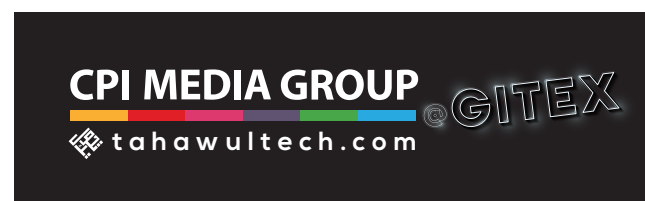




# 60 MINUTES

## GITEX TECHNOLOGY WEEK

Show dates: 16-20 October 2023, Dubai World Trade Centre | Exhibition hours: 10am-5pm



DAY 3 AM

## Commvault signs agreement with CSC UAE to strengthen national data protection

Commvault has signed a Memorandum of Understanding with the UAE Cyber Security Council at GITEX Technology Week 2023 in Dubai.

Commvault, a global enterprise leader in data management across on-premises, cloud, and SaaS environments, has signed a Memorandum of Understanding (MoU) with the UAE Cyber Security Council at GITEX Technology Week 2023 in Dubai.

The UAE Cyber Security Council was formed in 2020 by the Cabinet of the UAE



to support the UAE's ongoing commitment to safer digital transformation. The

Council is tasked with creating and developing regulatory and legal frameworks that focus on cybersecurity and cybercrime, as well as securing present and upcoming technologies in the region, all in the name of improving the country's cybersecurity outlook.

► CONTINUED ON PAGE 3

## Masdar City and Huawei join forces to accelerate net zero

Masdar City and Huawei signed an MOU at GITEX to power knowledge-sharing, enhance information systems, promote carbon-conscious information and communication systems, and promote Huawei's Net Zero Campus Framework.

Masdar City, a ground-breaking sustainable urban community in Abu Dhabi, and Huawei, a leading global provider of information and communications technology infrastructure, have joined forces through a Memorandum of Understanding that will help power the UAE's journey to net zero.

The agreement, signed on October 17 at



GITEX GLOBAL 2023 by key Masdar City and Huawei leaders, will lead to knowledge-sharing and capacity-building in net zero development, help reduce the carbon

footprint of Masdar City's information and communications technology (ICT) infrastructure, and

► CONTINUED ON PAGE 3

## Sophos anticipates business challenges for the year ahead

Harish Chib, VP, Sales - Emerging at Sophos discusses the company's channel goals and vision for the year ahead, the biggest challenges businesses are facing and the key technologies driving innovation.



Harish Chib

### What are your channel goals and vision for the year ahead?

We have launched our adoptive cybersecurity portfolio, which is a data lake with its own AI engine, as well as it has a global threat research team. We are providing threat intel to all our products and services, such as firewall, MDR services, email and Wi-Fi

► CONTINUED ON PAGE 4

## Resecurity introduces digital identity protection in UAE

Resecurity is dedicated to safeguarding citizens and businesses in the UAE from cyber threats.

Resecurity, Inc. (USA) is thrilled to announce the introduction of their award-winning Identity Protection (IDP) service in the United Arab Emirates (UAE). This cutting-edge IDP service, brought to you by Resecurity, is dedicated to safeguarding citizens and businesses in the UAE from cyber threats, effectively fortifying the UAE's Digital Frontier.

The grand launch of this service is taking place at GITEX Global



2023 in Dubai, a premier global technology event. Resecurity is proudly exhibiting their offerings in their state-of-the-

art pavilion (H2-B50), showcasing intelligence-driven cybersecurity,

► CONTINUED ON PAGE 4

## Pure Storage Simplifies Data Resilience and Enables an Enhanced Service Operations

New Disaster Recovery as-a-Service solution and scalable AI-powered management capabilities support secure, sustainable, and smart enterprise business operations.

Pure Storage, the IT pioneer that delivers the world's most advanced data storage technology and services, has announced critical new data resilience offerings, including the introduction of Pure Protect™//DRaaS, a unique Disaster Recovery as a Service (DRaaS) solution, new energy efficiency guarantees for its

Evergreen® portfolio, and scalable AI-powered storage services via its Pure1® management platform to global enterprises.

With the introduction of consumption-based disaster recovery via Pure Protect, a unique data resilience scoring system via Pure1, and updates to Evergreen subscriptions that include

a new Paid Power and Rack commitment, Pure Storage enables enterprises to adopt a complete, end-to-end storage strategy that assures data resilience, reduces labor costs, accelerates sustainability initiatives, and delivers unrivaled TCO benefits.

"Enterprises are challenged by an evolving business landscape -

innovation is up, but so are data security threats, energy sources are expanding, but climate change must be addressed, and labor participation is at an all-time high, yet budgets are tightening and talent is harder to find. The introduction of Pure Protect™ //DRaaS, unique Pure1 capabilities for subscription lifecycle



operations, and an industry-first sustainability commitment underscore Pure's pledge to deliver the most secure, smart, and energy-efficient storage services required by modern businesses," said Prakash Darji, VP and GM,

Digital Experience Business Unit, Pure Storage.

### Industry Significance:

The rate of devastating ransomware attacks and the increasing frequency of natural disasters are upending business continuity more often each day. While many organisations recognize the importance of a disaster recovery (DR) plan, current DR solutions on the market are complex, expensive, and disruptive. Likewise, the current energy crisis, new environmental

► CONTINUED ON PAGE 6





# CYBERSECURITY FOR ALL.

All threats,  
all businesses,  
all people.

*Get fierce defenses for a  
world of complex threats.*

**Barracuda.com**

**Barracuda will be at GITEX Global 2023  
Booth: H24 - C50**



▶ CONTINUED FROM PAGE 1

Commvault...

The collaboration will help protect UAE data and support government and private sectors with their continued digital transformation journeys. Commvault will support the UAE Cyber Security Council across cloud, both on premise and off premise workloads, whilst providing Risk Visibility on data protection. Commvault's team of global experts will also offer Ransomware recovery services, as well as proactive data security through Commvault's industry leading solutions. The agreement will help raise awareness of the dangers of cyber-crimes and outline best practices to ensure greater defence against data threats across the region.

HE Dr. Mohammed Al Kuwaiti Head of the Cyber Security Council of the United Arab Emirates Government said that the cooperation with Commvault, the leading



global company in the field of data management across local, cloud and SaaS environments, falls within the framework of the Council's keenness to enhance cyber security awareness culture in work places. Cyber security awareness enhances ways to confront cyber challenges and protect the privacy of digital information services for patients and the IT sector in general.

Dr. Mohammed Al Kuwaiti stressed the importance of protecting data, developing the skills of work teams in the field

of digital safety, and the ability to respond to any challenges related to data and the digital sector. He indicated that the Cybersecurity Council is building a robust base to establish a safe and solid infrastructure for cybersecurity in the UAE. The Council intends to make this topic an integral part of the internal work culture for institutions and individuals. This change represents an embodiment of the leadership's vision and the UAE's proactive approach towards addressing the various challenges

imposed by fast-paced digital technology transformation.

Dr. Al-Kuwaiti stressed that cooperation with Commvault is in this field comes in response to the rapid technological development in our contemporary world. This rapid development requires that we preserve health records, ensure information security and data privacy.

Yahya Kassab, Senior Director & General Manager – KSA & Gulf for Commvault, said: "We are proud to be partnering with the UAE Cyber Security Council

We are actively working with both government and private sector organisations to help guarantee greater data protection and ensure enhanced sustainability, productivity and flexibility with the use of data".

to provide cutting edge, AI driven, technologies to protect and manage UAE data. The nation has been ahead of the curve for many years by launching a clear Cyber Security strategy and vision, whilst continuing to grow and develop in the midst of rapid digital transformation. Today we are witnessing increasing Ransomware threats and cyber challenges both in the UAE and wider region. We are actively working with both government and private sector organisations to help guarantee greater data protection and ensure enhanced sustainability,

productivity and flexibility with the use of data".

Commvault's modern data protection platform delivers a unified customer experience, helping them secure, defend, and recover their data on-premises, at the edge, or in the cloud. Customers rely on Commvault for the broadest support of legacy applications, modern workloads, and SaaS applications, all managed through a single intuitive platform. With Commvault, customers get enterprise-grade data protection that delivers agility and cost optimisation in the hybrid world.

▶ CONTINUED FROM PAGE 1

Huawei...

promote the adoption of carbon-conscious ICT through Huawei's Net Zero Campus Framework. The framework, released earlier this year, is designed to help organizations reduce the energy demand of ICT systems and operations while switching to clean energy.

Masdar City, already home to one of the largest clusters of LEED Platinum buildings in the world, has three net zero energy buildings currently under construction, the first of which will be completed in October 2023. Huawei is home to several low-carbon campuses and is creating new technologies to support sustainability as one of their strategic priorities.

"Masdar City already develops the most high-performing, energy-

This new partnership will be a powerful enabler for decarbonisation".

efficient buildings in the region", said Mohamed Al Breiki, Masdar City's executive director of sustainable real estate. "Optimising ICT systems is a vital step in reducing our energy demand even further and cutting tech-related carbon emissions. This is yet another way for us to help lead the way for other cities who want to chart a course to net-zero".

"We are delighted to announce our partnership with Masdar City to accelerate the UAE's journey to net zero", said Safder Nazir, Senior Vice President, Public Sector, Huawei Middle East and Central Asia. "Through this MOU, we aim to empower knowledge-sharing, promote the

drive toward carbon-conscious ICT to reduce tech-related carbon emissions, and promote Huawei's Net Zero Campus Framework. We recognise that technological innovation plays a crucial role in sustainable development, and this collaboration with Masdar City will set a benchmark for the cities and campuses of the future".

In addition to optimising existing ICT systems at Masdar City, Huawei will advise on Masdar City's upcoming Command and Control Centre, which will feed data related to energy, water, and waste management in all Masdar City-owned

buildings to a central location. This will allow facilities managers to monitor and improve building performance in real-time.

Masdar City will look for opportunities to amplify Huawei's Net Zero Campus Framework, launched earlier this year to support organizations that wish to decarbonize. The Huawei Net Zero Campus Framework recommends a stepwise approach towards a net zero campus. This could begin with addressing

campus operations, along with net-zero energy development.

A smart campus solution supports a collaborative work environment, while a net zero energy campus implements key energy initiatives such as reducing energy consumption, generating energy onsite, and actively managing energy consumption and energy trading. The net zero-carbon campus strives for a net zero balance between the carbon emitted into the

atmosphere and the carbon removed from it.

Al Breiki signed the MOU on behalf of Masdar City, while Nazir signed the agreement for Huawei.

"We have always known that technological innovation helps drive sustainable development", said Al Breiki. "This new partnership will be a powerful enabler for decarbonisation. We look forward to setting an even higher benchmark for how cities of the future will operate".





▶ CONTINUED FROM PAGE 1

## Sophos...

protection. We are trying to educate our partners to move away from coin product selling and go into a more trusted advisor role for their customers. This means you have to start adding a layer of services to your customers. We're training them to become a kind of managed service providers, so they engage daily with their customers.

**From your company's perspective, what are the biggest challenges businesses are facing and how do you work with partners to solve these?**

There are a couple of challenges in the GCC region. One is a geopolitical challenge as we need to make sure that the nations are sharing information and

they're cooperating with each other, which due to complex relationships, is sometimes difficult. This creates a challenge for customers too.

The second challenge is resource constraint as they have limited budgets and a lack of skill manpower with customers. When it comes to cybersecurity, the digitalization has happened so fast in our region that it's getting difficult for businesses to keep pace with the cloud adoption. Therefore, it's getting challenging for customers to manage all of this with their limited budget.

Thirdly, it's getting really difficult to always keep upgrading and chasing your network making sure it's always up to date and protected. The attackers are getting very smart and are doing targeted attacks, so it's better for companies to adopt cyber resilience, which isn't just getting

**We need to make sure that the nations are sharing information and they're cooperating with each other, which due to complex relationships, is sometimes difficult".**

yourself protected, but getting ready in case these attacks happen, what is your readiness and how well you are equipped to come back or to mitigate these threats and make sure that your business suffers minimal damage and you are back up and running to serve your customers and clients. Cyber resilience is one of the challenges we are seeing, so partners need to educate their customers and every company can develop it with the help of Sophos

range of products and services. That's our goal for partners.

**How important is an event like GITEX Global for your company – and what value does it bring for your organisation?**

Sophos has been participating at GITEX for more than 14 years, and this has been one of the best leading platforms for us to demonstrate all our product launches and services. It's a platform where we exchange knowledge and get some information

on direct conversations with not only existing customers, but also potential prospects. We get to learn about what's the new thought process of the business, what CSOs are thinking about it, what their priorities are for the upcoming years and what the major issues are.

This platform gives us that direct engagement with customers and our partners. We've been busy working with all the partners, but this is the time when we talk about, not exactly business, but strategic discussions with each other about their growth plans and market trends.

**From your company's perspective, what are the key technologies and trends that you're seeing that will drive your innovation and product roadmap for the next 12 months?**

We have recently launched Sophos incident response service for 45

days for any customers, which are actually in active threats or active attacks, and they need immediate help. This means rather than going into all the red tape process, they can directly come to us within a day and we'll start working to make sure we mitigate and utilize those threats and we provide them 24/7 45 days monitoring services to ensure they are now stable and there are no such attacks happening. This is one of the key services we have launched.

Apart from that, we are also working very actively in our network firewall space, ZTNA services and cybersecurity as a service for our customers. We are also working on launching new access points and Wi-Fi six days access points for the market. We are constantly evolving, developing our AI based spread intel model and driving more automation to reduce the noise level of attacks.

▶ CONTINUED FROM PAGE 1

## Resecurity...

threat intelligence, and risk management solutions.

Gene Yoo, CEO of Resecurity, stated, "Identity Protection by Resecurity is pivotal in fortifying Dubai's digital infrastructure and bolstering the Emirate's digital economy. This Resecurity solution is designed to shield both citizens and businesses from the escalating risks of account takeover, fraudulent activities, and malicious online behaviours. Its mission is to empower society to protect online identities and minimise the perils of account takeover, personal data breaches, online-banking theft, and scams. We are proud that



our solution has already saved multi-million dollars for major Fortune 100 organisations in North America, LATAM, and APAC. Now, we are thrilled to extend its protection to one of the world's largest business, trade, and digital economy hubs in the Middle East".

The availability of this groundbreaking service in the UAE follows the introduction of the second cycle of Dubai's Cyber Security Strategy by Sheikh Hamdan. This strategy aims to create a society that is safe from cyber threats, and Resecurity's

Identity Protection (IDP) solution will assist countless consumers and companies in the UAE in pursuing this goal. Victims of cybercrime will have the means to safeguard their accounts and personal data through continuous monitoring and proactive early-warning notifications.

Christian Lees, CTO of Resecurity, affirmed, "We are excited to bring Resecurity's IDP service to citizens and businesses in the UAE, showcasing its advanced features and capabilities. Our goal is to empower individuals to take control of their online presence, ensuring protection from identity theft, fraud, and other malicious activities. With Resecurity's IDP, users can confidently navigate the digital landscape, knowing that their personal information is secure".

Cyber threats targeting digital identities have become a significant issue in the Middle East, resulting in online banking theft, fraud, and other scams. These malevolent actions also inflict damage upon enterprises through network intrusions, intellectual property theft, and data breaches, resulting in significant

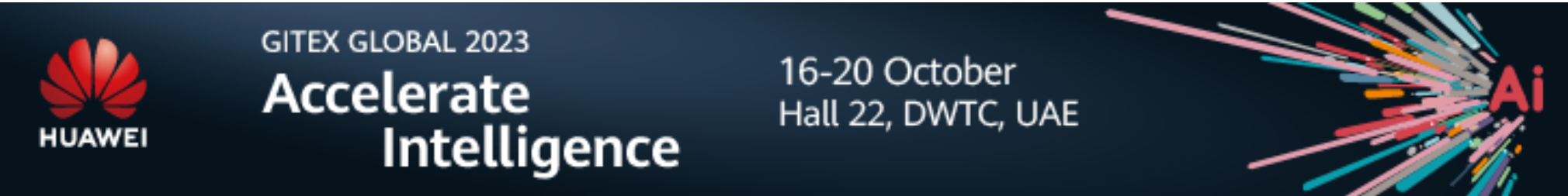
financial and reputational harm.

Resecurity has launched a new service specifically to aid users in safeguarding their online identities. This service actively monitors stolen data, specifically searching for leaked passwords, national identification documents, personal information, and payment data —items frequently peddled by cybercriminals on the dark web.

Shawn Loveland, COO of Resecurity, explained, "Resecurity is pioneering accessible cybersecurity services, making them available to everyday citizens who may not be fully aware of the lurking cyber threats. Cybercriminals often exploit the digital identities of children, women, and law-abiding individuals to commit cybercrimes and fraud, causing detrimental impacts on the victims' personal lives and privacy".

For more information regarding Resecurity and its comprehensive cybersecurity solutions, please visit the official company website at <https://www.resecurity.com>. For real-time updates and information about GITEX Global 2023, and how to participate, please visit the event's official website at <https://www.gitex.com>.

**Identity Protection by Resecurity is pivotal in fortifying Dubai's digital infrastructure and bolstering the Emirate's digital economy".**

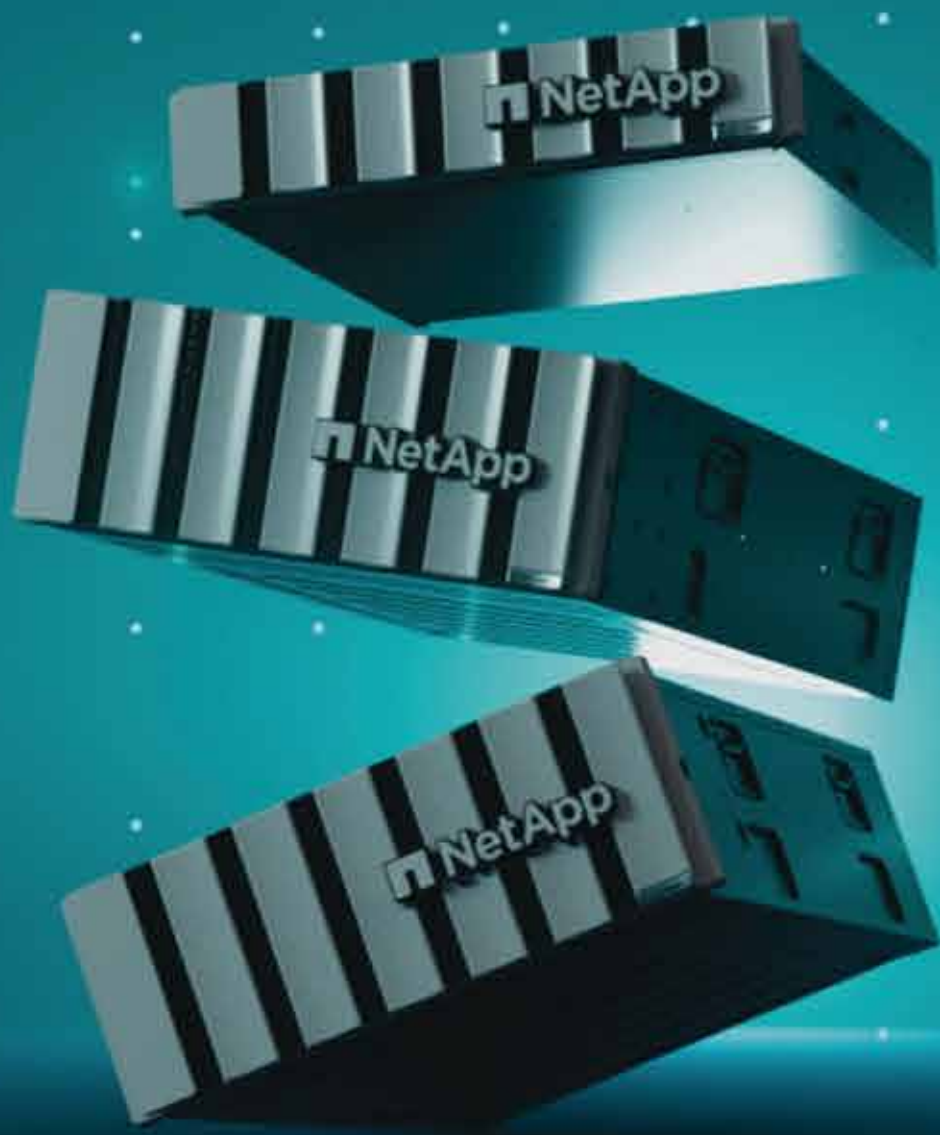






# Flash forward to the future

All flash for every budget.  
Simple, secure, and sustainable.



For more information contact : [netapp@logicom.net](mailto:netapp@logicom.net)  
or visit: <https://distribution.logicom.net/netapp/>



► CONTINUED FROM PAGE 1

## Pure Storage...

regulations, and ethical imperatives to improve corporate sustainability have led companies to set ambitious net-zero goals, but reckoning with the typical data center’s power demands has remained challenging. And with digitization at scale and data proliferation and fragmentation, end-to-end operations management further aggravates the skill and budget shortages for IT.

Today’s introduction of Pure Protect //DRaaS and updates to the Pure Storage Evergreen portfolio not only address these critical industry pain points, but also set new milestones for customer-centricity with compelling guarantees.

### News Highlights:

- **Assured Data Resilience:** Pure Storage enables enterprises everywhere to maximize data protection with a complete, multi-layered data resilience strategy built from the ground up. With intrinsic data protection built into its Evergreen architecture via ActiveDR™, ActiveCluster™, and SafeMode™ Snapshot capabilities, Pure Storage



Prakash Darji

has now expanded data resilience with new trusted operations capabilities and a new disaster recovery service:

- **Pure Protect //DRaaS,** a new consumption-based Disaster Recovery as-a-Service solution, drastically reduces complexity, cost, recovery time, and business disruption in the wake of disasters and cyber disruptions. Organizations now have clean environments with multiple restore points to recover clean copies of their on-premises vSphere data, to native AWS EC2, no matter

- what underlying storage infrastructure it is, while ensuring data centers remain isolated for investigation.
- **Data Resilience Score,** within the Pure1 Data Protection Assessment, underscores Pure Storage’s trusted operations by providing better transparency in the adoption of Pure Storage and industry-leading data protection and backup partner technologies, while offering the ability to assess entire fleet configurations against leading practices.
  - **Zero Data Loss Guarantee,** across the

- Evergreen portfolio, provides peace of mind that customers data will not be lost due to Pure Storage hardware or software issues. In the rare case of any data corruption, Pure Storage assures data protection with advanced data recovery services for any hardware or software product-related incidents, at no cost.
- **Enhanced Service Experience, Everywhere:** With Pure Storage’s AI-powered asset and lifecycle management services and policy-based automation, customers can achieve operational excellence, anywhere and on any scale.
  - **Asset Management and Genealogy** allows customers and Pure Storage to jointly optimize Labor costs to run and operate storage. Customers get full transparency to manage Evergreen assets, contracts, subscriptions, and lifecycle, and get visibility into capacity, energy, and rack space usage. Customers can also view how each asset or subscription has evolved over time, including software updates, ramps, expansions, and renewals, and gain insight into upcoming lifecycle events such as EOL, upgrades, or

- contract expiration.
- **Subscription Lifecycle Operations:** Customers now benefit from a subscription viewer to understand when subscriptions require attention and renewal, predictive tracking of capacity utilization with actionable alerts to optimize reserve commit vs on-demand consumption, and new SLA indicators to track how well Pure Storage is meeting performance and efficiency SLAs. Customers can plan for future demand, trigger in-app workflows to request quotes, or use the new Pure1 Marketplace for a simplified subscription shopping experience. Partners can take advantage of these capabilities via APIs and early notifications of lifecycle events (EOL, renewal) to deliver seamless procurement experiences to joint customers.
  - **Policy-driven Upgrades** take the guesswork out of choosing the right Purity release and simplify fleet management. They help customers strike the right balance between frequent upgrades and maintaining a secure and supported storage environment based on their organization’s goals.
  - **Pure1 Mobile App** enables customers to get insights

- and alerts even on the go as well as manage cases and get the latest information and news from Pure anywhere in the world.
- **Guaranteed Energy Efficiency While Saving Money:** With the only Paid Power and Rack Space commitment in the enterprise Storage as-a-Service market, and unique energy, density, and upgrade guarantees, Pure Storage is not only committed to providing the most sustainable storage solutions in the industry, but is also determined to make being green easier and more affordable for global customers.
- “Asset tracking and subscription management have long been challenges for any enterprise organization, creating bottlenecks, driving unexpected costs, and hindering productivity of our staff. The latest AI-powered asset management capabilities within Pure1 have enabled us to both improve consumption of our existing subscriptions, while transparently tracking SLAs, and effectively and accurately manage our storage infrastructure – from capacity utilization to renewals - from a single management platform,” said Josh Holst, Vice President of Cloud Services, Involta.

# Mozn and UAE-based Astra Tech Partner To Fortify Fintech Security Via AI-Capabilities

The AI powerhouse forges strategic alliance with the tech pioneer to unleash innovation and security in fintech.



Regional AI powerhouse Mozn, a leader in enterprise AI technologies, inked a landmark partnership with Astra Tech, a pioneering, UAE-based tech company. This alliance aims to strengthen their joint ability to tackle unique compliance challenges in local and global markets while setting a course for international expansion.

This collaboration aligns seamlessly with the growth

strategies of both Mozn and Astra Tech, offering a compelling synergy between their distinctive strengths. The partnership was signed at the Fintech Surge event held recently, in the presence of Dr. Mohammed Alhussein, CEO and Founder of Mozn, and Abdallah Abu Sheikh, Founder of Astra Tech and CEO of Botim.

This strategic move not only supports Mozn’s

expansion goals into the UAE market but also aligns perfectly with its dedicated efforts to strengthen the compliance framework in the country. The objective is to enhance the overall compliance landscape, promoting increased safety and transparency in financial operations. With Astra Tech’s PayBy-powered Botim platform consistently breaking

traditional banking barriers, this partnership ensures that the app’s 150 million users can operate the offered fintech capabilities with an additional layer of security.

“Mozn’s alliance with Astra Tech is a robust union aimed at fortifying the financial infrastructures of tomorrow”, said Dr. Mohammed Alhussain, CEO and Founder of

Mozn. “By combining our AI-driven compliance solutions with Astra Tech’s unique business model, we’re setting a new industry benchmark for rigorous compliance and financial fraud prevention. The dynamism and growth potential of the UAE market inspires us, and we are uniquely positioned to address its compliance complexities. Together, we’re not just expanding our geographical footprint; we’re strengthening the very fabric of global financial security”.

Abdallah Abu Sheikh, Founder of AstraTech & CEO of Botim said: “Our collaboration with Mozn is a strategic leap forward in realizing our Ultra app vision swiftly, showcasing the robustness of our innovative fintech products. Our PayBy-powered Botim app has seamlessly evolved into a comprehensive platform, offering a diverse array of financial services, from peer-to-peer transactions and international money transfers to prepaid cards. The platform’s inclusive approach empowers individuals who lack traditional banking access to seamlessly conduct global transactions, benefiting both users and merchants. Moreover, our

**Our collaboration with Mozn is a strategic leap forward in realizing our Ultra app vision swiftly, showcasing the robustness of our innovative fintech products”.**

fintech capabilities are further fortified with the integration of AI-powered anti-money laundering (AML) solutions like FOCAL, ensuring enhanced security and compliance across our offerings”.

Mozn continues to lead efforts in strengthening the global financial industry, with its flagship platform, FOCAL, at the forefront. FOCAL has conducted over 2 billion checks to empower clients in improving customer experience efficiency while achieving compliance through a risk-based approach. This commitment to excellence has garnered FOCAL recent accolades, including a spot among the Top 200 FinTech Companies globally and one of the Top 25 in the “Digital Business Solutions” award by practitioners’ organizations’

# DigiGlass by Redington Re-Imagines Security Operations Center at GITEX Global 2023

DigiGlass experts will host live technology sessions on the importance of AI and OT security and attendees can understand better how they can elevate their cybersecurity postures effectively.



Dharshana Kosgalage

At GITEX Global 2023, DigiGlass by Redington, managed security services brand of Redington, a leading technology integrator and innovation powerhouse,

is highlighting its revolutionary Security Operations Center, reaffirming its commitment to re-imagining cybersecurity in the digital age. The MSSP brand's

participation at the iconic five-day tech show revolves around three facets – offering AI-embedded advanced capabilities in cybersecurity, preventing disruptions with robust

OT security, and leveraging data analytics to safeguard businesses from emerging threats. AI is pivotal in fortifying cybersecurity, offering unique capabilities to identify, thwart, and counteract evolving cyber threats. Through sophisticated algorithms, AI can scrutinize extensive datasets, pinpointing irregular patterns indicative of potential cyber threats or suspicious activities. Spanning anomaly detection, real-time threat intelligence, predictive analysis, and automated incident response, organizations can significantly strengthen its cybersecurity resilience. Equally vital is the establishment of a resilient OT security strategy, safeguarding industrial control systems and critical infrastructure from cyber threats. At a time when cyber threats are growing in complexity, DigiGlass signifies a revolutionary change in cybersecurity solutions. DigiGlass

**DigiGlass’ SOC has expanded over the last few months, in response to escalated threat landscape, and offers continuous monitoring of network traffic”.**

is a comprehensive cybersecurity framework designed to safeguard organizations against evolving cyber threats and vulnerabilities. DigiGlass’s SOC is a centralized unit embedded with capabilities for monitoring and managing customers’ security hygiene. It comprises cloud-based

cybersecurity and OT security offerings with country specific data sovereignty compliance. Customers can benefit from the completely automated framework and monitor their environments within a single pane of glass. Dharshana Kosgalage, Head of Technology Solutions Group, Redington Middle East and Africa, said, “DigiGlass by Redington uses threat intelligence and machine learning to proactively identify and mitigate advanced cyber threats. DigiGlass’ SOC has expanded over the last few months, in response to escalated threat landscape, and offers continuous monitoring of network traffic, user behavior, and system activities, providing real-time insights into potential security risks. At GITEX Global, we are hosting thought leadership sessions and showcasing our comprehensive portfolio of solutions to help customers safeguard their digital future.” Meet the DigiGlass by Redington experts at Stand A1 in Hall 5 to know more on how you can re-imagine your cybersecurity strategies for the digital future.



## Do More With Sharepoint And Power Platform

- ✔ Improve internal collaboration
- ✔ Maintain Business continuity
- ✔ Enhanced employee productivity
- ✔ Quick & informed decision making
- ✔ Compatibility across multiple devices
- ✔ Reduces Third-party tool dependency

Get started today!

+97317700777  
acsales@almoayyedcomputers.com  
www.acme.tech

+914040117924  
sales@acmeglobal.tech  
www.acmeglobal.tech





# Juniper Networks expands on AIOps leadership with new Cloud Instance

Juniper Networks expands on AIOps global leadership with New UAE Local Cloud Instance driven by Mist AI.



Juniper Networks, a leader in secure, AI-driven networks, recently announced that its wireless access, wired access, NAC, indoor location and SD-WAN solutions, all driven by Mist AI, will have a local cloud instance in the UAE. Juniper customers and partners in the region will receive the benefits of a cloud-native

architecture, which includes microservices agility, resiliency and elastic scale, as well as local hosting and storage. In the Middle East, it is becoming increasingly important to validate where data is stored due to data privacy and cybersecurity concerns. The launch of the Juniper UAE Cloud instance helps to align with security

standards, enabling Juniper to deliver more secure, resilient and automated AI-driven cloud services in support of digital transformation initiatives while their data is stored on a locally hosted cloud. The Juniper Mist solutions deliver unsurpassed automation, insight and assurance for simplified operator

experiences and exceptional user experiences. The entire Juniper campus and branch portfolio is managed via a common Mist cloud and AI engine for assured client-to-cloud experiences across the wired, wireless and WAN domains. Proactive actions and self-driving network operations avoid problems before they

arise, eliminating as many as 90 percent of inbound trouble tickets. Juniper has also been named as a Leader in the 2022 Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure for the third consecutive year, with Juniper being placed highest in execution and vision. The company is recognised as the only Visionary in the 2023 Gartner® Magic Quadrant™ for SD-WAN. “Many UAE organisations integrate cloud-driven AI services into their broader IT strategies, making cloud services essential for the future. Juniper has seen substantial traction for our AI-driven campus and branch portfolio with top enterprises choosing the company’s best in class solutions, operated via the cloud. To further boost this momentum, Juniper will offer a strong cloud instance in the UAE, promoting digital transformation, spurring innovation and reducing operational costs for enterprises throughout the UAE and the extended Gulf region”. - Yarob Sakhnini, Vice President, Emerging Markets, EMEA at Juniper Networks

**Juniper will offer a strong cloud instance in the UAE, promoting digital transformation, spurring innovation and reducing operational costs throughout the UAE”.**

“Cloud adoption is snowballing in the Middle East, driven by widespread efforts by organisations to modernise their infrastructure and applications. There is also a significant shift in the regulatory environment, which is pushing companies towards secure and compliant cloud solutions. As a result, most enterprises in the region are increasingly preferring locally hosted cloud solutions”. - Jebin George, Senior Research Manager – Software & Cloud, IDC Middle East, Turkiye & Africa

# Avaya unveils cutting-edge solutions for enhanced customer experiences

Veronica Martin spoke to Ahmad Dorra, Customer Engagement Solutions Sales Leader MEA & Turkey at Avaya to discuss their new products and solutions and GITEK Global, the key technologies and trends driving innovations and how important GITEK Global is for Avaya.

Can you tell our readers what new products and solutions you are demonstrating and launching here this week at GITEK Global?

We, at Avaya, are a leader in customer experience and have been helping a lot of brands and government entities guiding them towards reaching their desired customer experience. As we know each organisation has a unique position in their customer experience journey, this insight leads us as a buyer to deliver a unique approach to our customers. This year we are looking at the new

**We will be showing our customers how we can integrate our technology without disrupting their digital transformation journey”.**

branding and customer experience integrating AI in all verticals. This means we are implementing generative AI beyond just the persona that we used



Ahmad Dorra

to demonstrate before and taking it across all personas within the organisation in order to empower all employees at all levels. From your company’s perspective, what are the key technologies and trends that you’re seeing that will drive your innovation and product roadmap for the next 12 months? Generative AI is the

evolution of AI and the key trend today’s market. We are seeing all customers want to adopt to the digital transformation and also a big hype on analytics, as they really want to leverage their analytics to understand how their business is going and what people are talking about their brands. We are focusing to deliver this style of innovation to our customers, but,

at the same time, we need to make sure that we’ll deliver without disrupting their current operation. That’s what I call it, innovation without disruption. How important is an event like GITEK Global for your company – and what value does it bring for your organisation? GITEK has become huge worldwide and a

great opportunity for us to demonstrate our power, what we are doing to become more innovative and what we can deliver to our customers. Besides, we will be showing our customers how we can integrate our technology without disrupting their journey. They can choose their journey at their own pace, and we are here to support them to deliver it in the most effective way.



# Catalyst of change

Anita Joseph caught up with Ranjith Kaippada, MD, Cloud Box Technologies, to find out how the company is playing a pivotal role in safeguarding businesses against evolving cyber threats and ensuring seamless digital transformation.



CLOUD BOX  
TECHNOLOGIES

**Could you provide an overview of the comprehensive solutions portfolio offered by Cloud Box Technologies and how the company contributes to the smooth and seamless digital transformation journey of businesses?**

In recent years, the surge in digital transformation has been palpable across various industries in the UAE. Companies are increasingly recognising the value of this shift and the associated business benefits that it brings. However, this journey is not without its challenges. In fact, there are many uncertainties surrounding digital transformation, often overlooked or misunderstood by people. However, these uncertainties must be openly discussed and effectively addressed to ensure its successful implementation and resolution.

Amid the buzz surrounding digital transformation, Cloud Box Technologies (CBT) steps in as an expert consultant, guiding businesses through a step-by-step progression in this transformative process. Recognising that each customer's journey is unique, CBT tailors its solutions to the specific needs of each client, capitalising on digital technologies to elevate businesses to the next level.

Since every customer has a unique profile, it makes it impossible to standardise digital transformation technology or processes across all companies. Therefore, it is imperative to base our approach on understanding each customer's experience and focus on the key areas where digital transformation can make an impact. At CBT, we analyse the various digital technologies that can elevate businesses to the next level, acting as a catalyst for this progression. For instance, the requirements for a hospital will differ from those of a retail business or the banking sector. Precisely comprehending each customer's needs is a

**At CBT, we analyse the various digital technologies that can elevate businesses to the next level, acting as a catalyst for this progression.**

fundamental step. Investing in data and analytics is a significant undertaking, albeit expensive, and while the market offers numerous reporting and data analytic tools, the question of investment readiness arises. As a System Integrator, we firmly believe in the necessity of these tools to drive transformation. Guiding customers towards the right product and tool selection, as well as effectively consolidating and deriving valuable insights from data, is a key service we provide.

Stepping into the realm of technology, we leverage our expertise to guide customers through the adoption of new technologies. Our approach varies based on the specific industry, be it healthcare, banking, or others. While our uniqueness lies in our market approach, success hinges on effective consultation and providing accurate information to customers. Our role is to understand industries, recommend the most suitable technologies for business profitability and cost reduction, and guide customers seamlessly through the whole process.

In short, as the momentum behind digital transformation grows, CBT acts as an advocate for customers, providing expert guidance that ensures a smooth and purposeful digital transformation. Instead of offering standardised solutions, CBT pinpoints core areas where transformation is required based on each customer's unique experience and objectives.

**For digital transformation to be seamless, there**

**needs to be the right set of skills. Do you think there is enough skilled workforce out there today to meet the demand for new technology implementation? How does Cloud Box Technologies address the scarcity of skilled professionals?**

The shortage of skilled professionals is a pressing issue in today's market. Convincing CEOs and investors of the importance of technology adoption can be challenging, as the understanding of its implications often varies between C-level executives and the general workforce. Bridging this gap requires a bottom-up approach, where employees across all levels comprehend the significance of digital transformation. CBT recognises this necessity and employs a specialised team of skilled engineers who possess the expertise to understand customer needs and effectively facilitate the transformation. We ensure that the right skill sets are in place to guide clients through successful digital transitions.

We step in as a specialised technology partner, differentiating ourselves from other resellers by being a Value-Added Service Provider. Our focus is sharp – we select specific verticals, and at present, our strength lies in the healthcare sector, along with hospitality and retail industries. CBT excels in identifying gaps within individual verticals, enabling us to pinpoint the necessary skill sets to address specific needs. Our team consists primarily of technically skilled engineers who adeptly grasp customer requirements and provide the right solutions. Our current success is underscored by the simultaneous management of nearly a dozen products, ensuring that our experts are strategically positioned to guide customers through a successful digital transformation. This track record of accomplishment has led to an increasing trust in our capabilities year after year.

**Can you elaborate on the significance of Security Operations Centers (SOCs) in today's landscape and how CBT contributes to securing businesses against advanced cyber threats?**

Digital transformation is not an isolated activity. It is not just enough to implement extensive technological changes, safeguarding these investments also becomes paramount. Security Operations Centers (SOCs) play a pivotal role in this aspect, and CBT's SOC provides round-the-clock monitoring and support, ensuring that no cyberattacks compromise a business's digital infrastructure. While many SOC merely detect threats, CBT's SOC goes further by enabling instant response and recovery.

Our SOC service offers a comprehensive approach to cybersecurity that combines advanced technology with human expertise. Our team is equipped with the latest tools and technologies to detect and respond to cyber threats in real-time. We also have a deep understanding of the threat landscape and can anticipate new attack vectors before they even emerge. This holistic approach safeguards against data loss and ensures rapid recovery in the event of an attack, setting us apart in the market.

Our SOC service can also help you meet regulatory compliance requirements. Many industries are subject to strict data protection regulations, such as HIPAA and GDPR. Failure to comply with these regulations can result in hefty fines and legal penalties. Our SOC service can help you stay compliant by monitoring your systems for any potential violations and providing you with regular compliance reports.

**How is SOC expected to help CBT, particularly with its future growth plans?**

Cyberattacks and cybersecurity are here to stay, just as we anticipate virus attacks and counteract them with antivirus solutions. The prevalence of

widespread cyber-attacks and security breaches is undeniable, but defending against this onslaught is the challenge. Although multiple Security Operations Centers (SOCs) exist, not all offer round-the-clock protection within the UAE. Many rely on foreign operations and manpower, lacking local presence. This is precisely where CBT takes the lead. We're making substantial investments in a 100% local SOC, based in the UAE, ensuring continuous monitoring of potential threats. Our skilled team of engineers, well-versed in SOC dynamics, local intricacies, and cutting-edge technology, provides end-to-end support. This commitment differentiates us from competition; we're here to demonstrate unwavering support to our customers at every step.

**We all know that the future is unpredictable, with rapid technological advancements and ever-growing cyber threat-attack vectors. So, what is CBT's go-to market strategy going to be, for the GCC market in particular?**

CBT's strategy revolves around teamwork, collaboration, and differentiation. Rather than serving as a mere intermediary, CBT positions itself as a digital transformation enabler. By bridging the gap between vendors and customers, CBT ensures that technology messages are effectively translated and implemented. This unique approach has earned CBT a reputation as a premium cluster System Integrator, with a focus on both quality and relevance. With the addition of a local SOC, CBT plans to enhance customer trust and accelerate business growth, eventually expanding its presence to neighboring countries.

To sum up, Cloud Box Technologies stands out as a guiding force in the ever-evolving landscape of digital transformation, ensuring that businesses navigate this journey with expertise and confidence. By tailoring solutions, addressing

skill shortages, bolstering cybersecurity, and fostering collaboration, CBT remains at the forefront of driving impactful change across industries.

**THE CBT SOC WILL SUPPORT CUSTOMERS WITH THE FOLLOWING: THE CBT SOC WILL SUPPORT CUSTOMERS WITH THE FOLLOWING:**

**Continuous Protection** - 24/7 uninterrupted monitoring of network to detect potential threats.

**Security Intelligence** - Using the latest tools to identify and mitigate cyber threats in real-time.

**Quick and Effective Risk Management** -Comprehensive approach of advanced technology with human expertise helps detect threats and respond and mitigate risks quickly.

**Threat prevention** - Deep understanding of the threat landscape helps in providing potential view of the network anticipate new attack vectors even before they emerge.

**Proactive incident response strategies** - Proactive detection and response to threats in real-time reduce risk of data breach or cyber-attacks and help identify any potential weaknesses that can be exploited.

**Cost Savings** - The latest security solutions to help stay ahead of cyber threats and damage, thus saving potential costs incurred due to the security breaches.

**Regulatory Compliance** - Regulatory compliance such HIPPA and GDPR and regular compliance reports.





# Kaspersky and SADAFCO elevate cyber literacy in a critical infrastructure sector

Kaspersky and Saudia Dairy and Food Stuff Company have collaborated to share practices and improve cybersecurity awareness within the Middle East’s critical food infrastructure sector.

Kaspersky and Saudia Dairy and Food Stuff Company (SADAFCO) joined efforts to share best practices and elevate cybersecurity awareness within the critical infrastructure sector in the Middle East.

According to the ICS CERT landscape report by Kaspersky, malicious objects of all types were detected and blocked on 34% of Industrial Control System (ICS) computers in the first half of 2023. In the Middle East over this period attacks were detected on 36.8% of ICS computers, which is higher than the global average. The top industries under attack were energy (38.4%), oil & gas (31.0%), and manufacturing (21.4%). All these attacks were blocked after detection.

ICS computers are used in oil & gas, energy, automotive manufacturing, building automation infrastructures and other spheres to perform a range of OT functions – from the workstations of engineers and operators to supervisory control and data acquisition (SCADA) servers and Human Machine Interface (HMI). Cyberattacks on industrial computers are considered to be extremely dangerous as they may cause material losses and production downtime for the controlled production line and even the facility as the whole. Moreover, industrial enterprises put out of service can seriously undermine

a region’s social welfare, ecology and macroeconomics.

There are different types of cyberthreats that Industrial Control Systems face – malicious scripts, spy trojans, worms, ransomware, among others. The Middle East was one of the regions with the highest percentage of ICS computers on which malicious scripts and phishing pages were blocked in the first half of 2023 (14.3% in the Middle East compared to 12.7% global average). Malicious scripts serve a broad range of goals: from collecting data, tracking and forwarding users to malicious websites, to downloading various malware, such as spyware and/or covert crypto miners, to the system or the browser.

Spyware is another prominent threat for ICS. The Middle East had a high percentage of ICS computers on which spyware was blocked in the first half of 2023 (8.3%).The global average stands at 6.1%.

The Middle East was also one of the regions with the highest percentage of ICS computers attacked by ransomware in the first half of 2023 (0.56% vs. 0.32% global average).

Mission critical applications heavily leveraged within the critical infrastructure sector are often used as gateways or targets of evolving cyberthreats. To mitigate the

consequences, ensuring compliance with data privacy legislation in terms of data collection, handling, storage, deletion and governance of third-party partners has become mandatory.

“The food industry is part of the critical infrastructure sector and protecting it against evolving cyberattacks from different threat actors is a national priority in Saudi Arabia. As digital transformation gains momentum, cybersecurity must be a vital consideration, from the product evaluation and development stage, to testing and delivery. While technical defenses are crucial, so is awareness among the workforce. We strongly believe that training and education needs to be a continuous process. Our measures at SADAFCO are designed to the highest possible standards and follow three core tenets – cybersecurity training, communication and accountability. We have implemented an annual calendar of targeted cybersecurity training and education activities that are endorsed at all levels of our business management team. We are pleased that we have taken steps to protect our company and thereby contribute to the broader goal of safeguarding critical industries in Saudi Arabia”, said Shrikanth Andali, CIO at Saudia Dairy and Food Stuff Company.

**The food industry is part of the critical infrastructure sector and protecting it against evolving cyberattacks from different threat actors is a national priority in Saudi Arabia”.**

“When it comes to ICS, all world regions have their specifics. The Middle East is a major global energy hub, with numerous critical infrastructure facilities, including oil and gas refineries. Protecting these facilities from cyber threats is of paramount importance to ensure a stable energy supply worldwide. It should also be noted that many Middle Eastern countries are undergoing rapid industrialisation and modernisation, often involving the deployment of new ICS technologies. These systems may not have robust cybersecurity measures in place, making them potential targets,” comments Evgeny Goncharov, Head of Kaspersky ICS CERT. “By understanding the risks related to ICS, organizations can make informed decisions, allocate resources wisely, and efficiently fortify their defenses. In doing so, they not only protect their bottom line but also contribute to a safer and more secure digital ecosystem for all”.

To understand more about the ICS threat landscape, meet the Kaspersky experts at Stand H25-A30, Hall 25 at GITEX Global 2023, or read more here.

To keep your OT computers protected from various threats, Kaspersky experts recommend:

- Conducting regular security assessments of OT systems to identify and eliminate possible cyber security issues.
- Establishing continuous vulnerability assessment and triage as a basement for effective vulnerability management process. Dedicated solutions like Kaspersky Industrial CyberSecurity may become an efficient assistant and a source of unique actionable information, not fully available in public.
- Performing timely updates for the key components of the enterprise’s OT network; applying security fixes and patches or implementing compensating measures as soon as it

is technically possible is crucial for preventing a major incident that might cost millions due to the interruption of the production process.

- Using EDR solutions such as Kaspersky Endpoint Detection and Response for timely detection of sophisticated threats, investigation, and effective remediation of incidents.
- Improving the response to new and advanced malicious techniques by building and strengthening your teams’ incident prevention, detection, and response skills. Dedicated OT security trainings for IT security teams and OT personnel is one of the key measures helping to achieve this.

To equip your organisation with the right knowledge and tools, SADAFCO recommends:

- With one wrong click potentially having major security consequences, educating and training the workforce must be a priority; it is the first line of defense against malicious attacks.
- Implement robust Environmental, Social, and Corporate Governance (ESG) practices that ensure strategic and operational alignment across all parts of the business.
- Review and evaluate cybersecurity and data privacy governance processes.
- Track your company KPIs against committed ESG metrics.
- Maintain transparency on cybersecurity measures across all levels of the workforce via regular corporate communications.



# **Are you confident your infrastructure can prevent a non-tolerable event?**

Too many companies with  
SOC2/ISO27001/PCI DSS certifications  
have been hacked.

We treat threats differently to ensure no intolerable  
damage occurs. Ever.

[global.ptsecurity.com](https://global.ptsecurity.com)



# What is coming ‘Next’

CNME Editor Mark Forker attended ‘Next 23’ in San Francisco, as Google Cloud ushered in a new cloud era, one that will be driven by advancements made in generative AI.



Sundar Pichai

Thousands of customers, partners, analysts, and international press descended on The Moscone Centre in San Francisco, for Next 23, the first in-person event held by Google Cloud since 2019.

However, back in 2019, Thomas Kurian had recently just been appointed as the CEO of Google Cloud, but as Sundar Pichai, CEO of Google and Alphabet said when addressing attendees during the keynote, he was excited about his vision for Google Cloud four years ago.

“The last time we were here in 2019, Thomas presented his vision for Google Cloud, and I was so excited about his plans, and over the last four years, Thomas and his team have built Google Cloud into one of the top enterprise companies in the entire world,” said Pichai.

Before handing the floor over to the Google Cloud CEO, Pichai highlighted the impact some of the major announcements such as Vertex AI and Duet AI are going to have for customers.

“I believe that we are only really starting to scratch the surface since when we made Vertex AI available. Our objective is to equip our customers with access to the right model for them to create and innovate. In terms of Duet AI, we already have 1 million users, and today, we are delighted to announce the general availability of Duet AI in Google Workspace,” said Pichai.

Pichai concluded his address by declaring that the company will continue to be bold and responsible, and said they are imparting on a ‘golden age’ of innovation.

Thomas Kurian kicked off his keynote by saying that the shift to AI will

**We want to help every person use AI, and we want to bring together the whole AI ecosystem so they can succeed in adopting AI.”**

represent one of the most profound changes in our lifetime.

He reiterated Google’s mission, which is to help every person to be able to use AI.

“Our generative AI products are delivering real results in every single discipline. We want to help every person use AI, and we want to bring together the whole AI ecosystem so they can succeed in adopting AI,” said Kurian.

Kurian outlined how customers were increasingly drawn to their world-class infrastructure, revealing that Yahoo is migrating 500 million mailboxes and 550PB of data to Google Cloud as part of their efforts to improve their e-commerce experience, whilst Mahindra Rise has utilised the capabilities of Google Cloud to help them sell over 100,000 SUVs.

Kurian highlighted the impact some of their new products are having in terms of delivering productivity and operational gains for their customers.

“Today, we are launching a new product called GKE Enterprise, which has been designed to enable multi-cluster horizontal scaling. Customers have already seen an increase of 45% in productivity gains, whilst reducing software deployment times by over 70%,” said Kurian.

In addition to this, he also spoke of his excitement at their partnership with NVIDIA.

“We’re also announcing the availability of our A3 VMs, based on NVIDIA’s latest 8100 accelerator GPUs. A3 offers 3 times faster training and 10 times greater networking than the A2, which is ideal for managing incredibly demanding AI workloads. We are also introducing the titanium system, a next-generation tiered offload architecture that underpins the performance advances we have made in our AI infrastructure,” said Kurian.

Kurian added that it was the company’s ambition to help companies streamline their productivity and operational efficiency with generative AI.

“We are in an entirely new era of cloud, fueled by generative AI. Our focus is on putting gen AI tools into the hands of everyone across the organization—from IT, to operations, to security, to the board room. As the industry’s most open cloud, our goal is to help companies use AI and other cloud technologies to streamline their operations, increase productivity, and create entirely new lines of business,” said Kurian. So, what exactly did Google Cloud announce at Next?

Below is a comprehensive breakdown on the new partnerships forged, new infrastructure and tools rolled out and the expansion made on Vertex and Duet AI by Google Cloud.

**Customer momentum:** Organizations across industries and around the world are choosing Google Cloud to digitally transform, and this year they’ve shared stories from Culture Amp, Deutsche Borse, eDreams ODIGEO, Government of Singapore, HSBC, IHOP, IPG Mediabrands, John Lewis Partnership, The Knot Worldwide, Macquarie Bank, Mayo Clinic, Priceline, Shopify, U.S. Steel, and Wendy’s.

In addition to this, Google Cloud also announced new or expanded relationships with The Estée Lauder Companies, FOX Sports, GE Appliances, General Motors, HCA Healthcare, and more.

Innovative gen AI startups, like Replit, Typeface, Jasper, and more, are increasingly choosing to build on Google Cloud.

In fact, today more than half of all funded gen AI startups – including companies like Contextual, CoRover, Elemental Cognition, Fiddler, and Quora are Google Cloud customers.

This includes 70% of gen AI unicorns, like AI21, Anthropic, Cohere, Runway, and others.

**New infrastructure and tools to help customers:** The advanced capabilities and broad applications that make gen AI so revolutionary demand the most sophisticated and capable infrastructure.

Google Cloud has key infrastructure advancements to help customers, including:

- Cloud TPUv5e: This is Google Cloud’s most cost-efficient, versatile, and scalable purpose-built AI accelerator to date. Now, customers can use a single Cloud TPU platform to run both large-scale AI training and inferencing.
- A3 VMs with NVIDIA H100 GPU: A3 VMs powered by NVIDIA’s H100 GPU will be generally available next month, enabling organizations to achieve three times better training performance over prior generation A2.
- GKE Enterprise: This enables multi-cluster horizontal scaling required for the most demanding, mission-critical AI/ML workloads.
- Cross-Cloud Network: This is a global networking platform that helps customers connect and secure applications across clouds. It is open, workload-optimized, and offers ML-powered security to deliver zero

trust.

- Google Distributed Cloud (GDC): GDC is designed to meet the unique demands of organizations that want to run workloads at the edge or in their data centers. The GDC portfolio will bring AI to the edge, with Vertex AI integrations and a new managed offering of AlloyDB Omni on GDC Hosted.

**Vertex AI platform expands:** On top of Google Cloud’s renowned world-class infrastructure, the company is delivering a comprehensive AI platform—Vertex AI—that enables customers to build, deploy, and scale machine learning models.

Customers have access to more than 100 foundation models, including third-party and popular open-source versions, as well as industry-specific models like Sec-PaLM 2 for cybersecurity and Med-PaLM 2 for healthcare and life sciences. New innovations include: Vertex AI Search and Conversation: Now generally available, the tools enable organizations to create Search and Chat applications using their data in just minutes, with minimal coding and enterprise-grade management and security built in.

- PaLM 2, Imagen and Codey Upgrades: This includes updating PaLM 2 to 32k context windows so enterprises can easily process longer form documents like research papers and books.
- Tools for tuning: For PaLM 2 and Codey, Google Cloud is making adapter tuning generally available, and introducing a new method for Imagen, called Style Tuning, so enterprises can create images aligned to brand guidelines with a small amount of reference images.
- New models: Google Cloud is announcing availability of Llama 2 and Code Llama from Meta, and Technology Innovative Institute’s Falcon LLM, a popular open-source model, as well as pre-announcing Claude 2 from Anthropic. Google Cloud will be the only cloud provider offering both adapter tuning and RLHF for Llama 2.
- Vertex AI extensions: Developers can access, build, and manage extensions that deliver real-time information, incorporate company data, and take action on the user’s behalf.
- Digital Watermarking on Vertex AI: Powered

by Google DeepMind SynthID, this is a state-of-the art technology that embeds the watermark directly into the image of pixels, making it invisible to the human eye and difficult to tamper with.

- Colab Enterprise: This managed service combines the ease-of-use of Google’s Colab notebooks with enterprise-level security and compliance capabilities, helping data scientists accelerate AI workflows.

From the beginning, Google Cloud designed Vertex AI to give users full control and segregation of their data, code and IP. User prompts and data, as well as user inputs at inference time, are not used to improve our models and are not accessible to other customers.

**Duet AI in Workspace and Google Cloud:** Google Cloud unveiled Duet AI at I/O in May, introducing powerful new features across Workspace and showcasing developer features such as code and chat assistance in Google Cloud.

At ‘Next 23, Google Cloud is making Duet AI in Google Workspace generally available, while expanding the preview capabilities of Duet AI in Google Cloud, with general availability coming later this year.

Workspace is the world’s most popular productivity tool, with more than 3 billion users and more than 10 million paying customers who rely on it every day to get things done.

With the introduction of Duet AI just a few months ago, Workspace delivered a number of features to make users more productive, like helping write and refine content in Gmail and Google Docs, create original images in Google Slides, turn ideas into action and data into insights with Google Sheets, foster more meaningful connections in Google Meet, and more. New enhancements announced today include:

- Duet AI in Google Meet: Duet AI will take notes during video calls, send meeting summaries, and even automatically translate captions in 18 languages. Duet AI in Meet also today unveiled studio look, studio lighting, and studio sound.
- Duet AI in Google Chat: Users can chat directly with Duet AI to ask questions about their content, get a summary of documents shared in a space, and catch up on missed conversations.



# Smart security for every home.

TryMe™  
Scan to  
experience



Ring lets you monitor every corner of your property. With a Video Doorbell at your door, Security Cameras and Alarm system around the house, you can create a Ring of Security around your entire home.

Ring... smart security for every home.



ring  
an amazon company

For more information, contact [mea@ring.com](mailto:mea@ring.com) or visit [www.ring.com](http://www.ring.com)

To learn more, visit us at  
**GITEX Global 2023**  
**Stand H20-B05**



# Tencent Cloud Empowers MEA Enterprises with New SuperApp-as-a-Service, AI and Media Capabilities

*Tencent Cloud's second year of participation in the significant tech event underscores company's commitment to growing its cloud business in the MEA market. The showcase also features the digital platform upgrade for Abu Dhabi's government services.*

Tencent Cloud, the cloud business of global technology company Tencent, today announced its showcase at the GITEX GLOBAL 2023, one of the world's largest and most inclusive tech events held in Dubai, United Arab Emirates. Attending for the second time, Tencent Cloud is looking to strategically grow its business in the Middle East and Africa (MEA) market, demonstrating its

unique and competitive solutions and ecosystems in the gaming, media, telecommunications and public sectors.

During the event, Tencent Cloud will be debuting the SuperApp-as-a-Service, along with their latest innovations, under the Tencent Cloud AI and media solution family, that will be tailored for MEA enterprises.

Leveraging the track records in supporting Weixin/WeChat ecosystem with over 1.1 billion monthly active Mini Program users, Tencent Cloud's SuperApp-as-a-Service features the Tencent Cloud Mini Program Platform (TCMPP) that transforms web and mobile apps into one light-weight mini program for aggregation, open to any cloud infrastructure with container-based deployment. It offers a robust digital infrastructure which is fundamental for enterprise and public



service transformation.

On 17th October 2023, Tencent Cloud and TAMM, under the Department of Government Enablement of the Emirate of Abu Dhabi, held a signing ceremony to celebrate their partnership, and this collaboration will transform the public services into mini programs and aggregate them on TAMM using TCMPP capabilities.

This lifestyle transformation has turned TAMM into a Super App, consolidating over 700 essential public services from more than 30 government entities and the private sector on a single, standardized mini program, to provide services including citizenship and work permit applications, business registration, industrial license applications, housing and property leasing, healthcare facility access, tourism information, inheritance services, insurance matters, traffic ticket management, education and work benefits.

## Tencent's Transformative Technological Solutions, showcased at GITEX 2023

Quick-training Digital Human is Tencent Cloud's latest solution, empowering businesses of all shapes and sizes to reap the benefits from the AI revolution. It supports enterprise users to create customized digital avatars with minimal training, as such meeting the increasing demand for digital avatars across a vast variety of fields, including customer service, sales and marketing, virtual tour guiding, and more. Furthermore, the Tencent Cloud e-know Your Customer (eKYC) solution, utilizes AI technologies to optimize identity authentication processes with document recognition, liveness detection, and face verification capabilities.

Recognised by Frost & Sullivan as the No. 1 cloud services provider in Asia Pacific in the media sector, Tencent Cloud will

also be officially releasing several products under its AI media solution portfolio at GITEX 2023, to cater to the booming digital content, media, gaming and entertainment demand in the MEA region. Tencent Cloud Smart Video Analysis Platform (SVAP), Intelligent Media AI Platform, will be showcased with their advanced capabilities helping media organizations, enterprises, and content creators in areas such as video content creation and moderation, and smart video analysis.

Dan Hu, Vice President of Tencent Cloud International for the Middle East and Africa, said, "Backed by our ecosystem-building experience in the consumer internet space, as well as our AI capabilities accumulated, including hosting apps and offering internet infrastructure for a billion of users, Tencent Cloud is well positioned to work with local partners in the MEA region to support the local public service transformation, enabling enterprises and international businesses to leverage Tencent technologies to access the Chinese market, in addition to undertaking their own digital transformations in local markets using Tencent products and services."

"At Tencent Cloud, we also believe that cloud technologies including super app solutions are essential to enterprises and

governments that embark on a digital transformation journey", Hu added. "We are pleased to be collaborating with TAMM to upgrade its digital platform for government services for all Abu Dhabi residents. We look forward to working with more enterprises, agencies and institutions in the region and globally through Tencent Cloud's products and solutions".

Sharing insights about the evolving landscape of cloud gaming, Dan Hu, Vice President of Tencent Cloud International for the Middle East and Africa, spoke with Ralph Simon, Chief Executive Officer at Mobilium Global, to discuss how 5G is shaping the future of video gaming, elaborating on the roles of cloud service providers in offering comprehensive gaming solutions, for telcos and gaming platform providers, utilizing technologies such as TRTC with low latency and Edge Computing Machine. During the fire-side chat, Dan Hu shared his excitement for future plans for the Middle Eastern market, as gaming services are expected to benefit significantly from 5G. He commented that AI will drive forward the next-generation gaming systems, as Tencent Cloud continues to offer its solutions to the Middle Eastern market for enterprise adoption, including the Tencent Cloud SuperApp-as-a-Service for digital transformation.

## International Business Posts Strong Growth

Tencent Cloud's international business presently covers Japan, South Korea, Southeast Asia, Latin America, Europe, the Middle East, Africa, and other major markets.

In the first half of 2023, Tencent Cloud's international business has

achieved a double-digit revenue growth and a 66% revenue contribution with the partner countries' ecosystems, with the Middle East being one of the fastest growing regions with many regional customers showing strong interest in exploring potential SuperApp projects.

Today, Tencent Cloud is investing in local partner ecosystems, particularly in audio and video live streaming, with the goal of becoming a preferred technology service provider in the region. They plan to expand their resources in the audio and video domain and deploy AI products in the short term, while also strengthening their global partner network by recruiting influential local partners in the Middle East.

Tencent Cloud's international business and government partners benefit from the company's wide portfolio of 400 technologies and connectivity solutions that support enterprise grade digital transformation through its global infrastructure network, covering more than 26 geographic areas across five continents and 70 availability zones, with more than 2800 acceleration nodes.

Now in its 43rd edition, GITEX Global stands as one of the world's most iconic tech events. This year, the exhibition is expected to host over 6,000 exhibitors and more than 1,400 speakers from over 180 countries. In 2022, the event attracted more than 5,000 companies and over 170,000 attendees. This year's GITEX Global is set to showcase the trending growth of AI over the past 12 months. Notable speakers from the tech industry will also cover a wide range of topics, including Cybersecurity, Mobility, Sustainable Tech, and more.

# The missing 'Link'

*Patrick Ramseyer, Vice President EMEA at LinkShadow discusses the importance of intelligent NDR – and how his company is steering CISOs away from the traditional siloed approach to cybersecurity.*

Patrick Ramseyer is an Irish-Swiss national who has enjoyed a stellar career in the cybersecurity industry.

He has spent most of his professional life in Switzerland, but he moved to the UAE in 2018, when he was appointed as the Managing Director of a well-known cybersecurity vendor.

In April of this year, he joined LinkShadow, where he has been tasked with the responsibility of driving their growth across the EMEA region.

In a candid discussion

with CNME, Ramseyer was transparent on the issues facing CISOs in the current cybersecurity climate, and how the solutions within their product portfolio are equipping them with the tools they need to both better protect their assets and save money.

He kickstarted the conversation by highlighting the need for large enterprise to move away from a siloed approach to security.

"One of the major challenges that stakeholders and CISOs are encountered with is the fact that they have

what would be described as a siloed approach. Essentially, that means they are building up their security operations centres around various teams for various products. For example, take a CISO with a team of 50 people working for him, he has a firewall team, end-point detection and response team, but they are all working in separate little silos, and ultimately what that leads to is a lot of 'noise'. When we say noise in security operations what we're talking about is false positives, which is basically security professionals investigating incidents of no importance, and that leads to 'alert fatigue'," said Ramseyer.

As Ramseyer pointed out, the lack of talent and skills on a global scale has fostered an environment in which staffing shortages is the norm.

"If you work in an air traffic control tower you work for 35-minutes and then you stop and take a 35-minute break because of the sheer pressure. However, security operations centres don't work like that because they can't afford to. They are on the go for 10, or 12 hours a day monitoring incidents and monitoring threats, and investigating other suspicious activity, so alert fatigue is a huge problem. If you speak to any CISO in today's climate he's going to tell you that the biggest problem, they face is staff and skill shortages," said Ramseyer.

Ramseyer reinforced how the siloed approach to security had become archaic, and stressed the need for security systems to be working in correlation.

"If my end-point detection and response is reporting that I have a couple of



Patrick Ramseyer

suspicious files on my computer, what you need to be able to do is correlate that with the fact that my PC is also negotiating with a website on a blacklist – and my intrusion detection system is saying that from another IP range in Russia there is an attempt coming through. So, essentially what you've got is the

intrusion prevention system team seeing one thing, the intrusion detection team seeing another picture, the firewall team seeing something different, and the same applies to the end-point detection and response team, but crucially nobody is correlating this,

► CONTINUED ON PAGE 15



► CONTINUED FROM PAGE 14

## LinkShadow...

it is all siloed. It's only when they get together once a week and they say we had this, and we had that – it's only then that the penny finally drops with them," said Ramseyer.

Gartner have proposed cybersecurity mesh architecture as a solution to the problem of siloed security.

Ramseyer outlined that it is essentially 'a new approach' businesses need to take, and he explained the benefits of LinkShadow's cyber mesh platform.

"We call LinkShadow, a cyber mesh platform, because it's a new approach that companies are supposed to take. It's all about taking a new approach to your security posture, and that's what LinkShadow is all about. What you're looking at with this new approach is instead of having multiple silos and multiple teams, you consolidate all of that into one package. It is based on the premise of middleware, which effectively eliminates all the things you don't need to see from all the other systems, and highlights and gives you the most important information that you need. What we do is very similar to that,

we're talking to your EDR, IDS, and firewall teams, and we're correlating and aggregating all this information, and that's where our AI and Machine Learning comes in, because you can't do that manually, the only way to do it is by using adaptive AI. The other element is being able to correlate the automation of all the responses, and that's all done using our AI engine," said Ramseyer.

LinkShadow has customer-centricity embedded into its core values as a company, and that has allowed them to understand the nuanced challenges facing CISOs.

In addition to this problems CISOs face in terms of SOC efficiencies and skills shortages, another consistent challenge they face is dwell time.

"There's no doubt that dwell time is a huge challenge for CISOs. How long is a threat inside my network before I actually find it? These are the types of metrics that CISOs are looking at. When you talk about insider threat you need to consider that it could be deliberate, or it could be accidental. You also have to monitor the lateral traffic, you have North and South traffic, which is in and out of your network, and then lateral

is inside user to user, by monitoring that traffic you can also detect anomalies," said Ramseyer.

However, according to Ramseyer the biggest question that underpins all of the above is how do businesses save money?

"A CISO will say to you that I need you to hand me a proposal that I can give to my CFO that demonstrates if we purchase this product then we're going to save money. You can show the cost savings very, very quickly, and the primary reason for that is the fact we have one user interface. For example, if I take the siloed approach, then I'll have 10 different types of interfaces, and 10 different panes of glass. Every vendor will tell you that they have a single pane of glass, but it's 10 altogether, it's not a single pane of glass. You have to take all those 10 interfaces and funnel them into one. By doing that you have one platform that shows you where your threats are, how to respond to the threats – and ideally it will tell you where you are wasting money. In addition to this, if you want to investigate further, or if you need a specialist for forensics then you can go into your firewall logs," said Ramseyer.

Ramseyer also highlighted the issue of 'vendor lock-in' that many

CISOs and IT directors face.

"A lot of CISOs and IT directors will talk to you about vendor lock-in – which essentially means they are over reliant on one particular vendor. CISOs don't like that because it takes the decision out of their hands, and maybe one vendor has a better end-point detection and response than the other, but because they are locked in, they can't use it. They want autonomy and choice. The big advantage we have is the fact that we integrate with any vendor, it's doesn't matter if your Microsoft, Sophos, or Kaspersky, we integrate with all of them via what is called bi-directional API. We're not only receiving information from them, we're also sending them activities in terms of response, so it's a two-way communication between each of those systems, and we have already over 60 done with all the main vendors, and this is what cyber mesh is all about. It is a common integration between all these tools that have a single platform, so that everyone can see what is going on in each one from the one pane of glass," said Ramseyer.

LinkShadow has drawn widespread acclaim for their intelligent NDR solution.

According to Ramseyer, CISOs at large entities want to know what their risk exposure is, and

LinkShadow's intelligent NDR can provide them with that.

"Traditional NDR by definition is network detection and response, which essentially monitors the traffic on the network and looks for anomalies and threats. However, what intelligent NDR does is not only monitors the traffic, but it also correlates it all with the other security tools. CISOs want to know what their risk exposure is? Large organisations are concerned about their risk exposure because it's a measurable metric, so they can say every month that my risk exposure was 9 or 8, so they can see they are improving. It's not really applicable here in the Middle East yet, but in Europe, if you get breached you have to account for everything that happened up until that breach. When you get investigated by the relevant bodies of data protection, they are going to ask to see everything you have in place, and if you can document and demonstrate that you have been making an effort to reduce your cyber exposure over a period of time then the fines will be a lot less. These businesses want to see their risk exposure and we can give them that through our intelligent NDR," said Ramseyer

Another key component within LinkShadow's intelligent NDR offering is their block count ratio.

"We have what we call a block count ratio, and what that essentially means is how many blocks did my security tool do? How many times did it block a blacklisted IP address, how many times did the end-point detection and response cut out malicious files. We can see by assessing each tool how effective they are. We can then give the CISO a lovely report where he sees these intrusion detection systems have only accounted for say .6% of their total blocks for a year, which is less than 1%, so does he really need that one, or do he really need a very expensive one? You could have a DLP system that cost you \$10,000, and you can have a DLP system that can cost you \$1million, but you might only need a \$10,000 one if your DLP is not a major concern, but you need to be able to determine that, and again that's where we come in. Ultimately, our intelligent NDR empowers CISOs to make the decisions based on the criteria that's important to them, and the No.1 criteria that it is important to any CISO is money because security is a blackhole when it comes to money," said Ramseyer.



## Zebra's Retail Management Solutions Accelerate Retail Transformation and Improve Customer Experiences

Helping Retailers Close the Gap between Strategy and Execution for Labor, Inventory and Customer Experience Plans. Find out more at Zebra Technologies





## STANDS TO WATCH



STARLINK

Stand: H3



RE-IMAGINING THE  
DIGITAL FUTURE



# ACCELERATING UNICORNS WITH SIA STARTUPS • ISVs • ALLIANCES

## You Can



Identify Market  
Gaps



Ideate and Innovate  
on Cloud



Create Disruptive  
Solutions

## We Can



Provide Dedicated  
Focus



Expedite Time to  
Market



Aid in Adoption &  
Innovation

## Together We Will



Build  
Competency



Define GTM  
Strategy



Align Commercial  
Strategy



Drive Marketing  
Strategy



## Talk to Us & Skyrocket Your Unicorn Journey

Visit us at Expand North Star (15-18 Oct) - Hall 7



## STANDS TO WATCH



DELL TECHNOLOGIES

Stand: H6-A1



GO BEYOND LIMITS

# WIN BIG

with StorIT & Dell Technologies

SCAN TO  
  
SIGN UP

*\*\*Valid for Dell Channel Resellers in UAE region only*



WIN HARLEY DAVIDSON BIKE



WIN PORSCHE SPORTS CAR



WIN GOLD COINS

**StorIT Distribution fzco**

Anantara Downtown Business Tower, Business Bay & Jafza 15, Jebel Ali Freezone, Dubai, United Arab Emirates  
P.O.Box 17417 | Tel: +971.4.8819690 | Email: [info@storit.ae](mailto:info@storit.ae) | [www.storit.ae](http://www.storit.ae)



## STANDS TO WATCH



RESECURITY

Stand: H2-B50





# GITEX GLOBAL 2023

# Accelerate Intelligence

16 - 20 October

Visit us at Hall 22

#HWGITEX23



Contact Us



enterpriseME@huawei.com



e.huawei.com/ae

Visit our Minisite





## STANDS TO WATCH



**TREND MICRO**

Stand: H2-E20



The Riverbed logo is displayed in a lowercase, sans-serif font. The word 'river' is in a light blue color, and 'bed' is in a light orange color.The GITEX Global logo is located in the top right corner. It features the word 'GITEX' in a large, bold, sans-serif font with a gradient from orange to blue. Below it, the word 'GLOBAL' is in a smaller, all-caps, sans-serif font. At the bottom, the dates '16-20 OCT 2023' and the location 'DUBAI WORLD TRADE CENTRE' are listed in a small, all-caps, sans-serif font.

# **Deliver Exceptional Digital Experience with Unified Observability and Acceleration Solutions**

Don't Miss Riverbed at **GITEX Global 2023!**

Visit Riverbed Technology to explore two industry-leading portfolios that drive enterprise performance and exceptional digital experiences. With Alluvio™ Unified Observability, transform data into actionable insights to deliver seamless, secure digital experiences for customers and employees. With Riverbed Acceleration, provide fast, agile, secure acceleration of any app, over any network, to users everywhere. Learn more at **riverbed.com**.

**Concourse 2, Booth CC2-18**

Dubai World Trade Center  
16<sup>th</sup> – 20<sup>th</sup> October 2023



## STANDS TO WATCH



VEEAM

Stand: H7-D20



# Secure Your **Digital Future**

Simple. Secure. Resilient.



**Secure Your Enterprise IT Footprint  
For A Safer Digital Journey**

[www.raqmiyat.com](http://www.raqmiyat.com)

UAE | KSA | INDIA





# DOES YOUR DATA PROTECTION LEAVE GAPS? Question it.

See what makes Commvault the only unified data protection that covers all your data, wherever it lives. Data protection vendors have been throwing around a lot of big claims and buzzwords that could put your data at risk. It's time to question it all.

**COMMVault**® 

Learn more at  
[commvault.com/questionit](https://commvault.com/questionit).

