Integrating Technology, Driving Growth

TechTalk

GALAXY
Integrating Technology | Driving Growth

GALAXY OFFICE AUTOMATION PVT. LTD. Issue No. 111, September 2021

Upcoming Events

Hyperscale your cyber security Platform

Do join us for this exclusive event to learn how to hyperscale your Cyber Security platform with Checkpoint and Galaxy.

Event Topic-Check Point Maestro Hyperscale Network Security

A new way to utilize current hardware investment and maximize appliance capacity in an easy-to manage Hyperscale network security solution to bring our networks and data center to the world of hybrid clouds. With Maestro, organizations can simplify their data center workflow orchestration and scale up their existing Check Point security gateways on demand — the same way as they can spin up new servers and compute resources in public clouds.

Give your employees the Power of Mac

MD SPEAKS

Anoop Pai Dhungat
Chairman & MD

Dear Readers,

As things are slowly coming closer to what they were before the COVID-19 era, I wonder whether we will ever get back to those times. Every time, we think that it's over, a new variant of the virus raises it's ugly head in some part of the world or the other. More importantly, some of these are believed to even infect and severely affect the vaccinated. We are seeing new waves affecting parts of USA, Europe and now India. Though the number of hospitalisations and deaths are a fraction of what happened in the earlier waves, it is still a cause for caution. Essentially, we must learn to live with the virus by taking adequate precautions while going about our lives and businesses like earlier.

By the end of this month, most of us at Galaxy and our families will be fully vaccinated. I am proud to share that all through the complete and partial lockdowns, we have been able to serve our customers in the best possible manner while taking all precautions to ensure that our people and customers remain safe.

Do reach out to us to learn the areas where we could assist you to stay ahead of your competition by adopting cutting edge technology solutions.

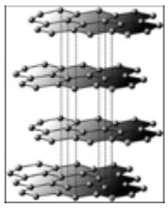
Happy reading

Future Is Now

Harder than a diamond, stronger than steel, super conductor ... Graphene Is Unreal

Imagine a material that is just one atom thick, 300 times stronger than steel, harder than a diamond, a fantastic conductor of heat and electricity and super-flexible to boot.

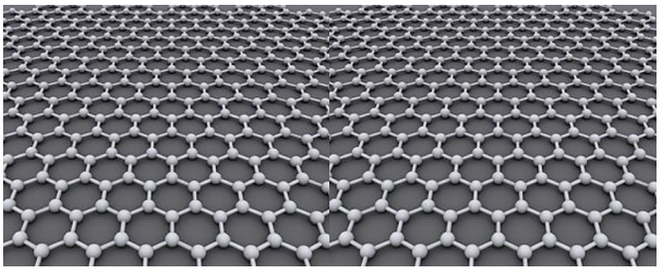
This might sound like the stuff of science fiction, but believe it or not, such a material already exists.The name of this super material is graphene and it is one of the most exciting prospects in science today.



The relationship between solid graphite and monolayer graphene.

In the latest graphene-related research – released last week – researchers from Vanderbilt University found a way to overcome one of graphene's most problematic flaws – a high sensitivity to external influences which causes graphene-based devices to operate more slowly than they should. The researchers found a way to dampen external influences on the graphene and could then observe electrons moving through their graphene three times faster than was previously possible. This development could pave the way for a new generation of graphene-based devices including touch screens and solar panels. Graphene is a new structural form of carbon – one of the most versatile elements in the universe. It was discovered in 2004 by Russian-born physicists Andre Geim and Konstantin Novoselov, who jointly received the 2010 Nobel Prize in Physics for their discovery.

Graphene is a single, flat layer of carbon atoms packed tightly into a two-dimensional honeycomb arrangement. The in-plane (two-dimensional) carbon-carbon bonds in graphene are the strongest bonds known to science. It is these bonds that give graphene its unbelievable mechanical strength and flexibility.



It is essentially a single layer of graphite, the material found in pencil "lead". When you draw on paper with a pencil, weakly bound graphene sheets in the graphite spread over your paper like a pack of cards.

But because graphene is so thin – the thickness of a single carbon atom – it is extremely difficult to see. This is one of the reasons it took researchers so long to find graphene sheets among thicker stacks of graphite. Despite being so thin, graphene is an excellent conductor of electricity. Electrons flow through graphene with almost zero electrical resistance. This unusual property, and the fact graphene is nearly invisible, makes it an ideal material for the transparent electrodes used in computer displays and solar cells. While scientists have known about graphene since 2004, it was in 2010 that researchers from Samsung and Sungkyunkwan University took a critical step in developing the commercial applications of this material.

They developed a scalable fabrication method which enabled them to produce transparent and flexible graphene electrodes measuring 30 inches (76cm) diagonally. This method enabled them to manufacture multi-layer electrode films and incorporate these into a fully functional touch-screen panel device capable of withstanding high strain.

As a result of this development, it won't be long before graphene will power the displays on your favorite electronic gadgets.One of the most promising aspects of graphene is its potential as a replacement to silicon in computer circuitry.

The hybrid workplace: Balancing trust and risk

While all signs are pointing to a future of work that combines working from home with time in the office, this puts employers at a difficult crossroad. Employers know that data breaches are far more likely to occur when staff is working away from the office.

Most enterprises just were not designed for remote working. For decades, India's workforce has been rooted in a repetitive business routine – a full workday with a hectic commute on either side. The Covid-19 pandemic has turned that model on its head, with masses of employees now demanding more flexible working policies from their employers long-term.While vaccine rollouts are gathering pace across the country, and many are predicting a return to "normal" in the future as a result, it's unlikely workforces will be returning to the office on a full-time basis in the short-term. Rather, hybrid models - a flexible approach that enables employees to blend working from different locations (home, on the go, or the office) are expected to become the norm.

In line with this, many organizations already have a plan for their employees to work from home one or two days a week, while some have even granted the opportunity to work remotely on a permanent basis.

A difficult crossroad

While all signs are pointing to a future of work that combines working from home with time in the office, this puts employers at a difficult crossroad. Employers know that data breaches are far more likely to occur when staff are working away from the office. In fact, according to data presented by the Indian Computer Emergency Response Team (CERT-In), the number of cyber security incidents reported across the nation in 2020 rose by over three times since 2019 and twenty times when compared to 2016.

Therefore, it has become imperative for employers to provide their employees the trust, confidence, and tools they demand to work flexibly wherever they want.

There are numerous safeguards IT leaders can deploy to reduce this risk, from ensuring staff receive adequate cyber security training to deploying anti-phishing protection. Businesses that have been forced to adapt quickly to this new way of working must also make sure that the defenses they have implemented to protect remote workers during the pandemic are no longer just temporary and are suited to supporting flexible working on a longer-term basis.

Stronger measures

As Indian organizations enter this new norm of hybrid work models, the first step that should be taken is to ensure staff have a virtual private network (VPN) installed on their laptop so they can benefit from the same security capabilities afforded to them in the workplace wherever they may be. When in the office, employees are usually surrounded by several rings of security - from email and gateway security to frequent software updates and on-hand security support - and it's important to ensure preventative measures are in place while they work remotely. After all, the riskiest cyber threats are the ones that haven't been detected yet, which means prevention is the ultimate cure.

According to IDC, by 2024, over 50% of enterprises will replace outdated operational models with cloud-centric models that facilitate rather than inhibit organizational collaboration, resulting in better business outcomes. In line with this, cloud security will be another important area businesses must tackle to ensure employees can securely work remotely. Video conferencing services, for example, have become extremely popular during the pandemic, but they are by no means infallible; there have been high-profile instances of threat actors gaining access to video meetings, particularly as more and more people work from home networks. With this in mind, businesses must implement stronger security measures, such as checking meeting links, requiring multi-factor authentication (MFA) and, importantly, ensuring employees are working on devices that have adequate protective measures in place.

Evolving threats

Opportunist hackers have dramatically shifted the way they operate as a result of the shift to mass remote working - something that will likely continue as businesses settle into a hybrid way of working. With employees working from laptops on home networks, phishing attacks have grown in popularity to become the most prevalent cybersecurity threat.

At Galaxy, we implement security solutions to ensure that your data is being accessed by the correct sets of people even though they are working remotely. We also offer productivity tools to ensure that there is no slacking or loss of efficiency by moving workloads to remote workers. Our portfolio comprises a wide range of Work From Anywhere Tools that can keep your business running efficiently even during lockdowns. These tools cover remote desktops, remote workstations, GPU virtualization solutions, employee productivity solutions, desk booking solutions, endpoint backups as a service, endpoint devices, remote working kits and a lot more.

Cloud Native Security-Security Automated Everywhere

Check Point cloud native security, delivered through Cloud Guard, provides automated security and advanced threat prevention to protect your cloud assets and workloads from the most sophisticated cyber-attacks. Secure your cloud and workload environment with one unified cloud native security platform—automate security posture management, gain visibility of threats, and control your workloads across clouds.

Unified Security for Multi-Cloud

Cloud Guard unifies cloud security to provide intelligent threat prevention. Securely protect and prevent threats across AWS, Azure, Google, VMware, IBM Cloud, Oracle Cloud, Alibaba Cloud, Kubernetes, etc. All from one platform. Provide centralized visualization for all of your cloud traffic, security alerts, assets and auto-remediation all from one platform.

Security and Posture Management

Through High Fidelity Posture Management, Cloud Guard delivers zero trust, multi-layer, advanced threat prevention, leveraging enriched intelligence with the highest levels of intelligence inputs, in context.

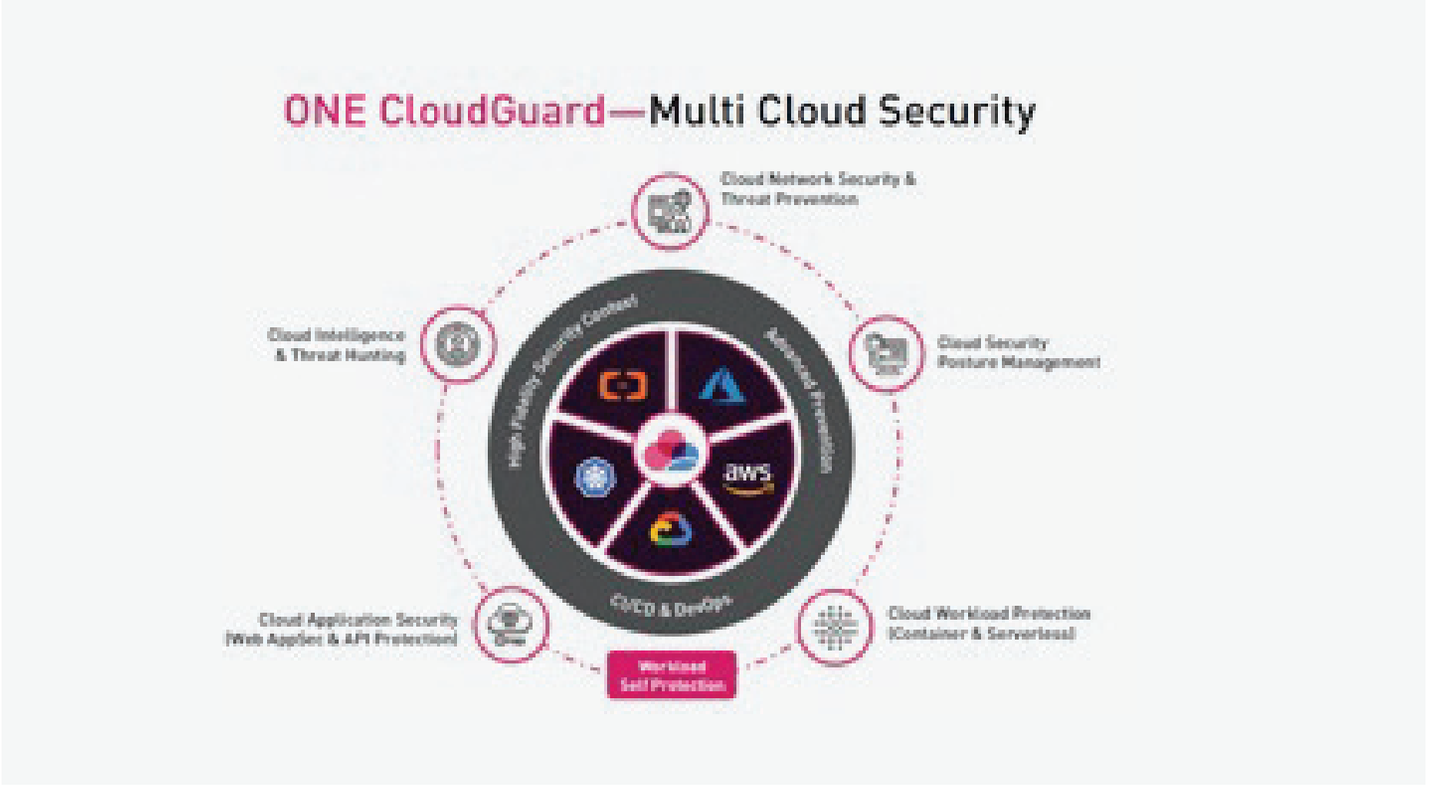
In addition, with its comprehensive compliance and security engine, Cloud Guard prevents critical security misconfigurations, and ensures compliance with more than 50 compliance frameworks and best practices.

Automated DevSecOps

Cloud Guard allows organizations to shift-left for DevOps to seamlessly evaluate security posture, configuration, and governance during CI/CD. Seamlessly scale and deploy your security in real-time through integration with tools like CloudFormation and Terraform and evaluate posture pre-deployment to scale across thousands of assets. Automatically define applications security profiles and enforce zero trust boundaries between workloads.

Cloud Network Security

Cloud Guard Public Cloud Network Security provides advanced threat prevention and network security through a virtual security gateway—automated and unified across all your multi-cloud and on-premises environments. cloud Guard provides cloud native protection with the industry's highest security effectiveness, and supports rapid deployment, agility, and automation of CI/CD workflows. Create consistent policy to manage security across on-prem and multi-cloud environments.



Special Focus

Cloud Security Posture Management

cloud Guard Cloud Security Posture Management automates governance across multi-cloud assets and services including visualization. Through cloud Guard High Fidelity Posture Management visualize and assess security posture, detect misconfigurations, model and actively enforce gold standard policies, in context and with enriched intelligence. Protect against attacks and insider threats, cloud security intelligence for cloud intrusion detection, and comply with regulatory requirements and best practices all from one unified platform.

Cloud Workload Protection

cloud Guard Workload Protection provides seamless vulnerability assessment and runtime protection of modern cloud workloads, including serverless functions and containers—automating security with minimal overhead across your multi-cloud environment. Continuously scan workload environments to increase security posture and provide continuous observability and assessment, with self-protection to continuously evaluate and adapt security posture.

Cloud Web App & API Protection

Cloud Guard moves application security closer to the edge of the workload, giving more real-time granular protection than a traditional Web Application Firewalls (WAFs). Cloud Guard protects web applications and APIs from the most sophisticated types of threats, with an automated, cloud-native security platform. Where traditional WAFs are built using “one-size-fits-all” rule tables even though no two applications are the same, Cloud Guard transcends rule-based security by leveraging the power of AI. Automation is a critical component which ensures that security is maintained even in dynamic app development cycles.

Cloud Intelligence and Threat Hunting

Cloud Guard Cloud Intelligence and Threat Hunting provides cloud-native threat security forensics through rich, machine learning visualization, giving real-time context of threats and anomalies across your mutli-cloud environment. Detect anomalies, activate alerts, quarantine threats, and remediate threats automatically, utilizing the largest threat intelligence feed.

Leverage unified cloud approach to drive agility

One of the aspects of leveraging cloud as the innovation platform – from creating test beds to trying new applications and tools or leveraging CI/CD or DevOps seamlessly.

Technology continues to advance at an impressive rate. Enterprises are grappling to meet business objectives with speed and agility. They are focusing on business strategies where the cloud can be the execution venue of modern technologies, which in turn, will help them achieve business goals, improved revenues, and efficiencies. To make businesses future-ready, companies are modernizing their IT infrastructure and increasingly investing in secure hybrid multi-cloud solutions with the hope to swiftly integrate new business channels and revenue growth. Another aspect of leveraging cloud as the innovation platform – from creating test beds to trying new applications and tools or leveraging CI/CD or DevOps seamlessly. But to leverage the true power of the cloud, CIOs or CTOs must have a cohesive cloud strategy in place. Even today, it is a challenge for them to ensure that these hybrids multi-cloud infrastructure work cohesively to achieve the true promise of the cloud: be it agility, scalability, automation, or cost-efficient operations.

Achieving business goals with cloud

A connected cloud ecosystem, application modernization, and secure cloud infrastructure are becoming the top priorities for CIOs and CTOs. A recent report by IDC, "India cloud predictions for 2021 and beyond," indicates that by 2024, over 50% of enterprises will replace outdated operational models with cloud-centric models and 20% will adopt connected cloud strategies to counter business challenges.

To achieve this, businesses need to build a confident cloud strategy to encounter the huddles around procurement, migration, data integration, and cloud management. The cloud strategy has to be aligned with the larger business objective, deliver business expectations, and offer a seamless, secure, and connected digital estate. CIOs must aim to become more agile and innovative, as they want businesses ready for the digital world. At the same time, businesses are also looking for an integrated platform where security takes the center stage to ensure a secure and compliant cloud infrastructure that is backed by resilient network connectivity. A hybrid multi-cloud ecosystem that can protect critical data and deliver business agility and cost-saving business operations can be the answer. It's imperative to identify the right-fit, however a cloud strategy can only be selected when companies evaluate business objectives in the context of IT architecture and the right shared responsibility matrix.