



Bedata ready.

Commvault is a worldwide leader in delivering data readiness. Our intelligent data management solutions work on-prem and in the cloud, allowing you to store, protect, optimize, and use your data. Always.

commvault.com

CONTENTS









News roundup from the security industry in the region and beyond

6

12 Marcus Josefsson, VP EMEA at Nozomi Networks on the cyberthreats that OT & ICS environments face, and how the Nozomi Networks' product portfolio can be leveraged to boost cyber resilience. 20 Murali Vellat, Division Manager at Bulwark Technologies, to find out how the company's strong partner ecosystem and focus on stable, steady growth, has positioned it as the VAD of choice in the IT domain.

24 Anoop Das, Enterprise Manager, Middle East at Mimecast on the company's channel strategy, technology investments and roadmap for the year.



DCLTechnologies

Cyber and ransomware attacks are the enemy of today's data-driven business





Preserve data integrity and confidentiality with layers of security and controls

00	-
7	
00	-
00	-

Isolation Physical and logical separation of data within a vault



Intelligence

Machine learning and analytics help ensure recoverability

Cyber Recovery



EDITOR'S NOTE



Talk to us: E-mail: anita.joseph@ cpimediagroup.com

> Anita Joseph Editor

EVENTS



DATA BACKUP

NEED FOR EFFECTIVE

BACKUP SOLUTIONS

World Backup Day's main goal is to raise awareness about the importance of data backup and encourage individuals and organisations to take action to protect their valuable data. The primary objective of World Backup Day is to educate individuals and organisations about the importance of backing up their data. This awareness campaign seeks to prevent data loss and ensure that people have access to their valuable information when they need it.

The rise of cloud migration and affiliated services has meant that the physical data

center is no longer the heart of the IT infrastructure. Many enterprises still rely on "legacy" backup solutions that were designed to protect physical on-site servers and are simply not fit for purpose in our hybrid world. These legacy backup mechanisms rarely yield good outcomes when protecting modern virtual or cloudhosted workloads. So why haven't more enterprises pivoted to solutions that cover cloud-hosted workloads like Licensing as

a Service (LaaS) or Software as a Service (SaaS)? It's partly because it's not the top priority for many - it typically has to start hurting before enterprises start moving. An equally significant factor is that many of these legacy solutions have vendor "lockin" making it harder for organisations to migrate their data to a different solution. When looking at backup solutions it is always best to look at vendors without any kind of lock-in for this exact reason - you'll

never know when you need to change or move things around.

This issue of Security

Advisor focuses on the need to back data upno longer a casual option but a crying need. We speak to experts to find how data backup has changed and evolved over the years and what to expect next. Our special interviews and insight columns also bear testimony for the need for efficient and effective data backup solutions.

This issue of your favourite magazine is both insightful and inspiring. So, make sure you get your copy, Happy

Published by

Dominic De Sousa (1959-2015)

FOUNDER, CPI

ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.comm

PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@coimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@coimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAF

Tel: +971 4 5682993

© Copyright 2023 CPI All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Directo

Sabita Miranda

sabita.miranda@cpimediagroup.com

OnlineEditor Daniel Shepherd daniel.shepherd@cpimediagroup.com

Veronica Martin Contributing Editor SAME & Tahawultech.com

TENABLE CHOSEN BY WÄRTSILÄ TO SOLVE OT ASSET MANAGEMENT CHALLENGES

Tenable, the Exposure Management

company, has confirmed that Wärtsilä has selected Tenable OT Security to manage its operational technology (OT) asset inventory collection and provide holistic visibility into its OT environment. The deployment allows Wärtsilä to answer its customers' questions around asset delivery, reducing supply chain risks and taking a proactive stance on cybersecurity. Wärtsilä will extend the Tenable solution to its customers, allowing them to visualise their own OT environments.

Wärtsilä is a global leader in innovative technologies and lifecycle solutions for the marine and energy markets and was seeking to address three key challenges: Automated asset inventory collection, compliance reporting — IEC 62443, etc and OT vulnerability reporting.

Previously, this information was collected manually with the data being reported using spreadsheets. This process was time consuming and susceptible to errors and the data could have inconsistencies both in the way it was collected and reported.

With Tenable OT Security, an industrial security solution for the modern industrial enterprise, Wärtsilä can identify assets, communicate risk and prioritise action all while enabling its IT, security and OT teams to work better together.

"We tested multiple tools and found Tenable OT Security to have great discovery via vendor specific protocols. The workflow of the tool was a great fit



for our own needs but, beyond that, we realised that using the solution allowed us to develop and introduce new services to benefit our customers too," explained Ross Bailey, Cyber Security Expert, Wärtsilä. "With Tenable OT Security, we can help our customers to visualize their own OT environment. This allows them to adhere to the evolving compliance landscape and ultimately assists in protecting critical infrastructure."

INFOPERCEPT LAUNCHES INVINSENSE 4.0

Infopercept, a global cybersecurity

solutions and services company, has announced that it has launched Invinsense 4.0., a cybersecurity platform that covers offensive, defensive, and security compliance. The platform is now available in Software as a Service (SaaS) form. In addition to traditional IT and Cloud setups, Invinsense 4.0 now covers security in Operational Technology (OT) and Internet of Things (IoT) setups.

The new version of Invinsense 4.0, designed to simplify the management of defensive, offensive security and security compliance with three central consoles, includes:

 Invinsense Extended Detection and Response (XDR)—Integration of Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Extended Detection and Response (EDR), Threat Intelligence, Threat Exchange, and Case Management.

- Invinsense Extended Detection and Response plus (XDR+)—Deception and Patch Management
- Invinsense Offensive Extended Detection and Response (OXDR)— Integration of Vulnerability Management (VM), Breach and Attack Simulation (BAS), and RedOps.
- Invinsense GSOS—Covers security compliance, strategy, and awareness.

"Since the launch of the first version, Invinsense was designed to cover all three pillars: offensive, defensive, and compliance," said Jaydeep Ruparelia, CEO and Co-founder of Infopercept Consulting Pvt Ltd. "With the exponential



digital transformation happening in the entire world, all organisations have either started or matured their cloud journey. Infopercept has been supporting born-in-the cloud organisations by providing security in the cloud. Making Invinsense 4.0 available in Software as a Service (SaaS) mode was a step further to help organisations in their secured cloud journey."

SOPHOS PROMOTES JOE LEVY TO PRESIDENT OF SOPHOS TECHNOLOGY GROUP; APPOINTS BILL ROBBINS PRESIDENT OF WORLDWIDE FIELD OPERATIONS

Sophos, a global leader in innovating

and delivering cybersecurity as a service, has announced the promotion of Joe Levy to president of the Sophos Technology Group (STG). Sophos also appointed Bill Robbins president, Worldwide Field Operations.

Levy is currently Sophos' chief technology officer and chief product officer, and will retain these titles and the organisational structure of STG. As president, Levy will continue expanding Sophos as a leading global cybersecurity as a service provider. driven by its fast-growing Sophos Managed Detection and Response (MDR) and Incident Response (IR) services and a more than \$1 billion product portfolio that spans endpoint, network, email, and cloud security. Sophos MDR is the fastest growing detection and response service worldwide, supporting more than 15,500



customers. STG also includes Sophos X-Ops, a cross-operational threat and cybersecurity intelligence team of more than 500 experts. Levy will continue to report to Sophos Chief Executive Officer Kris Hagerman.

"Joe and his team continue to set new standards for both the pace and the quality of innovation as our technology teams deliver world-class



protection, detection and response for our customers, and provide a strong technical foundation to support Sophos' long-term success," said Hagerman. "Our product strategy, our technology delivery execution and our future technology roadmaps have never been stronger as a result of Joe's ambition, vision and guidance as a leader at Sophos.

EDGIO'S ADVANCED BOT MANAGEMENT ENHANCES MULTI-LAYER SECURITY PORTFOLIO

Edgio, the platform of choice for

speed, security, and simplicity at the edge, has announced the availability of their new Advanced Bot Management solution that proactively mitigates a wide range of evolving malicious bots while providing observability into good bots. Leveraging massive amounts of data continuously drawn from the platform's extensive global deployment, Advanced Bot Manager applies machine learning to detect bots based on both signature and behavioral fingerprinting. The solution runs natively on every server across the entire Edgio global network to inspect all traffic for bots in real time.

Leading analyst firm Forrester says about the bot problem, "Bad bots continue to consume resources and



overwhelm organizations, accounting for at least a quarter of all internet traffic." That said, proper bot management is critical to any online business or organization with internet-facing applications. Edgio's threat research and data science teams built the solution to mitigate a wide range of prevalent bot attacks, including account takeover (ATO), credential stuffing, fake account creation, gift card fraud, inventory scalping, scraping, application DDoS and more.

The solution is easily deployed in minutes and eliminates the need for code changes, SDK integrations or JavaScript injections that add complexity and impact user experience. It is infrastructure and network agnostic, giving customers complete freedom to easily integrate with their cloud, hybrid cloud or onpremises infrastructure. In addition, the Edgio Advanced Bot Manager agentless solution protects both web and mobile apps as well as API endpoints against all bot attacks.

ESET NAMED TOP PLAYER IN RADICATI MARKET QUADRANT FOR FOURTH TIME

ESET, a global leader in digital

security, has been named a Top Player in Radicati's Advanced Persistent Threat (APT) Protection - Market Quadrant 2023. Being a Top Player in one of Radicati's reports means not only that ESET is a current market leader with products that offer, both breadth and depth of functionality, but that they also possess a solid vision for the future.

ESET's key strengths highlighted in the report were the capabilities of its unified single-click security management platform, ESET PROTECT, which together with ESET Inspect delivers extended detection and response (XDR) with granular visibility, risk assessment, incident response, investigation, and remediation. The fact that ESET's solutions offer multilanguage support across its wide-spread network of customers and they, in turn, appreciate ESET's solutions for their easy of deployment and use, showcases



ESET's relentless drive towards improving their commitment to their customers. Also worthy of note is ESET's partnership with Intel, which combines ESET Endpoint Security solutions with Intel® TDT as an additional source of threat telemetry to assist in the detection of threats which use advanced evasion techniques.

"We are incredibly proud of our latest accolade from Radicati. Being a consistent

Top Player in our industry is testament to the fact that we are constantly improving and that our science-based, security-first approach to developing the global threat intelligence systems fueling our multilayered and efficient solutions is the right one," said Juraj Malcho, chief technology officer at ESET. "It is particularly gratifying to hear that our customers value our solutions, our expertise and the ease of use of our solutions."

TRELLIX APPOINTS ASH PARIKH TO CHIEF MARKETING OFFICER

Trellix, the cybersecurity company

delivering the future of Extended Detection and Response (XDR), has announced the addition of Ash Parikh to the role of Chief Marketing Officer (CMO). In his role as CMO, Parikh will lead global marketing teams to drive brand awareness, demand generation, and goto-market strategies of the XDR market leader.

"Trellix's XDR platform is helping our customers bolster their cybersecurity programs," said Bryan Palma, Chief Executive Officer at Trellix. "Ash's unique experience at the intersection of SaaS, cybersecurity, and data management perfectly positions him for amplifying Trellix's XDR leadership and ensuring our value proposition is accessible to millions of customers."

Parikh will report directly to Palma. He brings to Trellix a nearly 30-year track record of leading teams, with 20 years growing and scaling enterprise software organisations at both late-stage private and mid-size public companies. Most recently, he served as the CMO of Druva, a SaaS vendor for data protection and cybersecurity. Prior to this, he spent over a decade leading the marketing organisation in various roles at Informatica. He is a member of the board of advisors for Yellowbrick Data and the CMO Council and has received several recognitions including 2022's Top 100 B2B Marketing Leaders by HotTopics.

"Since the pandemic, marketing has been disrupted, but very few know how to navigate. It takes a deep understanding of the customers' journey, an ability to



leverage the latest digital technology, and a dedication to sales and marketing alignment to drive meaningful engagement with customers. Trellix's XDR leadership is the perfect opportunity given the everincreasing threat landscape, and I'm ready to jump right in with my experience in data and cybersecurity," said Ash Parikh, Chief Marketing Officer at Trellix. "I look forward to telling the Trellix story and advancing the company alongside a world-class global marketing team."

Smart security for every home.



Ring lets you monitor every corner of your property, no matter where you are. With a Video Doorbell at your door and Security Cams around the house, you can create a Ring of Security around your entire home.

With Ring, you're always home.



INTRODUCING MICROSOFT 365 COPILOT: A WHOLE NEW WAY OF WORK

MICROSOFT HAS BUILT MICROSOFT 365 COPILOT WITH ITS EXISTING COMMITMENTS TO DATA SECURITY AND PRIVACY IN THE ENTERPRISE.

icrosoft is bringing the power of nextgeneration AI to its workplace productivity tools with Microsoft 365 Copilot. Currently in testing with select commercial customers, Copilot combines the power of large language models (LLMs) with business data and the Microsoft 365 apps, to unleash creativity, unlock productivity and uplevel skills.

Microsoft

Customers will experience Microsoft 365 Copilot in two ways –

Microsoft 365 Copilot isn't just a better way of doing the same things. It's an entirely new way of working. Copilot will work alongside Microsoft 365 customers in two ways:

- First, it is embedded in the Microsoft 365 apps people use every day — Word, Excel, PowerPoint, Outlook, Teams and more.
 - Today, the company also announced an entirely new experience: Business Chat. Business Chat works across the LLM, the Microsoft 365 apps, and a customer's calendar, emails, chats, documents, meetings and contacts to do things that people weren't able to do before. With natural language prompts like "tell my team how we updated the product strategy," Business Chat will generate a status update based on the morning's meetings, emails and chat threads.

"Copilot is not just any ordinary tool - it is the catalyst for a revolutionary new era of work that will enable businesses to achieve unprecedented levels of success. As part of our unwavering commitment to empowering organisations across the UAE, we are excited to launch this gamechanging AI-powered productivity tool to the market," said Naim Yazbeck, General Manager, Microsoft UAE.

"By harnessing the full potential of large language models, Copilot will completely transform the way we work. It will not only boost productivity and unlock creativity for businesses of all sizes and industries, but also pave the way for new and innovative ways of working that will drive growth and competitiveness across the UAE and beyond. This is just the beginning, and we cannot wait to see the profound impact that Copilot will have on businesses and industries, propelling them towards new heights of excellence and success," he added.

With Copilot, the customer is always in control. Customers decide what to keep, modify or discard. With these new tools, people can be more creative in Word, more analytical in Excel, more expressive in PowerPoint, more productive in Outlook and more collaborative in Teams.

Microsoft 365 Copilot is seamlessly integrated in the apps people use every day, helping them stay in the flow of work and freeing them to focus more on the task at hand and less on the busy work.

Microsoft has built Microsoft 365 Copilot with its existing commitments to data security and privacy in the enterprise, grounded in AI principles and Responsible AI Standard and decades of research. Copilot's large language models are not trained on customer content or on individual prompts. Microsoft 365 Copilot will deliver enterprise-ready AI at scale.



Secure Your Digital Future Simple. Secure. Resilient.

-0

7



www.raqmiyat.com UAE | KSA | INDIA

BUILDING CYBER RESILIENCE

ANITA JOSEPH CAUGHT UP WITH **MARCUS JOSEFSSON,** VP EMEA AT NOZOMI NETWORKS TO LEARN MORE ABOUT CYBERTHREATS THAT OT & ICS ENVIRONMENTS FACE, AND HOW THE NOZOMI NETWORKS' PRODUCT PORTFOLIO CAN BE LEVERAGED TO BOOST CYBER RESILIENCE IN CRITICAL INFRASTRUCTURE, INDUSTRIAL NETWORKS AND GOVERNMENT ORGANISATIONS IN THE REGION.

ell us about why GISEC is important and the products and solutions you are highlighting this year

GISEC is an important event where we get to meet with existing customers and partners, both new and potential. This year, however, is special, because we now have local cloud capability in the UAE which is something our customers, such as those in oil & gas, utilities, retail, critical national infrastructure, real estate, hospitals etc, find relevant and necessary. A lot of them wish to migrate to the cloud, but they would like to do that in a compliant fashion and that's what we help our customers with. We've also extended our product range with endpoint agents to capture visibility from endpoints on the network. So, those are the two main stories that resonate with our customers and partners at this stage.

What are your plans for the region this year?

This region is growing and we are market leaders due to the fact that we

were here a few years ago. Competition arrived a year back, and they have a lot to cover. We make sure we keep delivering the value we have been delivering over time to resellers, system integrators and of course, our existing customers.

We've captured most of the customer base in the type of verticals that we traditionally go after. So now we're in a place where we are focusing on areas like retail, hospitals etc. We've seen some very good progress; some very significant wins and our partners have been with us in this journey. We moved from securing oil and gas utilities, etc to helping out banks, retail outlets and hospitals, because these sectors have similar challenges with very similar networks. They are now waking up to the need for cybersecurity controls, regulatory compliance and so on.

What are some of the cyber threats that OT and ICS environments should watch out for this year?

We're going to keep seeing statesponsored threats and geopolitical tensions. In fact, state-sponsored attacks are extremely clever and advanced, and have been so for a while. We're also

seeing a lot of retail malware-off-theshelf stuff, as these are environments are becoming more and more exposed. Also, with the Internet of Things and the fact that everything's connected, means that everything is exposed. Today, environments, which we didn't think about that necessarily as critical national infrastructure are also getting compromised and we're seeing that the awareness that comes from traditional OT verticals are now spreading into everything from military to hospitals since they all have the same type of networks. So, they've all become super important and it's necessary to get visibility and cybersecurity controls across these as well.

How can Nozomi Networks' product portfolio actually be leveraged to boost cyber resilience in critical infrastructure, industrial networks and government organisations in the region?

From a product perspective, the first phase is always visibility-you can't secure what you can't see. And what we see is that when customers embark on this journey once they've finished with their assessments and drawn their plans, the first type of technology that they need to embrace is to try and understand what's going on. And Nozomi Networks plays a big part here, helping them understand what the assets are, what the network looks like, how communication happens there and so on. That's the first step.

Secondly, there are more and more compliance regulations coming in. So, we're also assisting customers from that perspective. And now we're able to leverage the cloud locally, and the endpoint agents provide even more visibility. The region is forward-leaning, it's innovative, but there's still so much to do. We've done maybe 5% of what we came to do, and the company has grown significantly over the last five years, just looking at this region from a revenue perspective. So, we've come a long way, but most of it is ahead of us. **1** TODAY, ENVIRONMENTS, WHICH WE DIDN'T THINK ABOUT THAT NECESSARILY AS CRITICAL NATIONAL INFRASTRUCTURE ARE ALSO GETTING COMPROMISED. COVER STORY / BACKUP DAY



orld Backup Day is a commemorative date celebrated annually by the backup industry and tech

industry all over the world. It highlights the importance of protecting data and keeping systems and computers secure.

World Backup Day started with a post on Reddit where a user wrote about losing their hard drive and wishing someone had reminded them about how important it is to backup data.

World Backup Day's main goal is to raise awareness about the importance of data backup and encourage individuals and organisations to take action to protect their valuable data. The primary objective of World Backup Day is to educate individuals and organisations about the importance of backing up their data. This awareness campaign seeks to prevent data loss and ensure that people have access to their valuable information when they need it.

World Backup Day encourages individuals and organisations to adopt backup solutions that suit their specific needs. Whether it's cloud storage, external hard drives, or tape backups, World Backup Day promotes the use of reliable backup solutions that ensure data is safe and easily recoverable.

Backing up data is only half the battle. World Backup Day also emphasizes the importance of regularly testing backups to ensure that data is recoverable in the

DISASTER RECOVERY AND DATA PROTECTION WILL PLAY A CRUCIAL ROLE IN 2023.

event of a disaster. Regular testing helps to identify any issues with the backup process and ensures that data is easily recoverable when needed.

World Backup Day aims to foster a culture of data protection where individuals and organisations prioritise backing up their data regularly. This culture encourages people to take proactive steps to safeguard their data and ensures that data loss doesn't become a major issue.

Overall, the main objective of World Backup Day is to create awareness and encourage people to take action to protect their data. By adopting reliable backup solutions and regularly testing backups, individuals and organisations can ensure that their data is always accessible and protected from potential disasters.

Security Advisor spoke to a few security industry veterans to learn more about data backup.

Edwin Weijdema, Field CTO EMEA & Lead Cybersecurity Technologist, Veeam

S ince the start of world backup day in 2011, technology and the data that powers it has continued to evolve. This is particularly true with enterprise organisations, which are more focused than ever on protecting and securing their data across increasingly complex IT environments. As we recognise World Backup Day 2023, what do enterprises need to focus on?

Firstly, a Modern Data Protection strategy and the deployed backup solution supporting it must be able to protect workloads across any IT environment. The rise of cloud migration and affiliated services has meant that the physical data center is no longer the heart of the IT infrastructure. Many enterprises still rely on "legacy" backup solutions that were designed to protect physical on-site servers and are simply not fit for purpose in our hybrid world. These legacy backup mechanisms rarely yield good outcomes when protecting modern virtual or cloudhosted workloads. So why haven't more enterprises pivoted to solutions that cover cloud-hosted workloads like Licensing as a Service (LaaS) or Software as a Service

(SaaS)? It's partly because it's not the top priority for many - it typically has to start hurting before enterprises start moving. An equally significant factor is that many of these legacy solutions have vendor "lock-in" making it harder for organisations to migrate their data to a different solution. When looking at backup solutions I would always advise looking at vendors without any kind of lock-in for this exact reason - you'll never know when you need to change or move things around.

You'd think backup and recovery go hand-in-hand (backup is what you use to recover to after all) but there is often a disconnect which makes data recovery less reliable than needed. This is due to how infrastructure is designed. Architecture built for backup might be able to duplicate 100% of its data and workloads in the space of 24 hours but when it comes to recovering this data and restoring it to the live environment, it might only be able to do 5% of this in the same time frame. It's like a motorway with six lanes in one direction. but only a single lane going the other way. Enterprises need to start designing their infrastructure with recovery in mind to



reduce downtime in the event of an outage or ransomware event and ensure they get the most out of their backups.

While many enterprises have made huge strides in how they think about backup, there are many who still have a long way to go. Backup needs to be transformed from an afterthought to the crux of the IT infrastructure. Building resilience to cyber-attacks or accidental outages is simply not possible without a modern backup strategy that is cloudnative and is built with recovery in mind.

Fred Lherault, Field CTO EMEA and Emerging Markets at Pure Storage

rganisations need a two-pronged strategy: advanced, immutable copies of their data and an ability to not just backup fast but to restore rapidly and at scale. Immutable copies are protected because they can't be deleted, modified or encrypted - even if an attacker gains access to sensitive data. They are also relatively easy to restore, but depending upon the situation might not be a viable option. Traditional tape or diskbased backup can restore roughly one to two terabytes an hour. That's not going to cut it for most organisations, as this could lead to hours or days of downtime which could cause immeasurable financial and reputational loss to the world's biggest organisations. Thankfully, some flash-



based solutions can offer speeds of up to 270TB an hour and are needed to get an

organisation up and running with minimal negative impact.

The final thing organisations should be doing is gaining a real understanding of their data, what internal and external policies govern its retention and, drawing up policies that avoid a "store everything forever" end-state and ensuring that the policies are adhered to. They should also ensure that the backup and restore performance capabilities can grow in sync with the amount of data protected. Only by doing this can organisations sustain backups for recovery, regulatory & compliance and ransomware mitigation purposes with the growing dataset sizes that we will see in the next 5-10 years, especially with unstructured data.

Dr. Johannes Ullrich, Dean of Research, SANS Technology Institute

ata should be considered "at risk" if it can't be found in at least three locations. Organizations should aim to maintain an on-premise copy, a cloud or online-remote copy, and an offline remote copy of critical data. In particular, sophisticated ransomware will attempt to disrupt recovery from backups, and any online backup, remote or local, is at risk.

Attackers are exploiting backup system vulnerabilities to access confidential information or to disrupt recovery after a ransomware incident. Cloud backups are often more vulnerable. Controls used to monitor access to on-premise backups do not always translate one-to-one to cloud-based systems. Designing a cloud-based solution, organizations need to consider how access is controlled, how requests to retrieve or store data are authenticated and how the backup live cycle from creation over retrieval to eventual deletion is managed.

One of the main reasons to invest in on-premise backups is to speed up recovery. Cloud and offsite backups will almost always be slower. In some cases, cloud backup providers may have mechanisms to accelerate the recovery of large amounts of data by shipping hard drives instead of using slower internet connections. Make sure you test recovery speed in order to better estimate how long it will take to recover large amounts of data.

Any data leaving your direct control, for example, physical backup media being shipped offsite, or cloud-based online backups, need to be encrypted before they leave the network you control.

Backups need to be encrypted while



in transit but also while at rest at the backup location. This may, in some cases, cause additional complexity, but rarely used backup data should always be encrypted.

Manikandan Thangaraj, Vice-President, ManageEngine

bisaster recovery and data protection will play a crucial role in 2023. With ransomware attacks constantly garnering headlines, organisations should get used to the fact that it is impossible to prevent ransomware attacks entirely. It's a question of when their operations will be affected by ransomware, not if. Moreover, with the rise of Ransomware as a Service (RaaS) over the past couple



of years, global ransomware damage costs are predicted to exceed USD 265 billion by 2031.

The only way in which organisations can withstand the threat of ransomware is by investing in disaster recovery solutions. Disaster Recovery as a Service (DRaaS) has been on the rise for the past few years and its market size is predicted to reach USD 41.26 billion by 2030. The winner of the battle between the backup service providers and threat actors who leverage ransomware will be determined by how quickly DRaaS providers can react to potential new threats.

Organisations should prefer solutions built on the Zero Trust security model to ensure data security. When it comes to data backup and recovery, using a Zero Trust strategy will boost your data security because you'll be authenticating both the user and the device initiating the backup. Of course, achieving Zero Trust is a long and challenging journey, but it is a must for organisations that care about data security. Zero Trust Network Access (ZTNA) is anticipated to increase by 31% in 2023 according to Gartner, making it the fastest-growing area of network security.

Another recommended strategy to meet today's evolving threats is to implement the 3-2-1-1 backup rule which is an update to the popular 3-2-1 rule with the extra '1' covering immutable storage. Immutability will restore your data to its original, unaltered state and get you back in operation within minutes of a breach, so you can be sure that you can recover your data even after a successful attack.

ANY DATA LEAVING YOUR DIRECT CONTROL NEEDS TO BE ENCRYPTED BEFORE THEY LEAVE THE NETWORK YOU CONTROL.

Morey Haber, Chief Security Officer, BeyondTrust

orld Backup Day celebrates, everything related to data, application, and electronic technology backups. For most technology professionals, they will consider the importance of backups for servers, critical assets, and all kinds of data to protect against outages, technology failure, and threats like ransomware. Unfortunately, organisations forget the importance of backups for security disciplines. For example, having configuration backups prior to making changes is crucial just in case the desired results causes an outage or

lack of service due to a mistake or undesirable secondary anomaly. In the world of privileged access management, backups are critical for detailed items like password history. Since privileged access management solutions vault secrets and passwords, and rotated them on a regular basis, at any point in time they could potentially be different between traditional backup intervals. If a system needs to be restored from a backup, then only the password history will tell you what the correct secrets or password was at any given time for the operating system, database,

A MODERN DATA PROTECTION STRATEGY AND THE DEPLOYED BACKUP SOLUTION SUPPORTING IT MUST BE ABLE TO PROTECT WORKLOADS ACROSS ANY IT ENVIRONMENT.



application, or any managed data. This fine detail is often overlooked when considering the importance of backups for security disciplines. On world backup day, technology professionals must consider all forms of backups not only for data and assets, but for individual security disciplines themselves, and their individual functions.



good recovery plan starts with a solid understanding of the business requirements. You need to understand some common acronyms such as SLA (service-level agreement), RTO (recovery time objective), and RPO (recovery point objective). Start with the RTO, the amount of time allowed for

Thomas LaRock, SolarWinds Head Geek

the recovery to be complete, and then RPO, the point in time to which you will recover. These two will combine to help define the SLA. For example, you could have a requirement to recover a database to a point in time fifteen minutes ago (RPO) and be allowed ten minutes for the recovery to be complete (RTO). If the volume of data is such that it could take you an hour to recover to yesterday, and the business thinks the SLA should be

A GOOD RECOVERY PLAN STARTS → WITH A SOLID UNDERSTANDING OF THE BUSINESS REQUIREMENTS. fifteen minutes, you can see a disconnect between expectations and reality.

Regarding backups, you should consider the following strategy: at least three copies in at least two different formats, one of which must be immutable, and one must be stored offsite. This may seem a bit much for your regular household computer, but for a corporate environment, it is a must. For businesses, regular backups are crucial, as they often deal with confidential data, which can result in serious consequences if lost or stolen. Remember, this is about minimising loss risk and improving your chances of recovery. Taking a backup once a year isn't as useful as regular backups more frequently, for example. And storing a backup on the same hard drive as your data isn't as useful as storing it on an external drive, or in the Cloud.

BUILDING A ROBUST DATA GOVERNANCE PROGRAM IN THE UAE WHEN DATA IS YOUR CURRENCY

BY LUCIA MILICĂ STACY, GLOBAL RESIDENT CISO AT PROOFPOINT



n our digital-first economy, data is the new currency—and it is growing in value for organisations, their customers and threat actors. The ongoing processes of the digitisation and the commercialisation of data are also receiving increased attention from regulators, who are pushing for more privacy protections.

In addition, a decentralised workforce is accelerating people-centric risks in 2023, making data protection much more difficult. In 2022, the global average total cost of a data breach reached an all-time high of \$4.35 million, according to IBM Security's Cost of a Data Breach Report. According to the report, remote work is partly responsible for rising costs. The report found a "strong correlation" between remote work and the cost of data breaches. Breaches, where remote work was a factor, cost \$1 million more on average.

When looking at this from a local lens, our research shows that long term hybrid work has intensified the data protection challenge for CISOs in the UAE. With employees now forming the defensive perimeter wherever they work, 32% of Emirati CISOs agree that they have seen an increase in targeted attacks in the last 12 months. And more than 1 in 3 (37%) say that increases in employee transitions means that protecting data has become a greater challenge, with investment in information protection topping the list of priorities for the next two years. When asked how employees were most likely to cause a data breach. UAE CISOs named malicious insider as the most likely vector, where employees intentionally steal company information.

This points to a growing need for better data governance. In the UAE, for example, the Data Protection Law ensures that personal data is being collected and processed in a lawful and fair manner, while maintaining the right of individuals to be informed about how their data will be used. A robust data governance program must acknowledge this changing environment and consider its implications while answering core questions, such as: Where is your data stored? Is your data protected or regulated? How is that data used (who has access to it)? How is that data protected?

Steps for developing a data governance program

The biggest challenge for many organisations is understanding where all their data resides and how to get visibility across their entire ecosystem. Data retention is another area of struggle and regulatory tension, especially since every regulation has different requirements. Taking a phased, layered control approach to data governance will help you address these challenges and answer the core questions we are considering.

A layered approach enables you to advance from developing and defining your data governance program to maintaining and optimising it. Discovery, the first phase in this approach, involves establishing the initial control. This is where you go through steps such as qualifying the laws and regulations that apply to your organisation, defining your data protection strategy based on data lifecycles, identifying the highest-risk users, discovering your digital footprint, setting up global inventory, and indexing the data.

In the second phase (detection), you're developing control capabilities by gaining context for all your user activity, intent,

THE BIGGEST CHALLENGE FOR MANY ORGANISATIONS IS UNDERSTANDING WHERE ALL THEIR DATA RESIDES AND HOW TO GET VISIBILITY ACROSS THEIR ENTIRE ECOSYSTEM. and access; identifying compromised accounts and phished users; and classifying sensitive or regulated data. You're also taking steps to track incidents and collect and capture data from all your sources.

And finally, the last phase (enforcement) is about growing full control capabilities, such as removing data from untrusted locations, providing a secure and compliant third-party exchange, enforcing data boundary protections, implementing full compliance supervision, and so forth.

By breaking down all the big questions into smaller, actionable steps, you're creating a programmatic approach that helps you protect data based on your highest risks and gives you the best return on investment. It's important to continuously assess the effectiveness of your program and optimize it. Your environment is dynamic and threat tactics change constantly.

Focus on human-activated threats

Although the enterprise landscape changes rapidly, people stay at the core of data protection. Encouragingly, organisational cyber preparedness has greatly improved in the UAE. Increasing familiarity with the post-pandemic work environment has left CISOs feeling better equipped to deal with cyber threats. Proofpoint's 2022 Voice of the CISO report showed that while 72% of Emirati CISOs believed they were unprepared for a targeted attack in 2021, this fell to 47% in 2022.

It's important to not get complacent as threat actors will continue finding creative ways to steal and monetize your data. Protecting data in a peoplecentric threat environment requires people-centric data governance controls. Creating a strong peoplecentric framework for your data governance program will better prepare you for whatever challenges come next—and in a better position to protect your most valuable currency.

WE COLLABORATE WITH OUR PARTNERS BY BRINGING VALUE TO THE TABLE, WHILE THEY BRING IN THE RELATIONSHIP WITH THEIR ENTERPRISE ACCOUNTS.

GISEC

GISEC

EMPOWERING PARTNERS

ANITA JOSEPH CAUGHT UP WITH **MURALI VELLAT**, DIVISION MANAGER AT BULWARK TECHNOLOGIES, TO FIND OUT HOW THE COMPANY'S STRONG PARTNER ECOSYSTEM AND FOCUS ON STABLE, STEADY GROWTH, HAS POSITIONED IT AS THE VAD OF CHOICE IN THE IT DOMAIN.

ho are the new vendors vou've onboarded this year? We've onboarded a vendor that is typically considered, the last line of defense against Ransomware. If you look at the current ransomware attacks, a hacker will do two things: the first is to take the data out of the organisation and the second is to encrypt the backup or storage. This company called Continuity has a product called StorageGuard, that can automatically detect, prioritise and remediate vulnerabilities and security misconfigurations in their clients' storage and backup systems. This will help them protect their data and ensure recoverability. StorageGuard is equipped with tools to scan hundreds of storage and backup devices, provide a very clear and comprehensive report in terms of what the gaps are and provide a mitigation plan in terms of what needs to be done to fix those gaps. The interesting thing is that there's hardly any vendor this space. Therefore, they have a head start, and they provide a very comprehensive defense strategy for data residing in storage and backup to prevent it from getting into the wrong hands.

Tell us about your partners who participated at GISEC 2023

Most of the partners we have today are system integrators based in the UAE and

other GCC countries that engage with enterprises day in and day out-they carry our solution stack. We collaborate with our partners by bringing value to the table, while they bring in the relationship with their enterprise accounts. They expect us to provide support and value and we have the technical expertise to make sure we act on behalf of the vendor to provide technical, pre-sales and postsales support, making sure we bring the vendor's value and ethos to our partners as well.

What was the main objective of participating at GISEC this year?

GISEC being a security focused event is an ideal platform for vendors and distributors to showcase their security technologies to the market at large. The event gives both vendors and organisations the opportunity to understand the latest security technology trends, analyze new value propositions, tap into new opportunities and figure out how to mitigate risk and reduce the attack surface. Because GISEC is regional, it makes it a lot easier for us to reach out to the audienceboth enterprise and partners in GCC and showcase various products and solutions. This platform helps us to engage with prospects to understand their requirement and provide us the opportunity to help them understand our value proposition, better.

What are your plans for the regional market in 2023?

In 2023, we plan to continue with our expansion plans across the region. We've got a strong team in Saudi Arabia and we wish to enhance our presence there to have more footprint in the country. We will also continue to work in other countries of the region, such as Qatar, Kuwait, Oman and Bahrain.

We already have good vendors on board with us and will continue to build rapport in terms of reaching out to enterprises, sharing opportunities with partners, undertaking more channel management activities and supporting partners with the knowledge and information required to grow their business. Our strategy has been to always focus on our strengths and on the strengths of our partners. In fact, our USP is that we have a 360-degree view of the expectations of our partners, customers, vendors and the entire business ecosystem. Being in the industry for the last 23 years, we've been able to relate to our customers to ensure that we provide a very clear, go to market transparent strategy both for the vendor and partner. We believe that slow and steady growth is good for us, and we've been acquiring a lot of partners along the way, both in the UAE and in the region. We've also got a lot more vendors coming our way to address emerging trends in the cloud space. All of this will help us provide significant value to our customers and to the market as a whole. 🙎

CHECKMATE! HOW CYBERCRIMINALS CATCH CHESS PLAYERS IN A GAMBIT

long with the growing number of chess players online, the risk of related cyberattacks is also increasing. Kaspersky cybersecurity experts have discovered that chess players have been targeted by a range of different attacks from cybercriminals spreading malicious or unwanted mobile programs - even on Google Play - and Trojans and ransomware disguised as chess applications for PC and mobile.

Over the last decade, the world of chess has been growing rapidly with more and more platforms and apps for training appearing online, and numerous global tournaments organized in digital formats. However, the online development of chess has also piqued the interest of → WITH CHESS PLAYERS CONSTANTLY LEARNING NEW TACTICS AND PLAYING WITH OTHERS ONLINE, THEY OFTEN DOWNLOAD APPLICATIONS FOR THEIR COMPUTER AND MOBILE DEVICES -OFTEN FROM THIRD-PARTY SITES.

cybercriminals, who try to catch online chess players with a variety of tricks.

With chess players constantly learning new tactics and playing with others online, they often download applications for their computer and mobile devices - often from third-party sites. Needless to say, under the disguise of these apps may be hidden malicious files. According to the latest Kaspersky statistics, in 2022, cybercriminals made 139,203 attack attempts targeting almost 12,000 chess players.

In most analyzed cases, Kaspersky researchers discovered Downloaders able to install other unwanted programs, but there were also other Adware and even Trojans - malicious programs that can enable cybercriminals to gather credit card details, and credentials, modify data or disrupt the performance of computers. They also found cybercriminals spreading ransomware disguised as chess



applications, able to encrypt any files on the infected device. The majority of attacked chess players were in Russia, India, Vietnam, Brazil and Germany.

Kaspersky researchers also discovered that in the last several years, cybercriminals were distributing malicious mobile apps or unwanted software under the guise of chess games. One, simply called "Chess", was found on Google Play but has since been removed. Outside of Google Play, the scammers are also actively spreading mobile malware and adware via third-party sites. One of the apps we detected in 2023 sent SMS messages from an infected user's phone, making it a spamming tool for cybercriminals. The other, like most attackers' files hidden behind chess applications, is an adware that periodically opens advertising tabs in the browser against the user's will - mimicking a reallife application called "Chess Pro" on Google Play, with more than 100,000 downloads.

"The world of chess has changed dramatically in recent years, becoming digitalized, with training and even international championships taking place online, allowing players to globally share experiences and compete against each other. However, as we see, the popularity of chess is also being exploited by attackers, distributing thousands of malicious files disguised as chess. It's never been more important to remain vigilant and remember basic cybersecurity rules in order not to fall a victim to cybercriminals whether it's phishing emails, or suspicious mobile apps that only mimic chess," comments Igor Golovin, a security expert at Kaspersky.

"Chess world has been going digital for decades — one of the first computer games ever was chess. But recently, most of chess has made the digital jump, and not only casual gamers, but chess education, elite level competitions, chess clubs, schools, etc. For instance, our e-gaming platform FIDE online arena every month hosts over 600 tournaments. Thus, new challenges connected to digital world, are now key for chess: cheating, cybersecurity, ID management, connection between digital and OTB (over-the-board



play), computational power arms race, and more. Technology is changing the world of chess right now, so players shall be ready to answer those challenges" said Ilya Merenzon, CEO of World Chess.

To stay safe from mobile threats, Kaspersky recommends:

- Check the permissions of the apps that you use and think carefully before permitting an app, especially when it comes to high-risk permissions such as permission to use Accessibility Services. The only permission that a flashlight app needs is to the flashlight (which doesn't even involve camera access).
- A reliable security solution can help you to detect malicious apps and adware before they can start behaving badly on your device.
- iPhone users have some privacy controls provided by Apple, and users can block app access to photos, contacts and GPS features if they think those permissions are unnecessary.
- Update your operating system and important apps as updates become available. Many safety issues can be solved by installing updated versions of software 1

THE ROAD AHEAD

ANOOP DAS, ENTERPRISE MANAGER, MIDDLE EAST AT MIMECAST, TELLS ANITA JOSPEH HOW THE COMPANY'S CHANNEL-FIRST STRATEGY WILL CONTINUE TO DRIVE ITS GROWTH, TRANSFORMATION AND CUSTOMER REACH.

hat is the biggest market opportunity for you and your channel partners in 2023?

The adoption of hybrid work environments has added another level of complexity to the cyber threat landscape. With employees working in offices and remotely, the attack surface of where work happens, is wider than ever before - resulting in an onslaught of attacks targeting the cloud-based intersection of business communications, people, and data. New and emerging collaboration channels - Microsoft Teams, Slack, Zoom, WhatsApp, etc. - have grown in popularity because of the rise of hybrid work - and have now joined email as a primary attack vector for threat actors to exploit. But it's important to remember that criminals think about the outcome – not the vector – when launching their attacks. So, the problem can't be solved with communication security alone. Firstly, there's a people element and at Mimecast we have a big focus on security awareness training and providing contextual guidance to users about potential risks in email, which helps make them smarter. And while we're known as an email security company it's not just about email, it's actually about work and making sure you can have confidence in your digital work environment and are able to work protected. To address this, we work with our channel partners to deliver vital protection to companies of all sizes, by integrating with other security vendors who are focused on other categories of protection.

What technology investments will you make in 2023?

Last year we launched the Mimecast X1 platform, which now serves as the foundation for the Mimecast product suite. Powering fully integrated services that deliver industry-leading protection for communications, people, and data, the X1 platform makes information actionable and provides the reliability, resilience, and scale the modern threat landscape demands. In the Middle East we plan to launch our Email Security, Cloud Integrated solution. The gatewayless solution is designed to optimise protection for Microsoft 365 environments with scalable, best-in-class email and collaboration security. Typically deployed in less than five minutes, this solution is ideal for IT teams that need email security delivered the fastest way possible. We also plan to continue developing new tools and technologies that keep pace with the evolving threat landscape - looking deeper into social graphs, metadata, and other emerging chains of communication.

What challenges will customers will face in 2023?

The volatile state of the global economy will create tough budgetary conditions for customers in 2023. Organisations need to pivot from reactive patchwork cyber spending - causing widespread tool sprawl across cybersecurity - to proactive investment strategies closely aligned to their greatest areas of cyber risk. Making risk-driven investment decisions is the best way to preserve costs while maximising ROI amidst economic volatility. CISOs must also be able to effectively identify risk, measure its potential business impact, and then

ORGANISATIONS NEED TO PIVOT FROM REACTIVE PATCHWORK CYBER SPENDING TO PROACTIVE INVESTMENT STRATEGIES CLOSELY ALIGNED TO THEIR GREATEST AREAS OF CYBER RISK. articulate this to their executive board to secure adequate.

The cybersecurity skills shortage will also remain one of the biggest challenges for organisations. Many global organisations find it difficult to recruit appropriately skilled cybersecurity professionals, leaving teams under pressure and under-resourced. But the cyber threat landscape continues to accelerate at a rapid pace, driving higher levels of burnout and human error across the sector. The companies best positioned to offset cybersecurity's labour challenges are those adopting security tools and platforms that offer integration into an organisation's existing security ecosystem.

How will Mimecast successfully work with channel partners in 2023?

Our channel partners are a key component of Mimecast's success as a company. After rolling out new offerings, we'll look to our channel partners to engage with existing customers and new prospects. We rely on them to help guide buyers toward smart purchasing decisions that deliver real value for their organisation. They understand their customers' security environments and are able to provide them with additional offerings to improve their security posture.

What are your top priorities for 2023?

In 2023, we will continue to listen to our customer community with the goal to meet and exceed their expectations. Partners regularly speak to the end users and can share valuable insights on how we can help our customers so we will work closely with the channel to ensure success in this area. On a global level, we are building a new engineering centre of excellence in Mississauga, ON, Canada, which will serve as a key component in helping us grow our product offering and innovate. We also have other initiatives in the works to help amplify our product offerings and expand our market reach.



ENTRUST LAUNCHES ZERO TRUST READY SOLUTIONS

ntrust, a global leader in identity and data security,
is supporting organisations' Zero Trust journey with new foundational identity,

encryption, and key management solutions.

"Zero Trust approaches are reshaping security in a perimeter-less world. While the conversation often starts with identity and network access, organizations are quickly finding that identity and access management is only the beginning. A comprehensive Zero Trust framework starts with enabling trusted identities across users, devices, machines, apps, and workloads, and extends to a data protection strategy to secure data intransit, at rest, and in-use across both public and private cloud environments," said Bhagwat Swaroop, President of Digital Security Solutions at Entrust.

"Getting to a Zero Trust framework is a multi-year project, one that requires trusted partners to help you build your framework on a solid foundation. Entrust is uniquely positioned to help organizations establish Zero Trust foundations: including both highassurance identity and access management and applied encryption to help secure data today and for the post-quantum future. Moreover, our capabilities extend to comprehensive security posture management governing identities, entitlements, keys, certificates and secrets across multi-cloud, hybrid, and on-premises operations," Swaroop said.

To support this evolution, Entrust is introducing pivotal advancements in identity, encryption, and multicloud security to support Zero Trust frameworks. These include:

- Identity: Adding new passwordless, certificate-based authentication with smart keys and FIDO2 passkeys to the full-suite Entrust Identity IAM solution; as well as cloud-based Entrust PKI as a Service (PKIaaS) turnkey integration with Microsoft Intune and other mobile device management (MDM) providers to accelerate device enrollment at scale.
- 2. Encryption: Launching nShield 5, a high-performance, next-generation HSM with multitenant capable architecture and support for postquantum readiness.
- 3. Multi-Cloud: Releasing new Entrust KeyControl 10 solution, using an innovative approach that delivers consistent multi-cloud key and secrets policy compliance management, for data protection across SaaS applications, customer

databases, and workloads, both cloud-based and on-premises.

Identity: Cloud-based IAM solution passwordless options with FIDO-2 compliance, passkeys, and enhanced risk-based authentication

As enterprises continue to advance their Zero Trust projects, an identity-first approach to security is foundational. Entrust has been enhancing its Identity as Service (IDaaS) solution, a full-suite IAM platform. Enhancements include:

- New high-assurance passwordless capabilities that include certificatebased authentication, FID02 keys, FID02 passkeys and others.
- 5. Elevated security with enhanced risk-based adaptive multifactor authentication that seamlessly integrates additional risk factors from external providers and performs continuous validation throughout user sessions, as well as enforces appropriate step-up authentications.
- Support of outbound System for Cross-domain Identity Management (SCIM) for app provisioning in third-party cloud applications (service providers).
- Entrust also has enhanced Customer IAM (CIAM) capabilities,

enabling seamless and connected experiences for customers or citizens with passwordless authentication, digital signing, ID verification & proofing for a more secure digital experience.

Recognising that secure device enrollment at scale is critical to Zero Trust frameworks, Entrust also has added zero-touch, turnkey integration between its cloud native Entrust PKI as a Service (PKIaaS) and Microsoft Intune and other MDMs, allowing customers to leverage Entrust PKI seamlessly with their IT management platform in minutes – without the need for on-premise hardware or software. Organizations can enroll devices of any kind securely with extended key and certificate parameters to support advanced identification, authentication, and authorization schemes that enable Zero Trust frameworks.

Encryption: Next-generation HSM performance and crypto-agility

Encryption is at the heart of Zero Trust frameworks, providing critical protection for sensitive data. As demands on encryption continue to expand, Entrust is launching the next generation of its Entrust nShield Hardware Security Modules. The new nShield 5 HSMs deliver superior performance for the root of trust enterprises need across today's business-critical enterprise applications and provide a platform for the future cryptographic data protection needs of a post-quantum world. Entrust nShield 5 HSMs use an innovative multitenant capable architecture scheduled for certification to the FIPS 140-3 standard.

"As enterprises increasingly migrate business processes to the cloud, managing privileged access credentials and secrets continues to be a top priority. Ensuring that critical applications



and their underpinning cryptographic keys and secrets can be protected and managed throughout their lifecycle is vital. The launch of the new Entrust nShield 5 HSM gives our joint customers the robust hardware root of trust they need to protect their organizations' most critical assets," said David McNeely, CTO for Delinea, an Entrust partner.

"F5's deep experience in application delivery and security services helps customers protect their critical applications, ensuring they are safe, secure, and always available. The launch of Entrust FIPS nShield 5 HSM provides F5 customers with not only enhanced performance but also cryptographic agility for a rapidly changing threat landscape," said Arul Elumalai, SVP and General Manager of BIG-IP at F5, an Entrust partner.

Multi-cloud security: Redefining key management with decentralized vault and cloud-based compliance management

Protecting encryption keys is critical to

ENCRYPTION IS AT THE HEART OF ZERO TRUST FRAMEWORKS, PROVIDING CRITICAL PROTECTION FOR SENSITIVE DATA.

the Zero Trust foundation. The newest release of the Entrust KeyControl solution enables information security teams to centrally manage encryption keys and secrets across decentralized. multi-cloud applications. With this release, the KeyControl solution uses a unique, innovative decentralized vault-based architecture, combined with centralised compliance and risk management to deliver enhanced keys and secrets management. This approach lets an enterprise replace manual or ad hoc practices with consistent policy governance for data protection across customer databases. whether cloud-based, hybrid, or onpremises.

"In the face of persistent threats of cyberattacks, organizations demand cyber resilience for their data," said Joseph Razavian, Head of Security Alliances, Cohesity, an Entrust partner. "By running Entrust KeyControl 10 in conjunction with the Cohesity Data Cloud, enterprises not only gain automated and simplified encryption key management but can also better secure, manage and unlock value from their data no matter where their data is for comprehensive cyber threat protection."

Back in the driving seat

with Cisco Webex





Remote working made simple with Cisco Webex App and devices.

Your customers are rapidly adapting to an increased demand for remote and flexible working measures. We all know how stressful it might be to work away from the office when you do not have the right equipment to connect to your colleagues remotely.

As they move towards a more hybrid workplace, help your customers opt for solutions that are fully integrated and ultimately make remote working as simple as possible. Cisco Collaboration portfolio includes a range of devices that when paired with the Webex App deliver the ultimate collaboration experience.

Back in the driving seat with Cisco Webex

Are your customers asking for collaboration tools that:

- Can be used in any space i.e home, office without compromising on sound and connectivity quality
- Replicate the same immersive meeting experience of a boardroom
- Are easy to install and manage remotely from a single platform

What they need is Cisco Webex App combined with Cisco Desk Camera and Cisco Headsets.

Cisco Webex App

products of Cisco Webex.

One secure place to call, message, meet, and get the work done

- meetings with integrated conferencing devices and headsets Message, file share and one-click calling in always-on spaces with people
- inside and outside of the organization High-definition meetings integrated with the calendar and rich AI-powered transcriptions and real-time translations
- Powerful noise-cancelling technology
- Meeting templates and stage layouts
- Third party app integration

Cisco Desk Camera

Cisco's first device designed to bring high-quality 4K ultra HD video to every space. A collaboration experience in vibrant colors and an incredible low light performance. Plus, it's Al-powered and remote IT managed.

- 4K USB web camera with superb video resolution, frame rate .
- . Great quality in different light conditions, auto focus, auto whitebalance, adjustable FOV
- . High-quality microphone audio with background noise reduction
- . Secure facial recognition login and occupancy detection
- Direct connection to a personal computer. It can be fully mounted onto an external monitor, laptop, or even a tripod
- or a desk stand Manage Cisco Desk Camera in Control Hub

Cisco Headsets 700 series

Designed for mobility and outstanding noise cancelling performance in any work environment. Your customers will enjoy the premium audio quality, while benefiting from complete audio privacy, and will immerse themselves in a truly satisfying listening experience.

- Premium sound quality
- Powerful noise-cancelling technology
- Fully integrated with Cisco Webex solutions
- Powerful back end system to remotely manage firmware updates and installation
- User-app to truly personalise the headset experience for your customers
- Manage Cisco Headset in Control Hub

Webex App + Webex Desk Camera + Webex Headsets 700 series: help your customers make their remote working experience more enjoyable and productive.











SIMPLIFYING IT CHALLENGES

ABDUL REHMAN TARIQ, REGIONAL SALES DIRECTOR, MIDDLE EAST, SOLARWINDS TELLS ANITA JOSEPH ALL ABOUT THE COMPANY'S OBSERVABILITY PLATFORM.

ell us about the SolarWinds Hybrid Cloud Observability platform. What inspired the setting up of such a platform?

Building on more than 20 years of expertise in listening to customers and

building products designed to solve the problems they face in managing highly performant IT infrastructures, we heard them clearly say they're seeking more consolidated approaches to today's challenges. Hybrid Cloud Observability unites the world-class modules and capabilities of our Orion suite, together with our Secure by Design principles and approach, to create a truly fullstack observability offering built to meet customers wherever they are on their digital transformation journeys and take them where they need to grow.



How is the Observability platform expected to simplify today's IT challenges?

Our observability platform simplifies today's IT challenges by uniting data and people. Modern IT environments have an enormous number of moving parts, which makes problem-solving complex. If an application engineer spends three hours troubleshooting an app and finds it's really a DNS issue, they've lost three hours before the network team gets involved. Having all the relevant information in a single view is a key benefit and will help IT work together as a team again.

Digital Transformation is well underway. How is the SolarWinds Observability platform helping channel partners and customers harness the opportunities that this transformation journey presents?

Digital transformation pushes an organisation out of its comfort zone and it may need to use technologies it might not be particularly familiar with. Add to that constrained resources and budgets, and the complexity can create a real challenge. The SolarWinds Platform helps them optimise workloads, reduce the time to resolve issues, and plan migrations, turning those challenges into value.

The SolarWinds Platform provides a costeffective option for customers to accelerate their digital transformations. Our channel partners can help their customers with these problems without the unnecessary complexity and overhead associated with other options on the market.

Data Management is a huge issue today, given that it is disparate and resides in different places. How does SolarWinds Observability help eliminate tool sprawl and ensure effective data management? Tool sprawl and data proliferation can be a nightmare for IT teams to wrangle. If an IT professional needs five different tools to investigate an issue, they're wasting a lot of time. And that's without considering tool licensing costs! Worse, as data represents the lifeblood of today's enterprises, performance issues with its data estate can negatively affect the experience an organisation delivers to

 $\rightarrow \begin{array}{l} \text{THE SOLARWINDS PLATFORM PROVIDES A} \\ \rightarrow \begin{array}{l} \text{COST-EFFECTIVE OPTION FOR CUSTOMERS TO} \\ \text{ACCELERATE THEIR DIGITAL TRANSFORMATIONS.} \end{array}$

internal and external users.

Our platform-based approach allows us to consolidate a lot of different tools across all stacks and layers in IT. We collect metrics from the network, databases, local infrastructure, clouds, and applications and unite them in a single view, empowering organisations to become more efficient and effective in managing the complexity they face.

Are you planning any upgrades/updates to this platform, given that technology is rapidly changing? If so, what are they?

Constant change requires constant improvement. At SolarWinds, we engage our users continually to understand the updates and new features they need most. We connect with them through THWACK, our user community of more than 190,000 registered members, where they can suggest updates and other users can vote on them, meaning they have a real voice in our development roadmap.

One of the big things we're working on is a tighter integration with our service management solution, SolarWinds Service Desk. It's already possible to open, update, and close tickets automatically, and customers can pull inventory information from Hybrid Cloud Observability into Service Desk, but we want to take it further.



LEVERAGING THE TRUE VALUE OF DATA WITH CLEAR DATA STRATEGIES

MARTIN MAZUR, DATA & ANALYTICS PRACTICE LEAD @GELLIFY

ata has emerged as a crucial resource for businesses of all kinds, including those in the Middle East, in the current digital era. Data's worth is only increasing as society gets more datadriven, and companies that don't make use of it run the risk of slipping behind their rivals. Organisations must create clear data strategies that are adapted to their own business objectives and cultural setting in order to realise the full value of data.

The importance of enterprises in the Middle East adopting clear data strategies is highlighted by the enormous development of data, but before proceeding to the steps of creating one, there are a number of considerations involved due to the specificity of the demographics, where data strategy can be a slippery slope without these considerations.

Cultural context is an important factor to take into account while creating a data strategy. The region has a strong cultural heritage, which has an impact on how people use technology and interact with data. It is important to consider the local culture and values when gathering, managing, and analyzing data. For instance, firms must make sure that their data strategies adhere to regional laws and cultural norms because privacy and security issues are very important in the Middle East.

Implementing a data strategy also calls for a shift in organisational thinking and entrepreneurial culture. In 2022, a study uncovered an astounding statistic: 91.9% of respondents believed that people and culture are the biggest blockers of data-driven change. Workers need to be educated on the importance of data and how to use it to propel company expansion. Data must be viewed as a strategic asset that can drive innovation, better business processes, and improve customer experience. This culture of data-driven decision-making must be promoted.

Finally, the lack of trained talent in

the data science industry is another issue Middle Eastern businesses must deal with. Only 23% of Middle Eastern organisations have data science capabilities. This presents a huge challenge for businesses looking to create and apply data strategy. In order to address this issue, enterprises must either spend money on internal talent development and training or look for collaborations with data science companies on the outside.

While creating a data strategy might be challenging, it is crucial for Middle Eastern businesses looking to expand and remain competitive. A data strategy is a road map for how a company will gather, manage, and use data to accomplish its objectives. It must be compatible with the values, cultural, technological, financial, and legal aspects of the organisation. A successful data strategy must also be a dynamic that changes along with the business and acts as a GPS navigator towards organisations' data transformation journey.

In light of this, there is a need for Middle Eastern companies to develop and implement clear data strategies that align with their business goals and values. Creating a clear data strategy with all considerations listed may seem like a daunting task, but it can be broken down into three simple steps: assessment, target, and roadmap.

Step 1: Assessment Stage

The assessment stage is the first and crucial step of developing a data strategy as it provides a comprehensive understanding of how the organisation currently operates. It is essential to examine how technology is being utilised, how data is delivered to endusers, and how data is documented to generate insights. Consulting companies need to spend time and hold meetings with members at all levels of the organisation to gather this information accurately. The assessment stage typically takes up around 50-60% of the total time required to create a data strategy.

Step 2: Target Stage

Once you have assessed your organisation's current data capabilities, the next step is to identify your target data capabilities. Statistically 70% of executives are concerned that the organisation does not allocate sufficient capabilities and resources to reach the goals. To ensure success, defining your organisation's data-related goals and determining what capabilities are needed to achieve those goals is a crucial step.

During this stage, it is also important to take an agile approach and focus on quick wins. This means identifying areas where small improvements can be made quickly and focusing on those first, rather than what the majority of organizations do - focusing on a big-bang approach.

Step 3: Roadmap Stage

The final stage is where a lot of data strategies collapse. Organizations want 3 or 5-year roadmaps, whereas, in our opinion, roadmaps should be for 6 months to a year, and reviewed frequently. The reason for this stems from our experiences with clients: trying to create a roadmap and set costs for a long-term roadmap is unreliable due to the rapidly evolving field of data. There's a high likelihood that soon, a better and/or cheaper technological solution becomes available, rendering your long-term roadmap obsolete. It becomes important to monitor the strategy at shorter periods rather than reviewing it at the end of the long roadmap. Another aspect is that a longer roadmap requires more resource commitment, which can scare clients.

In conclusion, data is a critical asset for organisations in the Middle East, and developing clear data strategies is essential for fully leveraging its value. However, having a data strategy is just the first step: having the recipe and buying the ingredients doesn't mean the final product is ready, but there's still a long road ahead. A good data strategy will act as the GPS for you as your organisation navigates the journey toward its data transformation journey of staying competitive in the digital age.

F5 SAFEGUARDS DIGITAL SERVICES WITH NEW AI-POWERED APP AND API SECURITY CAPABILITIES

5 has announced new security capabilities to give customers comprehensive protection and control in managing apps and APIs across on-premises,

cloud, and edge locations. Specifically, new machine learning enhancements provide F5's cloud security portfolio with advanced API endpoint discovery, anomaly detection, telemetry, and behavioral analysis. As more transactions and customer engagements occur through digital channels such as web and mobile apps, organizations are seeking better solutions to provide secure experiences for their end users and maintain their trust. With APIs as the building blocks of modern web and mobile experiences, protecting these assets is the cornerstone of securing digital services.

F5 customers can now strengthen their security posture with a continuously improving analysis engine and unified policy enforcement. These capabilities enable secure app-to-app communications through validated and monitored APIs, thereby reducing the time security teams spend correcting false positives and accelerating timeto-deployment for new services. The



enhancements, as well as new managed service offerings for enterprises and service providers, accelerate the momentum of F5 Distributed Cloud Services, introduced in 2022 and bolstered by the recent launch of multicloud networking solutions.

Modern organisations continue to demonstrate a clear preference for hybrid solutions.

"Applications and APIs are the building blocks of the digital experiences through which we all work, bank, shop, access healthcare, travel, and play," said Kara Sprague, EVP and Chief Product Officer, F5. "And those experiences are only as secure as the most vulnerable app or API. With greater efficacy achieved via sophisticated profiling techniques and deployment options that span SaaS, packaged software, hardware appliances, and managed services, F5's app and API security solutions are unmatched. This announcement continues our mission to radically simplify app and API security. empowering customers to accelerate digital innovation with the confidence of comprehensive protection no matter how their apps are built or where they live."

F5 offers a full suite of capabilities to provide robust protection for apps and APIs across on-premises, cloud, and edge locations. Moreover, F5's end-to-end approach to security means that threat data can be gathered and analysed across all deployed locations, including ongoing and emerging attack campaigns detected by the F5 Threat Campaigns service. As part of a larger hardware, software, SaaS, and managed services portfolio that also provides best-in-class application delivery capabilities, F5 security solutions protect a diverse mix of distributed apps and APIs in any environment without adding further operational complexity. 1





OptiNANDTM TECHNOLOGY



Ultrastar[®] DC HC570 22TB^{*} HDD

GROW YOUR DATA, NOT YOUR FOOTPRINT

Exponential growth of data means organizations must find ways to efficiently store more data. The Ultrastar® DC HC570 22TB¹ HDD with OptiNAND[™] technology is the next leap in high-capacity hard drives, allowing data centers to maximize their storage, especially in footprint- and power-constrained environments.

Redington

Learn more at westerndigital.com.

©2023 Western Digital Corporation or its affiliates. All rights reserved. *ITB = 1 trillion bytes. Actual user capacity may be less depending on operating environment. Western Digital, the Western Digital design, the Western Digital logo, OptiNAND, and WD Purple are registered trademarks or trademarks of Western Digital Corporation or its affiliates in the US and/or other countries. All other marks are the property of their respective owners. Product specifications subject to change without notice. Pictures shown may vary from actual products.

For inquiries, please contact Shuja Kidwai at shuja.kidwai@wdc.com







Transforming Network Data into Real Insights

GET THE INSIGHTS, CONTEXT, AND CONTROL YOU NEED WITH POWERFUL FEATURES LIKE:

Incident analytics

- ML-driven root cause analysis and remediation
- Al-driven severity classification

Network health monitoring

 Create and monitor SLA categories and thresholds

Client troubleshooting

 Granular client connection diagnostics and event correlation

Data Explorer

Customizable visualization of historical data

Reporting

Curated reports of historical data

Service validation

Network self-validation via virtual client that resides on RUCKUS access point

Melissa AI-powered virtual network assistant

• Answers IT questions in natural language

IT service management integrations

Integration via webhooks with leading ITSM platforms such as ServiceNow and Salesforce to automatically initiate helpdesk tickets

Designate a third party for management

Two-tiered management–log in once to access multiple customer accounts under management

RUCKUS Analytics is a next-generation service for network analytics and assurance. Powered by machine learning (ML) and artificial intelligence (Al), it delivers comprehensive visibility into the operation of your RUCKUS enterprise network. The service accelerates troubleshooting and helps IT teams meet their network SLAs. With streaming network telemetry from network devices, RUCKUS Analytics automatically transforms data into deep insight. Get the information you need to be much more efficient in network assurance—freeing up time to focus on other projects. RUCKUS Analytics supports SmartZone and RUCKUS Cloud control and management architectures. If you prefer, you can designate a third party such as a RUCKUS networking solution provider to administer your account. Managed service providers (MSPs) can manage multiple end-customer RUCKUS Analytics accounts from within their own account.



Want to learn more? Scan this QR code and book a demo!

