posture, visibility and control – Time consuming

Ensure uniform security across cloud
ColorTokens helps you automate security using reusable security policy templates. You can use the policies to define and enforce user access to applications and databases, irrespective of whether they're inside the private cloud, or accessed on the public cloud. This flexibility ensures that you have uniform security and compliance on every segment of the network, saving hours of manual, error-prone configurations.

Tech News

VMware Adds Intelligence, Integrated AirWatch Mobility Management to Workspace One

VMware showcased its forthcoming Workspace One upgrade at VMworld with an integrated AirWatch UEM agent, extended Windows 10 management and AirLift to ease migration from Microsoft's SCCM and extended endpoint support.

VMware is broadening the reach and capabilities of its Workspace One digital virtual client and application management environment with extended capability and support for Windows 10 PCs, mobile PCs and IoT-based edge devices.

The company demonstrated its new Workspace ONE Intelligent Hub at this week's VMworld in Las Vegas. It combines into one application the Workspace One digital end user environment with VMware's AirWatch device and policy management tool for protecting information across corporate and employee-owned devices.

Workspace One is VMware's digital workspace and unified endpoint management (UEM) platform designed to give workers access to their desktop configurations and applications on any system or device. By integrating the AirWatch Agent with Workspace One, the new "intelligent hub" provides a single source of management, said Jeff McGrath, VMware's senior director of product marketing for Workspace One.

"It's a lot easier for the user because we can use that central point on the device to pipe more services to them and make it a more usable and feature-rich application," McGrath told Channel Futures. The new Workspace One Intelligent Hub user experience provides an embedded URL into the user workspace that defaults to an intranet or external web page, a notification service to issue organizational alerts and a search interface for finding contacts and those within a group.

"We will continue to add to intelligent hub with more capabilities to bring more engagement and value to the employee," McGrath said. "For example, we'll probably add some type of how-to capability so users can reset passwords, recover encryption keys [and] fix simple issues without opening a help-desk ticket to keep them working quicker, if there's an issue." McGrath said the company is in the early stages of training its solution-provider and integration partners on the new Workspace One upgrade, which is set for release by Nov. 2. "All of our certification courses already up to date on these new features," McGrath said.

Tech News

Cisco sets $2.3B deal for Unified Access & Multi-factor Authentication Security Firm

Cisco said it had closed the $2.35 billion deal it made for network identity, authentication security company Duo.

According to Cisco, Duo's zero-trust security model authorizes secure connections to all applications based on the trustworthiness of users and devices. Duo's cloud-delivered technology lets IT professionals set and enforce risk-based, adaptive access policies and get enhanced visibility into users' devices and activities. As more devices come onto the network remotely this issue takes on more importance.

"Outdated devices are particularly vulnerable to being compromised, which can easily spiral into a full-blown, major breach," wrote Richard Archdeacon, Duo Advisory CISO about a recent Duo study on remote access security. "Organizations don't necessarily need to block individuals from using their personal devices, but they do need to re-shape their security models to fit these evolving working practices. ... If you don't know what's connecting to the network, how can you protect data from being compromised?"

Duo in combination with products in Cisco's portfolio, including Umbrella, Stealthwatch, ISE, and Tetration, will let Cisco provide an end-to-end Zero Trust Architecture, wrote Gee Rittenhouse, senior vice president of engineering for Cisco's Security Business Group, in a blog about the Duo acquisition.

"Integrating our network, device and cloud security platforms with Duo's zero trust authentication and access products, Cisco's security architecture is equipped to address the complex challenges that stem from hybrid and multi-cloud environments in today's work environment," Rittenhouse wrote.

A few technical details of the deal include:

a. Cisco currently provides on-premises network access control via its Identity Services Engine (ISE) product. Duo's software as a service-based (SaaS) model will be integrated with Cisco ISE to extend ISE to provide cloud-delivered application access control.

b. By verifying user and device trust, Duo will add trusted identity awareness into Cisco's Secure Internet Gateway, Cloud Access Security Broker, Enterprise Mobility Management, and several other cloud-delivered products.

c. With Duo's Unified Endpoint Visibility, customers can see, track and report on all end user devices from a single dashboard. Duo's user and device reports give admins actionable data on user behavior and risky devices.

d. Cisco said integration of its network, device, and cloud security platforms with Duo Security's zero-trust authentication and access products will let customers quickly secure users to any application on any networked device.

The deal is Cisco's biggest since its $3.7 billion buy of performance monitoring software company AppDynamics in 2017, and its largest in the cybersecurity sector since its $2.7 billion Sourcefire acquisition in 2013. Duo, founded in 2010, has about 700 employees working from offices in Ann Arbor, Mich.; Detroit; Austin, Texas; San Mateo, Calif.; and London. According to a report from MarketWatch, Duo said in early 2017 that it had recorded $73 million in annual recurring revenue in 2016, growing that total 135 percent from the year before. In a similar announcement in early 2018, Duo said it had surpassed $100 million in recurring revenue. Duo Security was valued at about $1.17 billion as of its last funding round.

Cisco Security topped $2 billion in annual revenue for the first time in the 2017 fiscal year, reporting $2.15 billion in sales out of Cisco's total of $48 billion. Duo CEO and co-founder Dug Song and the Duo team are joining Cisco's Networking and Security business led by executive vice president and general manager David Goeckeler.

Special Focus

Lenovo to Debut a Hyper-Converged System for SAP HANA

Lenovo is releasing a hyper-converged system certified by SAP for SAP HANA HCI. The certification uses Nutanix AHV, the first hypervisor certified for production SAP HANA on Hyper-Converged Infrastructure

With the new Lenovo ThinkAgile HX Solution certified for SAP HANA, enterprises can now take advantage of SAP HANA workloads on a hyperconverged infrastructure that moves with the agility and scale of the business. These SAP workloads allow enterprises to reap the combined benefits of in-memory databases for faster access to integrated data analytics and machine learning, and scale for bandwidth demands in storage, compute and networking. Optimized for SAP HANA, the Lenovo ThinkAgile HX solutions are engineered with Nutanix to help customers realize their vision of an intelligent enterprise.

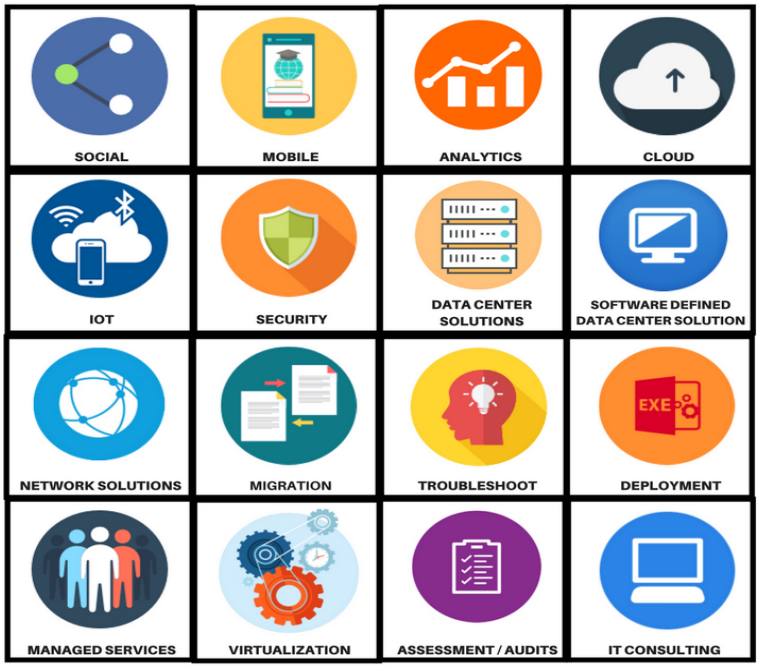
Built on Lenovo's newly announced ThinkAgile HX7820 four-socket system, this solution fits within the mission-critical category of Lenovo's best-in-class hyperconverged ThinkAgile HX portfolio. Customers who choose the SAP-certified ThinkAgile HX7820 can leverage Lenovo's deep SAP expertise to deploy SAP HANA workloads with confidence.

Lenovo's tight partnership with SAP helps customers realize their vision of the Intelligent Enterprise and translates into a seamless customer experience with end-to-end lifecycle management.

The ThinkAgile HX Solution for SAP HANA includes deployment of SAP HANA onsite by a Lenovo Professional Services team, plus full SAP solution support by Lenovo's experts. Lenovo's SAP Center of Competence and SAP architects can aid customers in planning their SAP HANA deployments.

The solution, configurable only with SAP HANA compatible options, is preloaded with Nutanix software in the Lenovo factory, where it is integrated and validated with best recipe firmware.

Ultimately, by relying on Lenovo and Nutanix to deploy SAP HANA, customers can run their SAP HANA workloads with blazing-fast performance, Lenovo uptime, and Nutanix simplicity.



About Galaxy

- One of the most respected Information Technology integrator of the best of breed products and solutions for Enterprise Computing, Storage, Networking, Security, Automation, Application Delivery, ERP and Business Intelligence.
- An ISO 9001:2015 organization, founded in 1987.
- Committed team of over 250 skilled professionals.
- PAN India presence.
- Trusted IT services provider to more than a 1000 companies.
- Experienced consultants certified on a wide spectrum of technologies.
- The Galaxy Technology Innovation Centre, a state-of-the-art integrated hardware and software laboratory, allows customers a hands-on look at the latest storage, backup, security, application delivery and virtualization technologies.
- Customer list includes many of India's leading corporations, banks and government agencies.
- Four business units collaborate to provide a full spectrum of services and ensure smooth projects. Together, they provide our customers with truly end to end professional IT Services.

NEWSLETTER COMPILED BY

Galaxy Office Automation Pvt. Ltd.
A-23/24, Ambika Towers, Ground Floor, Off Jijamata Road, Nr. Pump House, Andheri (E), Mumbai – 400093, India.

Phone: 91-22-42187777
Fax: 91-22-421877760
E-mail: galaxyinfo@goapl.com
www.goapl.com

VISION

"To become the most preferred technology solution partner by listening to our customers, anticipating their needs and providing reliability, flexibility, responsiveness and innovative products and services. Achieving market leadership and operating excellence in every segment of our company."

MISSION

"Total customer satisfaction; through innovative insights, quality service and excellence in technology deployment."

VALUE PROPOSITION

"With our strategic partners we leverage each other's' capabilities to deliver reliable and integrated solutions to the customer. Our consultative sales approach, execution capabilities and commitments helps our customers meet a wide range of end-to-end technology needs while remaining focused on their core businesses."