Integrating Technology, Driving Growth

TechTalk

GALAXY
Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 95 May 2020

Get Ready for the Remote - Work Future

This vast remote-work compulsion during lockdowns is also a great opportunity to prepare for the future — when automation has expanded the role of knowledge workers and the preferences of younger generations demand that organizations provide remote-work options.

Here are some of the Requirements and Solutions with which we can support our customers to get going in the difficult times and continue the business:

Requirement	Solutions
End Point Availability	Laptops on Rental / Purchase
Direct Desktop Access	Provide Desktop Access to machine in office from home device securely without any compliance violation
Power on Virtual Desktops	Secured, Quick Provision and immediate access to virtual desktops in cloud
Power on Virtual Machines or Applications	We can help quickly provision resources, capacity, applications on Cloud and give secure remote access to employees
Data Backup	Quick, Easy to setup and manage end point backup of data
Secure Access	SSL VPN configuration and MFA for Remote Access
Application Security	Provide secure access to your internal applications from any device
End Point Security	Secure all your existing, new and rented devices off or on the Network
Remote Infrastructure Management	Remote management of the infra for uptime and resolve the issues arising due to current situation
Workstation Workloads	GPU Virtualization and GPU based desktops in cloud

Contact our experts by dropping an email at **marketing@goapl.com** to start planning right now!

Anoop Pai Dhungat
Chairman & MD

MD SPEAKS

Dear Readers,

As we are almost 40 days into the total lockdown, the increasing number of infections just indicate that people in general have not been taking the lockdown and social distancing seriously. In theory, a 40 day lockdown would be 3 cycles of 14 days - the time during which an infected person can infect others. This should have been enough to reduce the new infections to a very small manageable number and a gradual return to normalcy. Instead, because of the recklessness (or maybe helplessness) of a few, here we are staring at an even longer lockdown.

We, at Galaxy, have been extremely busy working to enable our clients to work remotely in a very secure way. During the course of the lockdown, we have migrated data onto the cloud, implemented security solutions and even delivered laptops to essential services so that they could conduct their business is a safe and efficient manner. We have been discussing business continuity in the completely different context of long lockdowns that could become a regular occurrence, at least until a reliable cure is found or enough people have been vaccinated to spread the contagion. More importantly, a lot of people we have been talking to are seriously considering remote workers as a viable option even when commuting to office becomes possible. We have been working on a number of solutions that would enable our clients not only continue their business as usual but also save costs going forward by enabling "secure work from anywhere" solutions. Please get in touch with any of us and we will be happy to explain and demonstrate our solutions.

I am proud to announce that Galaxy is the first company in India to be appointed as a Managed Service Provider under the VMWare Cloud Program. This just revalidates our abilities of planning, migrating and supporting our customers on their journey to the cloud and leverage our partnership with VMWare to provide our clients with the best solutions.

In the meantime, I urge all of you to take social distancing and the lockdowns extremely seriously to prevent the spread of the virus.

Stay Home & Stay Safe

APDhungat

Future Is Now

MIT Scientists Are Building Devices to Hack Your Dreams

A team of researchers at MIT's Dream Lab, which launched in 2017, are working on an open source wearable device that can track and interact with dreams in a number of ways — including, hopefully, giving you new control over the content of your dreams.

The team's radical goal is to prove once and for all that dreams aren't just meaningless gibberish — but can be "hacked, augmented, and swayed" to our benefit, according to OneZero.

Think "Inception," in other words, but with a Nintendo Power Glove.

"People don't know that a third of their life is a third where they could change or structure or better themselves," Adam Horowitz, PhD student at MIT Media Lab's Fluid Interfaces Group and a Dream Lab researcher, told OneZero.

"Whether you're talking about memory augmentation or creativity augmentation or improving mood the next day or improving test performance, there's all these things you can do at night that are practically important," Horowitz added.

A glove-like device called Dormio, developed by the Dream Lab team, is outfitted with a host of sensors that can detect which sleeping state the wearer is in. When the wearer slips into a state between conscious and subconscious, hypnagogia, the glove plays a pre-recorded audio cue, most of the times consisting of a single word.

"Hypnagogic imagery or hallucinations is a normal state of consciousness in the transition from wakefulness to sleep," Valdas Noreika, a psychologist at Cambridge who is not involved in the research told VICE back in 2018.

Hypnagogia may be different for different people. Some say they've woken up from hypnagogia, reporting they experienced strong visual and auditory hallucinations. Others are capable of interacting with somebody in the state.

But the Dream Lab might be on to something with its Dormio glove. For instance, in a 50-person experiment, the speaking glove was able to insert a tiger into people's sleep by having the glove say a prerecorded message that simply said "tiger."

The device is meant to democratize the science of tracking sleep. Step-by-step instructions were posted online with biosignal tracking software available on Github, allowing everybody to theoretically make their own Dormio glove.

A similar device built by Dream Lab researcher and PhD candidate Judith Amores relies on smell rather than an audio cue. A preset scent is released by a device when the user reaches the N3 stage of sleep, a regenerative period when the body heals itself and consolidates memory. The idea is to strengthen this consolidation using scents.

They hope to let sleepers take full control of their dreams as well. A 2019 "Dream Engineering" workshop hosted by the Dream Lab discussed the world of "lucid dreaming," a state in which people realize they're having a dream while they're dreaming.

"It's such an exhilarating feeling to lucid dream," Tore Nielsen, a professor of psychiatry at the University of Montreal said in an MIT blog post. "You can try flying, singing, having sex — it's better than VR."

The problem, however, is that the science behind lucid dreaming is still murky. Only an estimated one percent of people are capable of entering this state regularly, making it difficult to study. The brain state during lucid dreaming is also not understood very well yet.

But other researchers are convinced there's plenty to gain from learning from our subconscious — rather than commanding it with prerecorded messages or scents.

"The unconscious, it's another kind of intelligence," Rubin Naiman, sleep and dream expert at the University of Arizona, told OneZero. "We can learn from it. We can be in dialogue with it rather than dominate it, rather than 'tap in' and try to steer it in directions we want."

https://bit.ly/2xVIBDx

Why cloud data protection is a must in the time of COVID-19 crisis?

Data explosion in recent times has complicated data management for organisations in India. Perhaps that is reason why IDC's Cloud Pulse 2Q19 estimates that 75% organizations in the country will invest in cloud-based infrastructure and applications to meet their business goals. Furthermore, Nasscom has predicted that the cloud computing market could hit $7.1 billion tripling to a compound annual growth rate (CAGR) of 30% by 2022.

However, as more employees connect remotely to work from home, cloud adoption could be ineffective without data protection. Cloud data protection systems are a must as they can ease increasing data complexity, provide a central access point, bring greater data visibility, lessen legal and regulatory risk, and save costs. Let us look at some key reasons why this is vital now than ever.

Simplify backup and recovery

Businesses have to be agile in their functioning. These unprecedented times are a real test of time. Companies are encouraging employees to work from home so that they ensure safety and business continuity. Simplifying data backup and recovery is one of the steps to ease and quicken the process of data management and accessibility, especially when the entire organization is connecting remotely. While traditional backup systems are cost intensive as well as time-consuming, a cloud data protection system expediates the backup process. As a single secondary copy of all data is stored in the cloud infrastructure, backup hardware is no longer needed locally. It also eliminates the whole concept of performing a traditional backup as it is being constantly updated accordingly to a configurable schedule. Hence, backups from any point in time, are always available and accessible from anywhere in the world.

Identify trends

To function effectively in a highly competitive environment, businesses must identify not just consumer trends, but also data trends from within the organization. Deploying a cloud system indexes the complete text of each data file, thereby enabling organizations to identify trends in data usage. For instance, it helps to track whether the sales team in a particular region is writing fewer contracts after a new regulation went into effect? An access to the entire data protection system hosted on a single dashboard provides decision makers with summaries of activity by service, by user, by device, and by date. This enables efficient top-level decision-making and impacts business growth positively. In the times of a pandemic, data trends are useful from the point of view of ensuring open communication with employees, most of whom are connecting remotely and at the same time offer them relevant information about the constantly evolving situation.

Easier malware/ransomware recovery

Malware is a real threat to organizations as it can result in grave loss of business data. Educating users and putting robust anti-malware tools in place can help with prevention, but they cannot help you once an infection occurs. A complete malware attack recovery needs the recent, comprehensive backups from the time before the attack occurred. The flexible backup capability of a cloud-based data protection system provides the most reliable, most thorough, most recent backups for easy recovery. At a time when employees are working from home, some of them even on their personal machines, there could be higher chances of data breach. Having a fool proof recovery system in place could put companies at ease in these difficult times.

Detection of data abnormalities

Just as staying at home is the best precautionary measure to contain the spread of COVID-19, when it comes to data protection, prevention is always better than cure in most cases. There are certain patterns before the occurrence of any threats such as renaming or encrypting mass files, abnormal traffic from a site, and deletion of thousands of database records at once. However, manual monitoring of company's data systems can prove to be inefficient, tiresome, and expensive. With cloud data protection system in place, organizations are immediately alerted in case of any unusual activity.

Cost effective

In times when revenues and profitability have taken a serious hit, companies will look at cost-effective options to ensure smooth operations. IT budget will also be under scrutiny. However, with cloud-based data protection, they do not have to buy and maintain backup and other data system hardware and software. It eliminates the need to physically store backup media off-site and deliver it to or from that site daily. IT teams are not required to manage multiple data systems hardware and media. In case of a server or website crash, there is quick recovery, which means less business interruption and less revenue lost. Increased data visibility empowers organizations to make better managerial decisions.

Just as Indian companies had begun recognizing cloud adoption as a crucial catalyst for business transformation, the outbreak of the COVID-19 pandemic has made it a key enabler for ensuring business continuity. Galaxy along with Dell Technologies offers Data Protection solutions for cloud, multi-cloud and hybrid cloud helps customers transform their data centers to enable greater operational efficiency, resiliency and scalability throughout the entire cloud infrastructure.

For a free consultation,
please email us at marketing@goapl.com

https://bit.ly/2SclyLF

Special Focus

VMware Carbon Black

CB Protection, has a long history of innovation in the market. Many have referred to CB Protection as a pioneer in the application control market.

Application control (also known as whitelisting) is used to lock down critical systems and servers. It's also one of the strongest forms of protection and organization can use to keep its endpoints protected from attacks, lock down systems, prevent unwanted changes, and ensure continuous compliance with regulatory mandates, including Payment Card Industry Data Security Standard (PCI DSS).

In conjunction with this desire to keep critical systems safe, organizations are increasingly looking to replace legacy antivirus solutions. Legacy AV, while effective against most KNOWN malware, does very little to stop advanced attacks. That's where Carbon Black comes in.

CB Protection 8.1 includes a new "File Delete" feature, allowing customers to meet PCI DSS standards (requirement 5) to replace legacy antivirus (AV). Customers who want to remove legacy AV and run CB Protection on their compliant devices can now do so without going through the compensating control process.

CB Protection 8.1 empowers customers to comply with the Payment Card Industry Data Security Standard (PCI DSS) by:

- Simplifying implementation and support of TLS 1.2 communication
- Adding two - factor authentication to the CB Protection console
- Making CB Protection a direct control for PCI DSS requirement 5, enabling customers to remove legacy antivirus without the need for going through the compensating control process

Features of Carbon Black

Superior Protection

- Prevent both known and unknown attacks with the precision of unfiltered endpoint data
- Stop advanced file less and ransomware attacks through the power of streaming analytics
- Replace traditional antivirus, meet compliance requirements, and integrate your stack with ease

Continuous Visibility

- Access the complete activity record of every endpoint, even if it's offline.
- See what happened at every stage of an attack with intuitive attack chain visualizations.
- Uncover advanced threats and minimize attacker dwell time.

Proactive Threat Hunting

- Fast search, zoom, and visualization of process trees and timelines to pinpoint threats.
- Consolidate threat intelligence for your environment to automatically detect suspicious behavior.
- Correlate network, endpoint, and SIEM data through open APIs and out-of-the-box integrations.

Respond Immediately

- Isolate infected systems and remove malicious files to prevent lateral movement.
- Secure shell access to any endpoint with Live Response.
- Automatically collect and store detailed forensic data for post-incident investigation.

In today's changing world, working remotely is the new norm. Galaxy offers VMware Carbon Black solution which aids the customer to consolidate multiple endpoint security capabilities using one agent and console, helping them operate faster and more effectively.

Dell Technologies bolsters PC security for remote workers

Cybercriminals are opportunistic by nature, altering their attack methods to compromise endpoints and access critical data. This is never truer than during times of change such as now with the overnight shift to a global remote workforce. With cybercriminals ramping up activity, organizations need to protect their remote workers starting with the devices they use to get their jobs done.

One area attackers will target is the PC BIOS, the core system built deep inside the PC that controls critical operations like booting the PC and ensuring a secure configuration. To protect against BIOS attacks, organizations need built-in security solutions to protect endpoints. In response, Dell Technologies is introducing Dell SafeBIOS Events & Indicators of Attack (IoA) to further protect its commercial PCs. SafeBIOS Events & IoA uses behavior-based threat detection, at the BIOS level, to detect advanced endpoint threats.

With remote work increasing security gaps and the high economic pressure for businesses large and small to perform, Dell Technologies is arming customers with security solutions and best practices to better secure their PCs so they can stay focused on serving their end customers.

As workforces transition to remote work nearly overnight, organizations need to ensure their workers' PCs are secure, starting below the operating system in the BIOS. Securing the BIOS is particularly critical because a compromised BIOS can potentially provide an attacker with access to all data on the endpoint, including high-value targets like credentials. In a worst-case scenario, attackers can leverage a compromised BIOS to move within an organization's network and attack the broader IT infrastructure.

Organizations need the ability to detect when a malicious actor is on the move, altering BIOS configurations on endpoints as part of a larger attack strategy. SafeBIOS now provides the unique ability to generate Indicators of Attack on BIOS configurations, including changes and events that can signal an exploit. When BIOS configuration changes are detected that indicate a potential attack, security and IT teams are quickly alerted in their management consoles, allowing for swift isolation and remediation. SafeBIOS Events & IoA provides IT teams the visibility into BIOS configuration changes and analyzes these for potential threats – even during an ongoing attack.

Detection at this level allows organizations to respond to advanced threats quickly and successfully, interrupting the attack chain before it's able to do more damage. The SafeBIOS Events & IoA utility is available globally today for download on Dell commercial PCs as part of the Dell Trusted Device solution.

With remote work increasing security gaps and the high economic pressure for businesses large and small to perform. Dell End Point Security offers built-in security, comprehensive threat management and data security features that help protect your competitive advantage. Contact Galaxy's solution team for more information.

https://bit.ly/3eOwngT

Cloud spend hits record high in Q1 2020, up 34% due to remote working demand

Cloud infrastructure services spend hit yet another record in Q1 2020, growing 34% to US$31.0 billion. Growth in cloud services was driven by organizations around the world moving to remote working as the COVID-19 pandemic hit. As a result, enterprises sought rapid access to compute resources in the face of lockdowns and disruption. A surge in demand for online collaboration tools, ecommerce and consumer cloud services drove sharp increases in cloud infrastructure consumption, benefiting all the major cloud providers. But this was offset by a slowdown in large complex enterprise migrations and transformational cloud projects as businesses called a halt to all but the most important IT tasks as lockdowns took effect. Demand from digital companies that were impacted by the lockdowns in sectors such as hospitality and travel was also impacted.

AWS maintained its leading position in cloud services, accounting for 32% of the total market in Q1 as sales grew 33%. In dollar terms, AWS outpaced its key competitors once again. Microsoft's Azure sales increased 59%, taking its share to 17%. Capacity limits were reached for Azure in certain markets, though this was due to unprecedented use of Teams, which did not have a direct impact on Azure revenue. This also forced Microsoft to restrict consumption for some services and new customers. Google Cloud held onto third place in the worldwide cloud infrastructure market in Q1 2020, followed closely by Alibaba Cloud. Both had a 6% share of the total cloud infrastructure services market. Google Cloud saw healthy adoption of its data and analytics platform in some of its key verticals, led by the public sector, healthcare, service providers and financial services, though this was partially offset by weakness in other segments. Google Cloud continues to invest in an aggressive hiring strategy for Google Cloud Platform, across both enterprise sales and technical resources. Alibaba Cloud was one of the first cloud service providers to launch initiatives to support businesses affected by the lockdown in China, with free credits and access to its DingTalk collaboration suite.

"This is uncharted territory for cloud service providers, giving a boost to consumption but creating new and often challenging customer dynamics," said Alastair Edwards, Chief Analyst at Canalys. "Cloud has become an essential tool to support business continuity in these difficult times. Many organizations have turned to the public cloud for its burst capabilities to meet a sudden spike in use. Platforms such as Zoom would not have been able to operate without the flexible infrastructure provided by the major cloud providers."

Cloud service providers are responding urgently to the surge in consumption. Microsoft announced an emergency plan, which included adding new server capacity to its data centers in the worst-affected regions. AWS has opened two new data center regions in April, in Cape Town and Milan, with more planned in coming quarters. Google Cloud unveiled plans to open four new cloud data centers in Asia, Canada and the Middle East. Alibaba Cloud unveiled a US$28 billion investment to expand its cloud business worldwide over the next three years.

"Enterprises have been forced to rapidly change their IT infrastructure strategies and investment priorities in response to the pandemic," said Chief Analyst Matthew Ball. "Cost reduction and protection of capital are priorities as the global economy weakens. Anything on-premises that does not improve current business continuity initiatives has taken a back seat as companies rethink budgets in the face of growing uncertainty or struggle to access physical data centers. At the same time, companies around the world urgently need access to flexible compute capacity to support remote working, collaboration, online commerce and security. Cloud infrastructure is an obvious short-term solution. This has been a boon for most if not all the major players."

Yet this does not tell the whole story. Cloud service providers have also felt the negative impact of a slowdown in large consulting-led projects, including SAP migrations, hybrid cloud deployments and other transformational projects that have provided a big boost to cloud growth in recent quarters. Cloud investment in the worst-affected vertical segments, such as hospitality, aviation, construction, tourism and manufacturing, is being scaled down or delayed. This has offset some of the short-term growth enjoyed during the quarter.

Don't let multi-cloud complexity delay your cloud journey! Galaxy can help your organization extend a consistent solution set across private and public clouds. Our strong OEM partnerships help you create a lasting multi-cloud strategy that unifies environments and reduces risk across your clouds.

https://bit.ly/3bfpMcg