Integrating Technology, Driving Growth

TechTalk

GALAXY
Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 89, November 2019

Galaxy registers a 45% growth in the first half of FY 2019-20

Despite the Indian economy slowing down in the current fiscal, Galaxy has managed to register a 45% growth compared to the same half last year. This is a result of their long term strategy of focusing on building their skills in cutting edge technologies. These skills are then used to implement solutions that help their customers to stay ahead of their competitors, making Galaxy more of a partner than a vendor or a service provider for them. This coupled with Galaxy's robust financial performance makes them the first choice system integrator for large enterprises across the country. Galaxy has been recognised by a range of OEMs for their sales performance as well as technical certifications.

Galaxy is proud to be the "First" partner in India to achieve the VMware Master Services Competency for Data Center Virtualization.

To know more, Get in touch with us on 022-46108777
or email us at marketing@goapl.com

MD SPEAKS

Anoop Pai Dhungat
Chairman & MD

I would like to thank all of you for contributing to the continued success of Galaxy. This has only been possible because of the trust and faith that our stakeholders have placed in us, and I assure you that we will not only live upto expectations but surpass them. We are poised to continue on this high growth path by leveraging our strengths in terms of technical abilities, financial stability, strong OEM relationships and our deep understanding of customer requirements. We are also actively looking to expand our market reach to other geographies by strategic alignments or acquisitions that will further add to our growth.

I am also proud to announce that Galaxy is the first partner in India to achieve the VMware Master Services Competency for Data Centre Virtualization. This is an endorsement of the quality of skills that we have for Data Centre service delivery. Please reach out to us for understanding more on how we can help you with data centre virtualisation.

Google Claims 'Quantum Supremacy' With New Processor That Could Change Computing Forever

Google says its quantum processor, Sycamore, finished a calculation in three minutes and 20 seconds - and that it would take the world's fastest supercomputer 10,000 years to do the same thing.

Google said it has achieved a breakthrough in quantum computing research, saying an experimental quantum processor has completed a calculation in just a few minutes that would take traditional supercomputer thousands of years. The findings, published Wednesday in the scientific journal Nature, show that "quantum speedup is achievable in a real-world system and is not precluded by any hidden physical laws," the researchers wrote.

Quantum computing is a nascent and somewhat bewildering technology for vastly sped-up information processing. Quantum computers might one day revolutionize tasks that would take existing computers years, including the hunt for new drugs and optimizing city and transportation planning.

The technique relies on quantum bits, or qubits, which can register data values of zero and one — the language of modern computing — simultaneously. Big tech companies including Google, Microsoft, IBM and Intel are avidly pursuing the technology.

"Quantum things can be in multiple places at the same time," said Chris Monroe, a University of Maryland physicist who is also the founder of quantum startup IonQ. "The rules are very simple, they're just confounding."

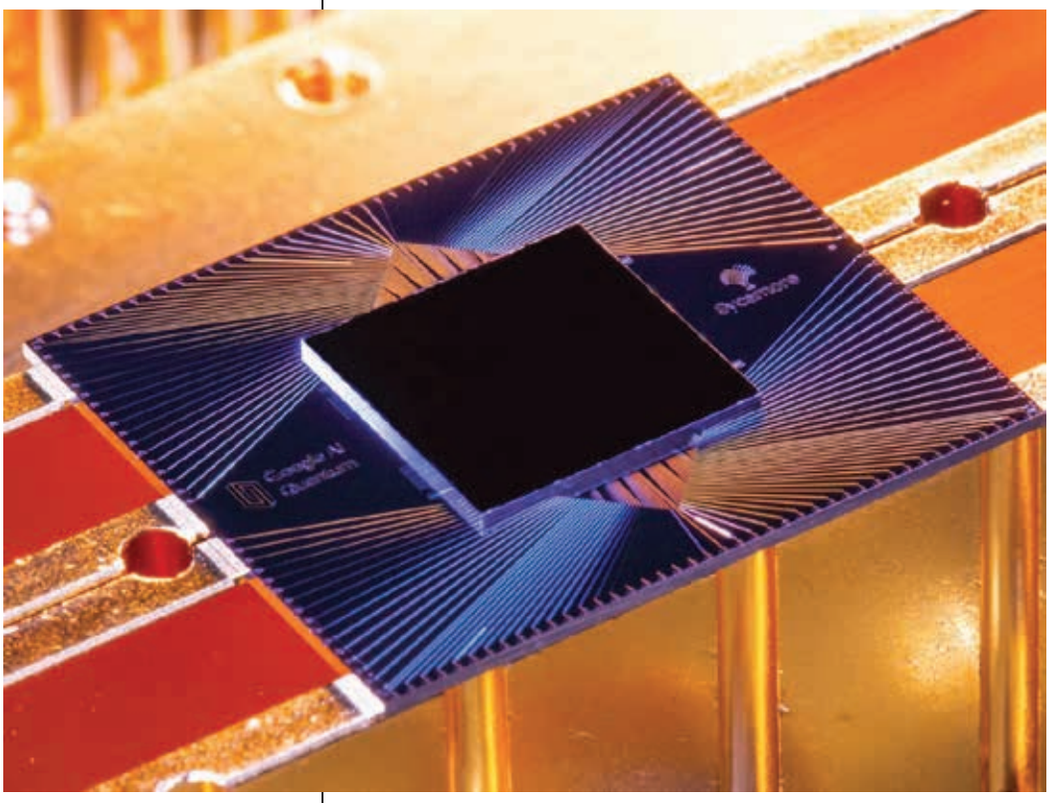
Google's findings, however, are already facing pushback from other industry researchers. A version of Google's paper leaked online last month and researchers caught a glimpse before it was taken down.

IBM quickly took issue with Google's claim that it had achieved "quantum supremacy," a term that refers to a point when a quantum computer can perform a calculation that a traditional computer can't complete within its lifetime. Google's leaked paper showed that its quantum processor, Sycamore, finished a calculation in three minutes and 20 seconds — and that it would take the world's fastest supercomputer 10,000 years to do the same thing.

But IBM researchers say that Google underestimated the conventional supercomputer, called Summit, and said it could actually do the calculation in 2.5 days. Summit was developed by IBM and is located at the Oak Ridge National Laboratory in Tennessee.

Google has not commented on IBM's claims.

Whether or not Google has achieved "quantum supremacy" or not may matter to competitors, but the semantics could be less important for the field of quantum research. What it does seem to indicate is that the field is maturing.



"The quantum supremacy milestone allegedly achieved by Google is a pivotal step in the quest for practical quantum computers," John Preskill, a Caltech professor who originally coined the "quantum supremacy" term, wrote in a column after the paper was leaked.

It means quantum computing research can enter a new stage, he wrote, though a significant effect on society "may still be decades away."

https://bit.ly/2NsFTt7

Deception: Luxury Item or a Life Saver for your Organization?

Findings from the 2019 EMA report: "A Definitive Guide to Deception Technology"; users of deception have reported great confidence in being able to quickly detect threats and state that dwell-time is reduced by more than 91% compared to non-users. Let us not lose sight of the fact that Mandiant's latest trend report indicates that the global average is 78 days, which exemplifies the lack of controls in organizations' tool kits for early and proactive detection of threats.

One of the misconceptions about deception is that only network-level traps are required for basic detection, however, not all deception technologies are created equal. A comprehensive deception solution will turn the network into an authentic minefield. This requires the use of high interaction traps that delay the activity of the attackers, decoys that allow the attackers to be attracted to the surface of these decoys and whose events can be monitored, the ability to identify recognition activities on the objects of the Active Directory as is done with tools such as BloodHound (without installing anything in the directory) and the diversion to a mesh of deceit gaining threat intelligence and in-depth telemetry for the analyst, as well as make use of automation to reduce the response time from hours to minutes.

The analogy is simple, assets are required to become "wolves in sheepskin" that respond to any suspicious activity before a breach is successfully completed, backed by a surface of authentic traps that are dynamically updated.

According to Gartner, automation is a priority today. We know this when it comes to deception solutions being able to automatically assist in the eradication of a threat in the event of detected ransomware, credential theft or when it comes to exploiting a non-active port on your computer, which is completely suspicious. Having the ability to isolate the source from the attack on the traps or through an integration with your firewall or NAC or EDR solution is something you can achieve in seconds.

When talking about visibility, Carolyn listed 4 key factors for attendees:

- Know where your assets are
- Understand the routes and attack techniques
- Implement internal visibility mechanisms
- Apply deceptive and asymmetric defensive technology that changes the position of the defender.

The approach is becoming a real lifesaver rather than a luxury item according to analysts.

Carolyn concluded that organizations that need to compare deception solutions should look to the recent Gartner and Cyber Source Data Wellington Research reports that identify some of the fundamental criteria associated with each vendor. We implore companies to do their research and draw conclusions that are most aligned with the needs of their organization.

Regardless of whether you are a CIO or a CISO, the objective is clear today: it is necessary to reduce the residence times of advanced cyber attackers and respond as early as possible to trivial activities such as the recognition phase or when a Ransomware begins to spread in its initial phase.

https://bit.ly/34hulu0

Dell Technologies Raises Bar with Next-Generation Data Protection Solutions

News Summary:

- New fast, secure and efficient PowerProtect DD Series Appliances power data protection for multi-cloud workloads
- PowerProtect DD appliances offer scalability and grow-in place capacity expansion, improved logical capacity by up to 30%[i] and data reduction by up to 65x
- For cyber resiliency, PowerProtect Cyber Recovery introduces PowerProtect Software integration and user experience enhancements
- Enhanced PowerProtect Software advances data management capabilities for ever-changing growth and data protection requirements

Dell Technologies is introducing PowerProtect DD Series Appliances, the next- generation of its Data Domain protection storage appliances, enabling organizations to protect, manage and recover data at scale across diverse environments. In addition, Dell Technologies is announcing new enhancements to Dell EMC Cyber Recovery, now Dell EMC PowerProtect Cyber Recovery, and to Dell EMC PowerProtect Software that will provide customers with cyber resiliency and support for workloads on PowerProtect DD Series Appliances.

Today's businesses are experiencing an overwhelming increase in the amount of data they create and retain. According to the Dell EMC Global Data Protection Index, organizations managed 9.70 petabytes of data in 2018, a 569% increase compared to the data managed in 2016. With PowerProtect DD Series Appliances, customers can equip themselves with a solution that supports their growing data needs, has the ability to quickly restore their systems in times of disruption and fosters business value and innovation through a secure path to existing data sets.

Introducing Dell EMC PowerProtect DD Series Appliances

As the newest addition to the Dell EMC PowerProtect portfolio, Dell EMC PowerProtect DD Series Appliances are built to simplify and provide operational efficiencies for data protection for multi-cloud workloads. PowerProtect DD offers:

- Faster performance. With up to 38% faster backups and up to 36% faster restores[ii], PowerProtect DD includes instant access and instant restore of up to 60,000 IOPS for up to 64 virtual machines, and support for 25GbE and 100GbE network speeds.
- Greater efficiency. PowerProtect DD is highly efficient, providing up to 1.25PB of usable capacity in a single rack with hardware-assisted compression improving logical capacity by up to 30%, driving up to 65x data reduction.[iii] This smaller footprint delivers power and cooling savings of up to 35%[iv], increasing ROI for organizations.
- Scalability to meet future demands. With flexibility and agility at its core and available in multiple configurations, PowerProtect DD provides scalability and grow-in place capacity expansion, ranging from 1 terabyte up to 1.25PB.
- Data protection for multi-cloud workloads. PowerProtect DD provides operational efficiency, resiliency and scalability across on-premises and hybrid cloud environments. It has an extensive cloud ecosystem with support across multiple public clouds and can natively tier deduplicated data, delivering cost-effective, long-term retention.
- Single pane of glass management. With PowerProtect DD Management Center, customers can gain aggregated management for multiple systems, manage capacity and replications, and monitor the health and status of all their appliances on-premises and in the cloud.

https://prn.to/34Giqf9

Trend Micro Acquires Cloud Conformity To Strengthen Its Position As In Cloud Security

Trend Micro has announced it has acquired Cloud Conformity, a Cloud Security Posture Management (CSPM) company. The acquisition broadens the cloud services Trend Micro can secure and resolves often overlooked security issues caused by cloud infrastructure misconfiguration.

"We have been laser focused on building integrated security for the cloud since its birth over a decade ago, unlike other vendors who are now attempting to stitch together disparate cloud technologies. As more enterprises move to the cloud, our customers feel they're operating amid a wild-west approach to cloud implementations that leave them with unmanaged risk. As an AWS technology partner of the year for 2019, Cloud Conformity understands these implementations and the risks. Their offering perfectly complements our own portfolio and provides immediate value to customers. Both the people and technology are a great fit for Trend Micro," said Eva Chen, CEO, Trend Micro.

"Our rapid expansion with AWS, complemented by our dedication to security and compliance, is made actionable and scalable through the Cloud Conformity tool. Their product provides us with greater visibility, the ability to improve performance and optimise costs, assuring continuous resilience as we grow," said Russell Jones, Principal Architect, Virgin Australia.

"Our research is clear that organisations of all sizes are adopting cloud-based delivery and, in doing so, are often using not only compute services, but also storage, messaging, and many other services. With this acquisition, Trend Micro is able to extend its security offerings to organisations looking for assistance with cloud security beyond securing compute workloads," said Fernando Montenegro, Principal Analyst with 451 Research.

"We are excited for the opportunities that will come from being part of the leading cloud security provider – amplifying what we do best, while allowing our offerings to expand in ways we couldn't have done on our own. We think customers will love this simplified approach to security and compliance across their entire cloud environment, including AWS, Azure and Google Cloud – providing security guardrails to let them go faster and do more," said Michael Watts, CEO of Cloud Conformity.

https://bit.ly/2JF6JNp

Smart Light Bulbs Can Hack Your Personal Information, Says Study

Smart bulbs are expected to be a popular purchase this holiday season. But could lighting your home open up your personal information to hackers? Now a new study from an Indian-origin researcher shows that the hacker's next prime target could be that smart bulb. Some smart bulbs connect to a home network without needing a smart home hub, centralised hardware or software device where another internet of things (IoT) products communicate with each other.

Smart home hubs, which connect either locally or to the cloud, are useful for IoT devices that use the Zigbee or Z-Wave protocols or Bluetooth, rather than Wi-Fi.

"Your smart bulb could come equipped with infrared capabilities, and most users don't know that the invisible wave spectrum can be controlled. You can misuse those lights," said study lead author Murtuza Jadliwala, Professor from the University of Texas at San Antonio in the US. "Any data can be stolen: texts or images. Anything that is stored in a computer," Jadliwala added.

Earlier this year Amazon's Echo made global headlines when it was reported that consumers' conversations were recorded and heard by thousands of employees. Now researchers have conducted a review of the security holes that exist in popular smart-light brands. According to the analysis, the next prime target could be the smart bulb that shoppers buy this coming holiday season.

If these same bulbs are also infrared-enabled, hackers can send commands via the infrared invisible light emanated from the bulbs to either steal data or spoof other connected IoT devices on the home network, the study said. The owner might not know about the hack because the hacking commands are communicated within the owner's home Wi-Fi network, without using the internet.

Smart bulbs have moved beyond novelty to a lucrative mature market. Last year consumers spent close to $8 billion, and that amount is expected to more than triple to $28 billion in less than a decade.

"These bulbs are now poised to become a much more attractive target for exploitation even though they have very simple chips," Jadliwala said. Jadliwala recommends that consumers opt for bulbs that come with a smart home hub rather than those that connect directly to other devices.

https://bit.ly/2NEVK88