ADVISOR LE EAST

HIGHLIGHTS

RESECURITY PALO ALTO **ACCEDIAN**

DECENTRALISING

DR NAVEEN SINGH, CEO & CO-FOUNDER AT INERY, A REVOLUTIONARY DECENTRALISED DATABASE MANAGEMENT SOLUTION POWERED BY BLOCKCHAIN TECHNOLOGY, TELLS ANITA JOSEPH WHY IT IS IMPORTANT FOR ENTERPRISES TO HAVE A DECENTRALISED DATABASE MANAGEMENT SYSTEM AND HOW THE COMPANY SETS A NEW BENCHMARK IN THIS SPACE.

🗱 tahawultech.com

....

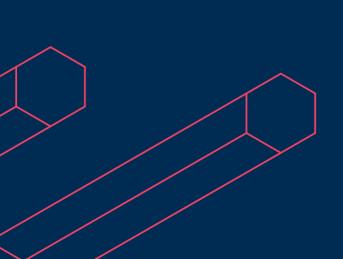
SUPPLEMENT



Be data 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

Securaty









- Roundup of top news stories from the security industry in the region and beyond
- Mehdi Paryavi, Chairman, IDCA, on how the global organisation helps the world build sustainable digital economies.
- Helmut Reisinger, Board member & CEO of EMEA & LATAM at Palo Alto, on how the region is particularly vulnerable to cyber-attacks and must be vigilant.
- Richard Piasentin, Chief Strategy & CMO at Accedian, on how the company is on a mission to make technologies that connect people and systems as transparent and effective as possible.

Fortinet Security Fabric

Broad

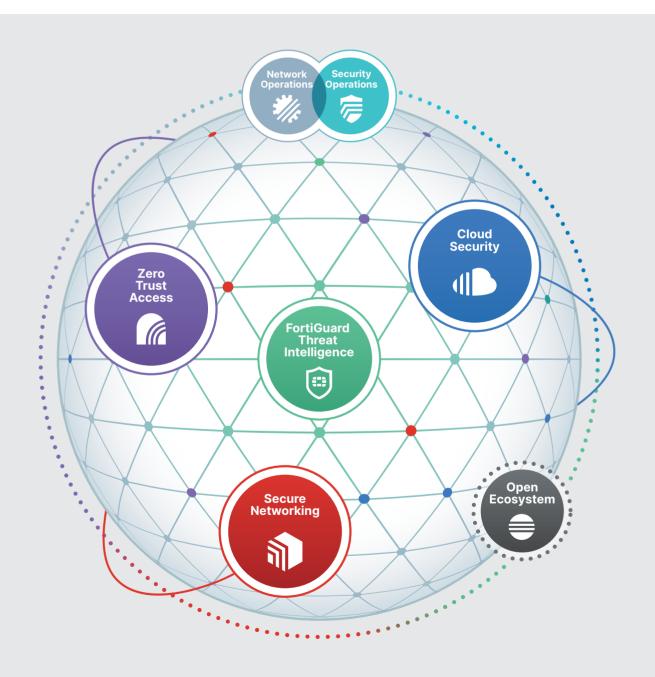
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with Al-driven security for fast and efficient operations







EDITOR'S NOTE



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

> **Anita Joseph** Editor

FVFNTS





THE POWER OF WEB5

The term "Web5' was first coined by Tim

Berners-Lee, the father of the Internet, as an open, connected, permission less, and intelligent web platform, or simply, the Emotional Web or Symbiotic Web. It was recently revived as an extra opensource, decentralised web platform that will be an interconnected network able to communicate with humans the way humans communicate with each other. According to Jack Dorsey, Web5 will be the amalgamation of the best features of Web2 and Web3, built **BREAKING** on top of the Bitcoin network. **DATA SILOS**

In this context, the drastically changing need for data prompts businesses to look for solutions that can meet the high demands of their consumers. However, centralised databases have proved to be costly, puzzling, and complicated, especially when extra layers are added to an enterprise's database. In addition, the infrastructures don't give businesses the ability to conduct query searches on vast amounts of data. A decentralised data system will break enterprise data out of data silos, enabling the seamless sharing of information that is consistent and reliable for decision-making. Hence, it greatly promotes innovation and the progress of modern business.

Enter Inery, a proprietary layer-1 blockchain and decentralised data

PRODUCTION AND DESIGN

Designer

Prajith Payyapilly

prajith.payyapilly@cpimediagroup.com

solution. Inerv integrates blockchain's decentralisation, immutability, and security features with distributed database management properties to enable next-gen innovation for data management. Our cover story focuses on data decentralisation, in an exclusive interview with Dr Naveen Singh, CEO & Co-founder at Inery, who dwells at length on how the company is at the forefront of creating a new paradigm for decentralised data management.

> We've also got lined up for you, special interviews with security frontrunners who were part and parcel of the recently-concluded GITEX Global. They talk of their

participation in the event and how their cutting-edge solutions and services are helping the security industry stay ahead of sophisticated and complicated attacks.

Not to be missed is a special opinion piece by Taj El-khayat, Managing Director - South EMEA at Vectra AI, on the 9 Cs of cybersecurity, and what they mean for the modern business. We've also got for you a very special analysis from Veeam Software, where they spotlight how organisations are increasing modern data protection for cloud workloads to reduce cybersecurity risks.

There are a host of other exciting developments and refreshing perspectives in this issue, which we're sure, will make for an interesting session. Happy Reading!

FOUNDER, CPI Dominic De Sousa (1959-2015)

Published by



ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Daniel Shepherd daniel.shepherd@cpimediagroup.com

OnlineEditor

Editor

Anita Joseph

anita.joseph@cpimediagroup.comm

DIGITAL SERVICES Web Developer Adarsh Snehaian webmaster@cpimediagroup.com

Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAF

Tel: +971 4 5682993

© Copyright 2022 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.

Sales Directo Sabita Miranda sabita.miranda@cpimediagroup.com

DELINEA SECRET SERVER INTRODUCES ADDITIONAL SECURITY FEATURES & ENHANCES DISASTER RECOVERY

Delinea,
a leading
provider of
Privileged
Access
Management
(PAM) solutions



for seamless security,
has announced new enhancements to
the Secure Shell (SSH) Cipher Suite and
Secure File Transfer Protocol (SFTP)
tunneling of Secret Server, its awardwinning PAM solution. Further additions
to disaster recovery capabilities help
ensure Secrets data and permissions are
available even during a disruption.

In 2021, 82% of breaches involved the human element; including the use of stolen credentials, phishing, misuse, or just error, according to the 2022 Verizon Data Breach Investigations Report. By centralising privileged credentials in an encrypted password vault, organisations can significantly reduce human-centered risk.

Enhancements to the SSH Cipher Suite provide customisation of the ciphers used when making SSH connections for various tasks such as credential discovery, password changes, or heartbeat. Heartbeat provides up-to-the-minute monitoring of passwords and credentials, and triggers alerts if they are changed outside of the vault or without knowledge. The new SSH Cipher Suite features allow users to easily set availability and application order for key exchange, MAC address, and encryption algorithms, allowing organisations to tailor ciphers to meet their best practices and increasing the security of the connections made through the vault. Admins can also easily remove old or non-approved ciphers and avoid remediation work should those ciphers be highlighted in a vulnerability scan.

KASPERSKY ENDPOINT DETECTION AND RESPONSE EXPERT RECEIVES STRATEGIC LEADER STATUS FROM AV-COMPARATIVES

Kaspersky Endpoint Detection and

Response Expert has received Strategic Leader status after comprehensive testing by AV-Comparatives. The recognition is for automatically stopping every attack, reporting them correctly, and the consistent mapping of MITRE's tactics, techniques, and procedures (TTPs). Testers also praised the product for both high return on investment, and low total cost of ownership (TCO).

According to the AV-Comparatives Enterprise EPR CyberRisk Quadrant - part of the Endpoint Prevention and Response (EPR) Test - Kaspersky Endpoint Detection and Response Expert received the highest level 'Strategic Leader', one of the best levels of effectiveness at preventing and responding breaches combined with reasonable product cost and operational accuracy. "Kaspersky Endpoint Detection and Response

kaspersky

Expert was able to protect against all the targeted attacks during the assessment, before the threats could progress inside and infiltrate the organisation's network. It demonstrated both cumulative Active and Passive Response rates at 100 percent" said Andreas Clementi, CEO and founder of AV-Comparatives. "We're pleased to receive the new confirmation about the true capabilities of Kaspersky EDR to actively protect enterprise infrastructure from targeted attacks. We participate in such complex assessments to independently verify that we develop efficient technologies inside the security solutions, and we are ready to protect customers' corporate networks" – said Alexander Liskin, Head of Threat Research at Kaspersky.

COHESITY & LENOVO EXPAND PARTNERSHIP TO STRENGTHEN CYBER RESILIENCE AND SIMPLIFY DATA MANAGEMENT

Building on their global reselling

relationship established in 2021, Cohesity and Lenovo have now teamed up to deliver pretested and certified solutions bringing Cohesity's modern data security and management platform on Lenovo's ThinkSystem servers. The expanded partnership delivers validated solutions designed to protect enterprise data from on-premises to the cloud and address three of today's highest-priority business issues—security, cloud, and data management.

"Protecting critical data and extracting business value from it poses significant challenges for enterprises. Legacy approaches to data security and data management with piecemeal solutions lead to operational complexity and cyber exposure while adding costs and compliance risks," said Gregg Petersen, Regional Director Middle East and Africa at Cohesity. "Our expanded partnership with Lenovo brings together two

COHESITY

industry leaders to offer our customers a simple and seamless experience. The partnership also enables customers to confidently strengthen their cyber resilience by protecting and, if necessary, rapidly recovering business-critical data wherever it resides from on-prem, hybrid, multicloud, and edge environments."

Customers will benefit from simplified ordering processes and a faster time to value, as the integrated solutions and their technical interoperability have been certified. The solutions can be ordered globally and directly from the Lenovo Data Center Solution Configurator (DCSC), which provides one-stop purchasing for the Cohesity SKUs, including support and services for all phases of the solution lifecycle.

EMT DISTRIBUTION ANNOUNCES PARTNERSHIP WITH XCITIUM DELIVERING ZERO TRUST ENDPOINT PROTECTION TO MIDDLE EAST & AFRICA

emt Distribution, a leading Value-Added

Distributor that offers next generation, cutting-edge technologies, has announced an enhanced partnership with Xcitium to deliver Zero Trust Endpoint protection to its customers in the Middle East and Africa.

Xcitium released its patented Kernellevel API Virtualization technology earlier this year, providing enterprises with the ability to isolate and remove threats before they can cause any damage. ZeroDwell Containment is a first-of-itskind system that proactively protects endpoints without any disruption to a customer's workflow.



"Our aim
is to help
organisations
in the region
maximise their
cybersecurity
while also allowing

our channel partners to enhance their technology portfolio's with the latest solutions," said M Mobasseri, CEO at emt Distribution. "Xcitium's technology prevents ransomware and other malware from causing damage no matter a customer's existing EDR, XDR or MDR solution. ZeroDwell Containment provides an additional layer of protection

to maximise defense against cyber threats."

At a time when more than 450,000 unknown threats and files are released daily, Xcitium's ability to eliminate dwell time is invaluable for security professionals who are inundated with threats and working against time to understand potential risks before they can do harm.

TENABLE APPOINTS MICHELLE VONDERHAAR TO CHIEF LEGAL OFFICER & GENERAL COUNSEL

Tenable, the
Exposure
Management
company, has
announced that it
has appointed Michelle
VonderHaar to chief legal officer and
general counsel. VonderHaar brings 30
years of domestic and international legal
experience, having held senior roles at
several large, high-growth technology
companies directing M&A, corporate
financing, governance, compliance,
litigation, global trade and other legal

VonderHaar most recently served as senior vice president, deputy general counsel and assistant secretary at HP, driving the transformation of the company's commercial global legal affairs team, expanding from a three-region model to nine geographic markets. Prior to joining HP in 2018, VonderHaar was the senior vice president, general counsel and secretary to the board of directors at Veritas Technologies. She has also previously held various legal positions in Symantec Corporation.

LOOKOUT PARTNERS WITH HPE ARUBA TO DELIVER INTEGRATED SASE ARCHITECTURE WITH ADVANCED DATA PROTECTION

Lookout, Inc., the endpoint to cloud security

company, has announced the integration of its security service edge (SSE) platform with the HPE Aruba EdgeConnect Enterprise SD-WAN platform. Lookout SSE with Aruba EdgeConnect provides customers with a best-of-breed secure access service edge (SASE) architecture that blends network security with an integrated security stack delivering secure web gateway, cloud access security broker, zero trust network access and data loss protection.

According to Gartner, "SASE is a key enabler of modern digital business transformation, including work from anywhere and the adoption of edge computing and cloud-delivered

applications. It increases visibility, agility, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and security services mainly via a cloud-delivered model. SASE can reduce the number of vendors required for secure access to one to two over the next several years." In addition, a recent Gartner survey found that 75% of organisations are pursuing security vendor consolidation in 2022, up from 29% in 2020.

"Aruba is excited to add Lookout to the Aruba EdgeConnect partner ecosystem," said Fraser Street, Aruba WAN Technical Alliances lead. "This best-of-breed integration combines Aruba's leading SD-WAN with Lookout SSE into a unified SASE architecture so that our enterprise customers can secure

matters.

their employees from the endpoint to cloud."

"As organisations seek to accelerate growth through the use of cloud services, the traditional enterprise security perimeter has evolved into a fluid, constantly moving edge. Users now interface with enterprise apps, data, and other users from wherever they may be, effectively moving the perimeter edge to their current location," said Sundaram Lakshmanan, Chief Technology Officer of SASE products, Lookout.

SECURING THE DIGITAL ECOSYSTEM

IN AN EXCLUSIVE INTERVIEW, **AHMAD HALABI**, MANAGING DIRECTOR (UAE), RESECURITY, TELLS ANITA JOSEPH ABOUT PARTICIPATION AT BLACK HAT AND WHAT MAKES THE COMPANY UNIQUE.

hat products and solutions did Resecurity showcase at the recently held Black Hat event in

Riyadh this year?

At Black Hat, we had the opportunity to showcase our Digital Risk Management Solutions that help protect entire enterprise ecosystems and monitor insider and outsider threats. One of the major solutions we have is Context CTI - a comprehensive cyber threat intelligence platform that helps law enforcement, governmental entities and financial sectors protect their critical data and identify any botnets, possible data breaches, movements, activities and malicious actors on the dark web and also reduce potential blind spots, so that they can ensure its safety.

We also showcased our EPP or the Endpoint Protection Platform-an advanced, next-generation threat detection and monitoring service to streamline and secure an organisation's cybersecurity environment. The EPP can detect Zero-Day vulnerabilities and potential malware based on signatures identified in the Dark Web which gives enterprises earlier security intelligence feeds before an attack happens. It is an extendable and highly scalable solution with its own ecosystem providing additional next gen services on top of a traditional security stack.

At the event, we also displayed our Identity Protection services comprising core cybersecurity services, including Vulnerability Assessment and Penetration Testing (VAPT) – an offensive & defensive ethical hacking to identify weaknesses and

mitigate them, malware analysis as well as investigations and threat analysis.

What differentiates Resecurity from its market rivals?

The digital economy is booming throughout the Middle East. With this rapid growth, cyberthreats have become rampant.

Resecurity is dedicated to helping more organisations throughout the Middle East secure their digital ecosystems and keep up with emerging cyberthreats with these investments.

We stand out with the quality of our data: from monitoring Threat Artifacts (IOCs, TTPs) and adversaries (communities and criminal marketplaces). We are also specialised in identifying information in the Dark Web-not just the usual information, but detailed information based on

www.tahawultech.com





historical information. Data is monitored 24/7 and constantly updated. We stay abreast of Botnets which can potentially severely compromise the critical data of organisations. We also have a dedicated Hunter Unit -a human intelligence research and development team that helps with the investigation, in addition to Artificial Intelligence.

In your opinion, what are the biggest security threats facing enterprises on a global scale? Is it still ransomware, or are there new threat actors at play?

Ransomware is still prevalent, but
Botnets are way more dangerous than
Ransomware, because the computers of
major companies can be compromised
without them being aware of it. At
Resecurity, we comprehensively monitor all
external, internal and cloud risks, and take
immediate action to destroy any malicious
actors/threats.

You've been quoted as saying your nextgen platform for enterprise end-point detection represents a 'revolution' in cybersecurity for businesses of 'all sizes'. Can you elaborate?

No matter how big or small a company/

RESECURITY IS DEDICATED TO HELPING MORE ORGANISATIONS THROUGHOUT THE MIDDLE EAST SECURE THEIR DIGITAL ECOSYSTEMS.

business size is, Resecurity can equip them with a next-generation cyber intelligence and security platform. We provide security for businesses both big or small, and ensure that their brand is well protected with us. Resecurity also continuously detects and monitors malicious actors and cyber threats, and investigate and prevent potential attacks on businesses before they happen.

How important is an event like Black Hat MEA for Resecurity to elevate and promote its mission?

Black Hat provides the perfect opportunity for us to show visitors the importance of Cyber Threat Intelligence for identifying cyber risks and threats. It also gives us a platform to generate greater awareness about the serious danger and damages that can affect brands and businesses if they don't maintain their security posture and regularly monitor their risk management capabilities.

Tell us about your market presence across the Middle East and plans for further growth in the next 12 months?

Frost & Sullivan has rated Resecurity as one of the top cyber threat and intelligence vendors. Then again, the Middle East is a key region for us, particularly in view of the growing landscape of cyberattacks. Therefore, we invest considerably in human intelligence sources across the region to deliver the best value to our clients.

In the region, we have physical presence in KSA, UAE, Jordan, Bahrain, Qatar and Oman, and have more expansion plans in the pipeline. Also, for the Middle East region in particular, we aim to hire local talent and introduce new capabilities and creativity to the local market in order for it to better adopt CTI technologies.

That's not all. We're partnering with several ISPs and MSSPs to enhance their capabilities, particularly in areas like dark web monitoring, identity protection and cyber risk monitoring.

Nuclias Connect AX3600

Access Point

< nuclias connect

HAILS THE END OF **SLOW BUSINESS**

The Wi-Fi 6-ready DAP-X2850 is on hand to unbeatable speeds, provide greatly increased capacity and interference-free coverage, paired with easy management by Nuclias Connect.



DAP-X2850







Intuitive Interface





Inexpensive Hardware Controller







THE NEW THREAT VECTOR: RANSOMCLOUD

GREGG PETERSEN. REGIONAL DIRECTOR - MEA AT COHESITY

he Middle East has quickly
embraced cloud technology,
with a huge rise in the number
of companies adopting this way
of working in just a few short
years. Supported by various government
initiatives, such as the UAE Vision 2021,
Saudi Vision 2030 and New Kuwait Vision
2035, and by the UAE's significant expansion
of its data centre infrastructure, a rapidly
growing number of businesses in the region
are adopting cloud computing tech. Saudi
Arabia, for example, has seen a 16% rise
in cloud services since 2019, with strong
growth echoed right across the region.

Many are choosing a multicloud solution, and little wonder – this flexible option offers

savvy companies a number of benefits.

Taking up a blend of services from a choice selection of public cloud, private cloud and on-promises providers gives organisations the chance to tailor the products and services they purchase to meet their particular requirements. This helps them optimise performance and better manage costs – and gives them the option to take up new services as they become available. Having more than one cloud provider can also be helpful if a provider has an outage, allowing companies to keep working despite the downtime.

However, this rise in multicloud solutions hasn't gone unnoticed by cybercriminals, who are intent on getting their hands on the growing amounts of data within the cloud. Ransomware attacks are evolving to become increasingly sophisticated and dangerous, with cybercriminals targeting the data stored in the cloud and using it for evermore nefarious purposes.

The evolution of ransomware

Ransomcloud attacks, where bad actors target the data and apps stored in the cloud and demand a ransom before they will release it, are on the rise. Generally, ransomware attacks focused on preventing businesses from accessing their data until the ransom has been paid, but it's often now about data exfiltration – actually stealing your data. And once they have their hands



on it, they can do anything they want with the information, like threatening to release it into the dark web unless a company pays the ransom.

If your company's sensitive customer data is released, there can be major problems in store, and the effects of a breach can be far-reaching. From reputational damage to customer loss and charges and fines for breaching data protection regulations, there is huge potential for significant harm to your business.

And in a multicloud environment, this potential is only magnified. The 2022 Thales Cloud Security Report found that 51% of IT professionals think it is more complex to manage privacy and data protection in the cloud and a frightening 45% had a data breach or failed an audit that involved data and apps in the cloud – up from 35% in 2021. With so much at stake, companies simply cannot afford to be casual or careless around protecting data when using multicloud technology.

Robust data management security

And how should an organisation ensure their sensitive data is robustly managed and protected against ransomcloud attacks? First, it's important to treat your cloud data the same way you would any other – storing, maintaining and backing it up in a highly secure manner. For this, it is necessary to adopt a highly sophisticated and advanced solution with a zero-trust principle at its heart. This means absolutely every person, route or node attempting to access data is strictly scrutinised and checked – and only then can they be authorised.

An added extra to the zero-trust approach is detection enabled by artificial intelligence (AI), which lowers the risk of data being stolen by spotting deviations and irregularities in the platform's backup data and therefore identifying potential attacks early on.

To further improve data security and make it harder for cybercriminals to steal the data, it's also an essential for data to be

encrypted. Backups must also be encrypted and must be able to be restored quickly if there's a breach.

A cutting-edge Software as a Service (SaaS) based data isolation and recovery system can be another vital tool in the fight against Ransomcloud. This makes it possible to connect, vault, and recover data in a cloud vault. These solutions are cleverly designed to thwart the attempts of cybercriminals by using a virtual air gap – through physical separation, and isolating network and management systems. To support business continuity, it is simple to recover the data from a data isolation platform such as this and deliver it back to the source location, or to other locations such as the public cloud.

Robust systems to reduce risks

With the exponential rise in multicloud solutions only set to rise in the UAE, it's important that companies put in place robust security systems to protect their all-important sensitive data and enable them to continue benefitting from the use of multicloud. With a zero-trust approach, detection and isolation driven by AI, and a cutting-edge data management solution, companies stand a good chance of staying ahead of ransomcloud and keeping their data secure. 2

RANSOMCLOUD ATTACKS, WHERE BAD ACTORS TARGET THE DATA AND APPS STORED IN THE CLOUD AND DEMAND A RANSOM BEFORE THEY WILL RELEASE IT, ARE ON THE RISE.

MAKING ECONOMIES FUTURE - PROOF

MEHDI PARYAVI, CHAIRMAN, IDCA, ON HOW THE GLOBAL ORGANISATION HELPS THE WORLD BUILD SUSTAINABLE DIGITAL ECONOMIES



The International Data Center
Authority (IDCA) has been
established to streamline,
structure, educate and give
direction to the Information Technology
industry. It was set up with the mission
of helping nations around the world
build sustainable digital economies.
We help them in a very diverse manner,

both in terms of education, advisory

ell us about IDCA

and mentorship, in order to build digital infrastructure that is future proof.

Tell us about the opening of your MEA Regional Office

This region is very important for us and comes with a lot of opportunities. After long and careful consideration, we've realised that we need to be locally present here due to the high demand for technology and everything related. We believe that our local

presence here will add immense value to end users, vendors and providers, so that's why we decided to be based here as well.

Who is your target customer?

We're targeting a broad range of people.
On the IT side of things, we've got experts,
consultants, manufacturers, vendors, service/
technology providers, cloud companies,
municipalities, states, nations, ministers of
education, ministers of economy, ministers



of technology-so we deal with nations, helping them build the right digital economy foundations. We also deal with institutions, corporates and governments alike, to build the right transformation plans, to be prepared for Industry 4.0.

What international experience does IDCA bring to the local market?

We come with extensive, in-depth experience because of our global exposure, the nature of our work, our interactions with international conglomerates, large corporations and government entities. I think our experience and exposure that we have internationally will bring a lot of value to this region, because there is fast-paced development here. But at the same time, we need to take a step back and make sure we make use of the experience of everyone else who has been here before us, to ensure that we take the right decisions going forward and avoid

mistakes. This region is a good example. Every construction project you see here is an example of learning from everybody else's experience and doing it better. So I think in the area of digital economy and digital infrastructure, our expertise, experience and diversity could bring exactly this.

What are the opportunities ahead for customers/end users?

Everyone will benefit. Let's look at the end users first. Very often, end users are not aware of how to host their data, where to host it, what benchmarking system to use-everybody's using a different system or mechanism. So how do they make a future-proof statement and confront the delivery claims in a mature manner? And how can the end-user understand what exactly the delivery claims are? We make it simple and easy for them to choose the best provider, so they will benefit in the best possible way.

We're very end-user based.

What are the opportunities for TELCO & Cloud providers?

Providers will get clarity about where to provide their services and which industry/ vertical to target. They will also understand the specific requirements of each industry, and how to provide customised services and categories that fit in with each of their needs. It makes their decisions easier because they will be able to understand their audience well.

Cloud providers will get a clear understanding about how to interact intelligently with their end users and how to address their various requirementsanywhere from AI and Machine Learning, to cloud computing and cloud services, all the way down to IT and physical infrastructure. All of this needs to come together in the form of an ecosystem whereby everybody will have a universal way of communicating, and bridging those gaps is what we do. We're here to create an intellectual dialogue between the facility guys, IT guys and application guys, as well as the decision makers-CIOs, CEOs, CFOs and show them the bottom line-show them what is their total cost of ownership for a specific IT decision versus another.

WE COME WITH EXTENSIVE, IN-DEPTH EXPERIENCE BECAUSE OF OUR GLOBAL EXPOSURE, THE NATURE OF OUR WORK, OUR INTERACTIONS WITH INTERNATIONAL CONGLOMERATES, LARGE CORPORATIONS AND GOVERNMENT ENTITIES.

THE 9 Cs OF **CYBERSECURITY**

TAJ EL-KHAYAT. MD - SOUTH FMFA AT VECTRA AL

rab Gulf nations' reputations for technological prowess are well deserved. From cloud to mixed reality and Al to IoT, GCC governments and businesses have been early adopters, unafraid of trying out new things. The United Arab Emirates (UAE), for example, ranks 10th out of 64 nations in the IMD's World Digital Competitiveness Index for 2021.

But GCC governments know they must protect their digital innovation communities against those who would leverage expanded attack surfaces for their own gain. This has led to regional governments leading the world in cybersecurity. Saudi Arabia was ranked third and the UAE fifth in the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) of 2021, which monitored the commitments of 194 countries throughout the previous year and gauged their maturity with regard to legal, technical and organisational issues, as well as their focus on capacity building and collaboration between stakeholders.

But even with GCI scores in the high 90s, both countries continue to experience a surge in threat actor activity that dates back to the emergence of the pandemic and the lockdowns that followed. It seems that even the most cyber-mature nations are still plagued by digital assaults. In other words, no matter how secure your digital estate, there is always room for improvement.

The 9 Cs of Cybersecurity Value

Vendors and their partners, as well as the human actors involved in the procurement, deployment, configuration, and management of security solutions must work together in this improvement story. To move security forward means to ensure that technology products and services can deliver the value envisioned when they were procured. To do this we must ask ourselves if we are devoting enough of our thinking to risk-based approaches. We must ask if our work is enhancing the efficiency of people and processes. And we must ask if we are really building more resilience against cyberattacks within our organizations.

The modern business security chain is made up of three basic types of professional — leader, builder, and user — each of whom has a specific role to play in collaborating with vendors and their partners to build better security environments. To ensure they are moving in the right direction, each of these players can check themselves against three different measures of value, for a total of nine "Cs" that can move threat postures forward.

1. Security leaders Controls

Leaders — C-level executives, including the CISO and other security chiefs such as the head of the SOC — must concentrate on which decisions will move their security

posture forward and provide visibility and controls that reduce business risk. Any solution must provide comprehensive coverage of the MITRE ATT&CK techniques and include as many MITRE D3FEND countermeasures as possible.

Compliance

Leadership teams will discover that the right security decisions will make it easier to meet customer, regulatory, and industry standards. The tightest compliance comes from being able to see as many threats as possible, and leaders should work towards this idyll.

Continuity

The leader has a responsibility to the employees and operations of the business. Continuity not only means being able to keep customer and partner data safe from prying eyes; it includes the ability to recover and move on quickly from any breach.

Security builders Coverage

The cloud and security architects and engineers who construct the digital infrastructure of the business must find ways to leverage the tools at their disposal to close the gaps in the ever-expanding attack surface. Where the complexity of modern IT stacks threatens to obscure threats from technologists, security builders must





advocate strongly for unified, high-coverage threat visibility across all attack surfaces.

Complexity

With the addition of multi-cloud and home networks to the tech mix, security builders must ensure that they have the means to consolidate and integrate existing technology, reducing costs and time to value, and guaranteeing that the complexity of any security solution is at a minimum.

Competency

Architects must be able to handle new kinds of architectures such as hybrid and multi-cloud, and the right security platform will have built-in intelligence to bridge any competency gaps that may emerge as organizations move to alien environments, thereby increasing resilience.

Security users Certainty

The analysts, threat hunters, and security team members who do daily battle on the threat landscape must have the capability to concentrate on the threats that matter most to the business. When confronted with an alert, security teams must have a high degree of certainty that it is not a false positive. This means an end to anomaly-based analysis and the adoption of more advanced threat intelligence to make accurate assessments in real time.

Context

In further advancement towards the elimination of alert fatigue, security teams must have access to more advanced alert triage and to advanced Al that is sensitive to attacker TTPs (tactics, techniques, and procedures). Providing the proper context to an alert can greatly reduce the time taken to mitigate a threat.

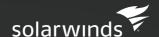
Community

Security users must share their insights with partners and peers. Experience is everything, and threat intelligence that comes from a wide array of sources has a far greater chance of adding value to a security ecosystem.

From C to C

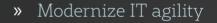
Applying the Cs is the fastest way to the next level of cybersecurity readiness. Threat actors have their methods, so we must employ our own risk-based measures to make their lives as difficult as possible. 1

TO MOVE SECURITY FORWARD MEANS TO ENSURE THAT TECHNOLOGY PRODUCTS AND SERVICES CAN DELIVER THE VALUE ENVISIONED WHEN THEY WERE PROCURED.



Today's IT agility is built on observability.

SolarWinds® Hybrid Cloud Observability helps ensure services and online applications are available, operate cost effectively, and deliver a fantastic and predictable digital experience.



» Accelerate cost savings and time to value

» Resolve issues faster with deep visibility and context

» Improve user experience and service availability

» Value across IT Ops, Dev Ops, and security



Learn more about Hybrid Cloud Observability and how we're re-envisioning the solutions you need to drive business results.

Visit solarwinds.com to learn more.

Decentralising | Decentralising | Property | Property

DR NAVEEN SINGH, CEO & CO-FOUNDER AT INERY, A REVOLUTIONARY DECENTRALISED DATABASE MANAGEMENT SOLUTION POWERED BY BLOCKCHAIN TECHNOLOGY, TELLS ANITA JOSEPH WHY IT IS IMPORTANT FOR ENTERPRISES TO HAVE A DECENTRALISED DATABASE MANAGEMENT SYSTEM AND HOW THE COMPANY SETS A NEW BENCHMARK IN THIS SPACE.

he Advent of Web5: What is it?

The term "Web5' was first coined by Tim

Berners-Lee, the father of the internet, as an open, connected, permissionless, and intelligent web platform, or simply, the Emotional Web or Symbiotic Web. It was recently revived by Jack Dorsey, Twitter's co-founder, as an extra open-source, decentralised web platform, that will be an interconnected network able to communicate with humans the way humans communicate with each other. According to Jack Dorsey, Web5 will be the amalgamation of the best features of Web2 and Web3, built on top of the Bitcoin network.

As a concept, Web5 should allow developers to utilise verifiable credentials, decentralised identifiers (DIDs), and decentralised web nodes in creating and deploying dWebs and dApps. The aim of web5, like Web3, is to hand back the ownership and control over data to the users/owners, or data self-sovereignty, from the shackles of the walled gardens of tech behemoths.

Where is Web4? And where is Web3?

Web3 was first coined by Gavin Wood, as the next iteration of the internet immediately after Web2, the current internet. This version of the internet is still in its embryonic stage, being developed by the mass as opposed to a single or few creators. Web3 is trying to solve the bottlenecks of the current internet, like data manipulation and privacy concerns, to create a decentralised, fair internet, with the users in control over their data and interactions over the internet.

Web4 is the alternative version for Web2 and Web3, rather than the next internet iteration after Web3. Also dubbed the Mobile Web, its infrastructure enables it to adapt to the mobile environment—connecting multiple mobile devices in the physical and virtual realms in real-time, regardless of location. Web4 forms a symbiotic interaction between humans and robots, making everyday life dependent on machines.



Relationship with Data Decentralisation

Web5 employs blockchain features, meaning that it will be open-source and decentralised. As the collective effort of the mass, the data will not be stored in centralised data centres, but instead spread across the network. Data over blockchains is encrypted using cryptographic functions and makes use of private and public keys, where only the owner of the private keys can access and decipher the data. Hence, the data will be secure from manipulation by big tech and security breaches.

As an advanced internet coming from Web3, Web5 has the capacity to revolutionise self-sovereignty with digital decentralised identities and data storage. It will connect more users and enhance their experience, given its robust and emotional aspect, while retaining their data and identity ownership.

Why Decentralised Data System is important for enterprises

Businesses and organisations have become data-driven, making data-intensive applications the backbone of any company that strives to succeed. The massive influx of big data has left companies with huge chunks of data that they barely use to meet their full potential. The existing systems are not mature enough to handle the rapidly changing data landscape, nor support adequate analytics for informed decision-making. This is coupled with the recent increase in security breaches in supply chains and data silos in departments that hinder innovations.

The drastically changing need for data prompts businesses to look for solutions that can meet the high demands of their consumers. However, centralised databases have proved to be costly,



puzzling, and complicated, especially when extra layers are added to an enterprise's database. In addition, the infrastructures don't give businesses the ability to conduct query searches on vast amounts of data.

A decentralised data system will break enterprise data out of data silos, enabling the seamless sharing of information that is consistent and reliable for decision-making. Hence, it greatly promotes innovation and the progress of modern business.

Consequently, inheriting blockchain properties like decentralisation, tamper resistance, owner-controlled assets, low network latency, and search query capabilities, mature infrastructures like IneryDB ensure unrivaled data security, speed, performance, and privacy. For instance, Inery converts enterprise data into cryptographic texts and store it on blockchain to reduce the data weight and increase its security, thus, mitigating high cost. Its interoperability

WEB5 EMPLOYS
BLOCKCHAIN
FEATURES, MEANING
THAT IT WILL BE
OPEN-SOURCE AND
DECENTRALISED.

feature allows business departments or systems to communicate and share data at high speeds without compromising data security, ensuring businesses exceed innovation with decentralised characteristics.

Decentralised Data vs Centralised Data

A centralized database collects, stores, and manages data from a central location or data centre. The data is often controlled by a single organisation or a few entities, who have absolute power over the functionality of the database. This exposes the data to a myriad of risks. These are:

- High latency: Since data is accessed from a single location, the system attracts high data traffic, which creates bottlenecks and makes the data inaccessible or lagged.
- Siloed ecosystems: Centralising data creates data silos, making the data unavailable to some departments in

EXISTING DATABASE MANAGEMENT SYSTEMS ARE NOT MATURE ENOUGH TO HANDLE THE RAPIDLY CHANGING DATA LANDSCAPE, NOR SUPPORT ADEQUATE ANALYTICS FOR INFORMED DECISION-MAKING.



- a company. This hinders innovation due to slowed decision-making due to data inconsistencies.
- Single Point of Failure: If a single server fails, the data in the entire data in the data centre is affected or becomes vulnerable.
- Privacy concerns: It is not uncommon for centralised data systems to share user data with advertisers or other big tech companies for their own gain. This compromises the user privacy policies.
- Security concerns: Their immature infrastructure makes them vulnerable to security breaches and data thefts.

 Breaking into a single server, for instance, gives the malicious actor access to the entire supply chain data.

In essence, centralised data systems are vulnerable, mainly due to the features that give them advantages in a sense; single location and centralised control.

Conversely, decentralised data lacks

BY DECENTRALISING DATA, INERY ENSURES THAT DATA IN AN ORGANISATION IS AVAILABLE TO ALL THE DEPARTMENTS, UP-TO-DATE.

the aspect of a single authority or central owner. The data in a decentralised network is distributed across multiple nodes/servers within the network. Every time data is added to the network, it is replicated on the existing nodes to ensure consistency. The changes or updates made to the data are added to the data history on the blockchain to ensure traceability. Generally, decentralising data solves the shortcomings of centralised databases. It ensures:

- Decentralisation: Data in a decentralised framework is spread across multiple nodes that belong to several users. This eliminates the risk of a single point of failure. Thus, when a single node is compromised, enterprises can still access their data from other nodes.
- Security: A decentralised database encrypts the data using cryptographic hashes, such that only the user with the correct private keys can access the information.
- Tamper resistance: Once data is stored on a blockchain, it becomes immutable or tamper-proof. This means that it cannot be modified, deleted, or updated. It makes the data resilient to changes by maintaining the data history to provide the information with more integrity and accountability.
- Scalability: Unlike centralised



DECENTRALISING DATA SOLVES THE SHORTCOMINGS OF CENTRALISED DATABASES.

databases that offer finite server resources, decentralising data ensures that data can be accessed simultaneously without compromising performance even as the number of users increases. Thus, a business can easily scale as its consumer base continues to grow without having to compromise service quality.

- Data accessibility: Enterprises can easily access data at any time from the nearest node, and leverage it as they wish without third-party controlling functionalities.
- Low network latency: Since the data is spread across multiple nodes, data traffic is not restricted to a single location, resulting in low latency and high speeds.

How Inery creates a new paradigm for Decentralised Data Management

Inery is a proprietary layer-1 blockchain and decentralised data solution. Inery integrates blockchain's decentralisation, immutability, and security features with distributed database management properties to enable next-gen innovation for data management. It aims to bring self-sovereignty back to the users using owner-controlled data assets and distributed databases.

The network's high-throughput capacity, unparalleled security, interoperability, and scalability, enable Inery to fuel the rise of a different economy, connect the disintegrated world, influence a new age of ownership, and introduce an agenda for the healthcare sector's future, among others.

Inery addressing privacy and data manipulation concerns

Data privacy and manipulation concerns stem from the power vested in a single or

central authority to manage and dictate how data is handled. Inery strips the entities of this power by enabling ownercontrolled data assets. It allows businesses to implement value contracts that give only the value contract owner(s) access to the database. The smart value contracts allow the owners to predetermine access to the database, that is, the actions that can be done on the data, who can access it, how it can be accessed, etc. Inery also enables custom permissions to users for data additions that have also been predetermined in the value contracts, managed through authorisation by private key holders who push actions in the value contracts.

The data spread across multiple nodes within the Inery network is encrypted using cryptographic functions to ensure that only the user with the correct private keys can access the data. This makes it impossible for tech monopolies to access and exploit user data for their own gains. To use, or even access, the data, third parties will have to ask for permission from the user or enterprise, who dictates all the actions and compensation for the data usage.

Inery also provides users with a rich set of complex queries for document retrieval, query searches, and CRUD (create, read, update, and delete) functionality, to perform actions on their database. It allows them the flexibility to implement database usage.

Inery's Interoperability and Scalability capacity

The importance of data cannot be stressed enough. It is the currency that fuels organisational growth that, when used appropriately, can help businesses and institutions scale or achieve their full potential. Inery understands the importance of data sharing and communication between departments



and the impact data silos have on the growth of a business or organisation.

By decentralising the data, Inery ensures that the data in an organisation is available to all the departments and up-to-date. Consistent data, achieved by replication of the same data to the involved nodes, is accessible to all the authorised departments for informed decision-making. Sharing data across the departments is fast, reliable, and secure, enabling the enterprise to communicate with shareholders without compromising the data quality.

The core of IneryDB, the decentralised data system, is enabling data portability through various verticals, while providing users with intuitive and simple interactions with the system. It also provides developers with the tools to create and deploy applications. In a nutshell, Inery offers users, including governments, financial institutions, businesses, real estate, the gaming

INERY'S POTENTIAL TO REVOLUTIONISE DATA MANAGEMENT HAS GARNERED ATTENTION FROM BOTH WEB2 AND WEB3 SPACES.

industry, etc., the capability to manage their own data. For instance, gamers can create, mint, own, and share NFTs in games, while the healthcare sector can handle its data, track drugs, verify the authenticity of medical products, and communicate with other healthcare verticals, among others.

What's next for Inery?

Inery's potential to revolutionise data management has garnered attention from both Web2 and Web3 spaces. Web2, Web3, or Web5, Inery plans to provide the foundation for a completely decentralised internet through its decentralised data management solution, IneryDB. Recently, Inery rolled out its first public testnet in preparation for its mainnet launch which is scheduled for Q1 2023.

INERY INTEGRATES BLOCKCHAIN'S DECENTRALISATION, IMMUTABILITY, AND → SECURITY FEATURES WITH DISTRIBUTED DATABASE MANAGEMENT PROPERTIES.

DELINEA APPOINTS TIMOTHY PUCCIO AS SENIOR VP OF GLOBAL CHANNELS & ALLIANCES

elinea, a leading provider of Privileged Access
Management (PAM) solutions for seamless security, has announced the appointment of Timothy Puccio as Senior Vice President of Global Channels and Alliances. Puccio assumes leadership of Delinea's world-class global partner ecosystem, consisting of value-added resellers, global systems integrators, strategic alliances, and technical partners.

"Partners turn to Delinea to provide cloud-ready and easy-to-use PAM solutions that help secure their customers' digital transformations. I'm excited to develop and lead the next phase of our channel strategy and partner program," said Puccio. "The demand for industry-recognised PAM continues to grow at a rapidly accelerating pace to keep up with modern cyber threats, and I'm looking forward to working with our ever-growing partner network to secure our customers with seamless security."

Puccio brings over 25 years of channel and sales experience in the software industry. Most recently, he served as Senior Vice President of Global Sales for Login VSI where he

> PUCCIO BRINGS OVER 25 YEARS OF CHANNEL & SALES EXPERIENCE IN THE SOFTWARE INDUSTRY.



built the company's global go-to-market team. Puccio was previously Channel Chief and Vice President of Global Channels and Alliances at Fuze, where he successfully led the channel sales strategy, driving broader adoption of the Fuze platform across the globe. Puccio's past endeavors include leadership positions at Carbonite and HP Software.

"Tim brings a wealth of direct experience and a successful track record to grow, enable, and lead our global partner program," said Rick Hanson, President at Delinea. "Delinea is committed to building a partner-focused organisation, and under Tim's leadership I know that we will surpass the expectations of both our partners and our customers."



DISPLAY & CONTROL SOLUTIONS WITH PRESENTATION MATRIX & SCALER













Hikvision is the world's leading IoT provider with video as its core competency, commercial display business also being its key focus area. Malco Technologies is an official Hikvision Displays distributor in the UAE, offering LED/LCD Video Walls, digital signage and 3D/transparent screens to suit every Boardroom, Media advertising, NOC/SOC control room requirements. By pairing with Kramer's Matrix switchers, VIA Connect PRO Wireless Collaboration Solution and Video Wall Controller etc. the applications are unlimited.









REDEFINING COMMERCIAL DISPLAY

ANITA JOSEPH CAUGHT UP WITH **SACHIN SRINIVASAN**, COMMERCIAL DISPLAY DIRECTOR AT HIKVISION MENA, TO KNOW MORE ABOUT THE COMMERCIAL DISPLAY MARKET IN THE REGION AND HOW HIKVISION CONTINUES TO LEAD THE WAY IN THIS SEGMENT.



ell us about the commercial display products you showcased at GITEX 2022
Hikvision is no longer only a security company, our business scope has become much broader. Hikvision is an IoT solution company with video as its core competency. Hikvision has been in commercial display solutions since 2008. Hikvision has introduced commercial display solutions in the MENA region from 2019.

I can confidently say that we have the A to Z solutions in commercial display: we have indoor LED solutions, outdoor LED solutions, LED module solutions, creativity solutions which includes the LED poster, the all-in-one LED, the 3D LED solutions and the transparent LED solutions. And we are also into the LCD video wall solutions. We also have the interactive display solutions for education and for meeting rooms. We are also into digital signage solutions where we offer screens with a built-in media player right from 22 inches all the way up to an 86-inch screen.

Can you tell us more about what benefits these products provide?

There's a huge market for commercial display in the MENA region and the verticals that we cater to-right from the retail vertical, the hospitality vertical and the government vertical. In fact, the retail vertical is one of the biggest verticals in commercial display. LED, in particular, has a huge demand in the MENA region.

We also have LCD video wall solutions. These are basically for control rooms, while the digital signage solutions are for retail. They are also used in the lobby areas of hotels, corporate and government verticals. Interactive displays are actually used in meeting rooms. Post the pandemic, cloud conferencing gained considerable traction. That's primarily why people began looking at meeting room interactive displays with a built-in camera and microphone.

We also have the education interactive displays. Education interactive displays are in great demand, especially from schools, colleges and universities. We have tied up



with education content providers, and we sell these interactive displays to leading schools and universities.

What differentiates Hikvision from other providers of commercial displays?

We not only provide the display, we also provide LED controllers along with our LEDs. In addition, we provide video wall controllers as well as the encoders and decoders. We've also launched some flagship products for our outdoor LEDs, with higher brightness, a very slim profile and very low power consumption which is the need of the market.

The brightness of an outdoor LED product depreciates by 8% every year. So if you buy a product that has a brightness of 6000 nits, in five years, its brightness will come down to 3000 nits. This means that it will not function properly during the day, which in turn, means that its functionality is reduced considerably. Therefore, we've come up with a product that has 10,000 nits

THERE'S A HUGE MARKET FOR COMMERCIAL DISPLAY IN THE MENA REGION. of brightness but can be kept at 6000 nits of brightness so that you get a uniform brightness for the next five years. Again, its power consumption is half that of the competitors in the market.

This saves a lot of money.

Even in our indoor LED products series, we've introduced a new series of Flip Chip COB LEDs. Flip Chips will take over the LED industry and probably in the near future, they might even replace the LCD industry completely. At the moment, the cost of production of the COB LED is very high, but in course of time, the pricing will come down as demand decreases.

We make COB LEDs from 0.4 mm pixel pitch, to 0.7mm, 0.9mm and 1.2 mm.

How important an event is GITEX for Hikvision?

GITEX is an important platform to showcase our solutions since it caters to the entire MENA region. People visit this event from all over the world and so it provides plenty of opportunities to showcase our cutting-edge products and solutions. Hikvision already enjoys a solid name in the security industry, and we would like to strengthen our reputation in commercial display. So this year at GITEX we showcased our 3D LED solutions, our transparent LED solutions, interactive display solutions and our COB LED solutions.

CYBERSECURITY WITH A DIFFERENCE

HELMUT REISINGER, WHO TOOK OVER AS BOARD MEMBER & CEO OF EMEA & LATAM AT PALO ALTO EARLIER THIS YEAR, TELLS ANITA JOSEPH THAT THE MIDDLE EAST REGION IS PARTICULARLY VULNERABLE TO CYBER-ATTACKS AND MUST BE VIGILANT.



alo Alto's presence at GITEX 2022.

For Palo Alto, GITEX is an important meeting place of the business and digital ecosystem. This year, specifically, seems to be busy and crowded, particularly now that the pandemic is almost behind us. What we are showcasing here is the unique platform approach that Palo Alto brings to the cybersecurity industry for our customers.

The background

The cybersecurity industry is highly fragmented and has multiple players. In fact, for every new problem that a hacker creates, a new company is created.

The hacker landscape has become an industry, with attackers who are up against



companies that are trying to protect. Today, cybersecurity is massive and more important than ever because of the rapid digitisation of companies. Data is also increasing massively. And, of course, the global economy has never been so connected.

This trend is significant for the Middle East, which has to strengthen and consolidate its critical infrastructure, taking cues from the recent attacks on the German rail network. In fact, data shows that the nation state attacks have increased over 100% in the past two years, which manifests itself in cyber battlefields such as the Russia-Ukraine conflict.

How Palo Alto steps in

Palo Alto Networks, the number one

OUR MISSION IS TO BE THE CYBERSECURITY PARTNER OF CHOICE, PROTECTING OUR DIGITAL WAY OF LIFE.

cybersecurity global firm with a 3.5 per cent market share, is shaping the cloud-centric future with technology that is transforming the way people and organisations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial

intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organisations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

Every day, Palo Alto Networks provides the visibility, trusted intelligence, automation and flexibility that helps complex organisations advance securely. By delivering a comprehensive portfolio and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organisations across clouds, networks, and mobile devices.



SOCIAL ENGINEERING: THE SILENT VECTOR

LAYALE HACHEM. SENIOR SOLUTIONS ENGINEER - BEYONDTRUST

o you know anyone who has clicked an unknown link in an email? Or inadvertently given an unauthorised party access to an MFA (multi-factor authentication) asset? Or otherwise divulged their credentials and compromised their digital security? Study after study suggests that you either know someone who has done one of these things or you have done one of them yourself. And even if you are a CISO, some of the most sophisticated cons can fool you too.

Welcome to Social Engineering 101. It fools more people than you might think, and it is on the rise. According to one report, in the United Arab Emirates (UAE), social engineering incidents went through a whopping 230% surge from the first to the second quarter of this year. And just one vendor recorded almost 3.5 million phishing attacks.

Social engineering does not, in itself, inflict damage. Rather, it is a means to make infiltration easier for attackers.

Verizon's 2022 Data Breach Investigations Report (DBIR) puts social engineering or the "human element" as the root cause of 82% of the breaches it examined. Clearly, security professionals have a mountain to climb. So where do they start?

It's been emotional

First, it is no secret that we humans are engines of emotion. It takes a lot of training and experience to short-circuit a social engineer's appeals to our curiosity, fear, and anger. Timely content that exploits a widespread feeling is a potent weapon. That is why the initial months of COVID saw massive spikes in cyberattacks around the world. But that is not the only trigger used by social attackers. They also, ironically, use trust — trust based on authority.

Even if it looks like your bank is warning you about something terrifying, like the closure of an account, caution is advised. Most banks and other businesses that rely on trust are open about the fact that they will never ask a customer to divulge sensitive information by phone or email.

It is therefore prudent to reach out to the authority in question if they appear to be contradicting that pledge.

Social engineering lies at the periphery of the average user's cyber knowledge, and those who are aware of it and how it works may think they are not significant enough to be targeted. They may not know that attackers just need a single inroad to begin lateral movement. And they may be unaware that phones, texts, and even snail mail are attack vectors.

Knowledge is power

So, the top advice to any enterprise is to educate users — all users. Train them to verify communications as legitimate by showing them how to identify the source. The email address should have the correct domain and the message should be addressed with the right name or job title (where relevant), and it should be relatively free of grammar and spelling mistakes and out-of-place or foreign characters.

Make sure employees are aware of their value to a threat actor and that no attacker will view them as the final step of infiltration. Explain, in general terms, what lateral movement means and impress upon employees the importance of vigilance. Give them an idea of the number of highprofile attacks that began with a misstep of someone at middle management or below. Follow this up with the reminder that even the simplest of personal information can be the first link in a chain of misfortune. Coach them to be conscious of their emotions and to treat an elevation in curiosity, fear, or anger as a possible indicator of an attempt at social engineering. Cold, calculated process is the preferred alternative to



impetuous reaction in an unguarded moment.

A few pointers for users can make the difference. Training sessions can teach them how to check hyperlinks' URLs for suspect endings such as ".ru." or "+" characters signs as a stand-in for a lowercase "t".

Let's get technical

IT, too, can play its part. All OSes and apps should be up to date with the latest security patches, and antivirus software should be properly licensed, appropriately patched, and performing full scans at regular intervals. Spam filters and firewalls can stop some nefarious emails before they hit inboxes.

On top of this, IT and security leaders should implement the principle of least privilege and perform regular audits of credentials to ensure that only those that need access to a resource are granted it. IT

administrators should only log on as such when performing tasks that go with the role. It is good practice to remove local admin rights for basic user accounts and restrict those users who do require privileges, such as network administrators, from accessing the Internet or checking email while logged on with their high-level privileges.

Another best practice is to rip and replace any software asset (especially an OS) that no longer receives patches or is about to go out of support. EOL systems are attractive vectors for threat actors and in the event that they cannot be replaced, they should not be used to connect to the Internet or receive email. IT and security teams can also perform penetration tests. While tests on infrastructure are always advised, when it comes to employees, pen tests should include social-engineering tactics to see if the training has stuck and to identify employees who may need further sessions.

SOCIAL ENGINEERING LIES AT THE PERIPHERY OF THE AVERAGE USER'S CYBER KNOWLEDGE, AND THOSE WHO ARE AWARE OF IT AND HOW IT WORKS, MAY THINK THEY ARE NOT SIGNIFICANT ENOUGH TO BE TARGETED.

Tale as old as time...

The art of the con predates the Internet, the computer, and even the abacus. But just as ancient is the human capacity for beating the con artist at their own game. Be vigilant, train potential victims, and tighten up defenses and social engineers will be left frustrated.

COMBINING PERFORMANCE WITH SECURITY

RICHARD PIASENTIN, CHIEF STRATEGY & CHIEF MARKETING OFFICER AT ACCEDIAN, TELLS ANITA
JOSEPH HOW THE COMPANY IS ON A MISSION TO MAKE TECHNOLOGIES THAT CONNECT PEOPLE AND
SYSTEMS AS TRANSPARENT AND FEFFCTIVE AS POSSIBLE.

Accedian for its growth and expansion in emerging markets.

We prefer to refer to emerging markets as dynamic markets; the main focus of our corporate strategy here is to enable our customers to move as rapidly as needed towards the adoption of new technologies, which, in the end, is not for technology's sake, but to enable innovation.

ell us about the corporate strategy adopted by

A major focus for Accedian is the convergence of performance and security – essentially a united platform for both performance management and cybersecurity threat detection. With this in mind, we launched Skylight Interceptor earlier this year, which is a highly innovative network detection and response solution. It helps customers protect their networks by delivering prioritised, context-rich incidents that speed detection and response to security threats. Skylight Interceptor also allows organisations to identify complex and sophisticated Zero-Day threats that are often missed by traditional perimeter security solutions. You've already got performance covered from Accedian Skylight, we're now combining performance and security into a single solution. This of course brings about a variety of savings – time to issue resolution, resources, costs, I could go on.

Also, specific to the region, we have launched partnerships with some very specialised Value-Added distributors, VADs and VARs, who provide IT services across the market. One of the unique features of our solution is that we are a cloud-based SaaS offering, and we can be implemented inside of a customer cloud as well. Combining that with our ability to offer both performance and cybersecurity threat detection on that same platform, for the VAD and VAR industries it creates a huge opportunity for rapid service adoption and service expansion capabilities.

Digital transformation is accelerating at breakneck speed now, particularly post the pandemic, in the region. What, in your opinion, are some of the challenges faced in this journey?

The end goal for enterprises undergoing digital transformation is to essentially achieve a state where network infrastructure just disappears, and digital tools and support structure just works, seamlessly and with consistent reliability.

To achieve this, a lot of really smart people usually have to assemble a new and specific set of technologies and implement new business practices or workflows for any number of business processes or tools. But, most importantly, this team would have to make sure that all of this performs consistently the way it's





supposed to. It's easy to put all the blocks together, but if one block doesn't work, the entire process falls apart. Therefore, the implementation and performance aspects in this architecture are absolutely critical.

From an organisational perspective, it's important to understand that during digital transformation, IT teams cannot afford to think about performance AFTER they deploy a solution, they have to think about it as they're developing or creating their new stack and processes. Even before the deployment of their transformation begins.

In addition, it's not sufficient in our modern business world to implement a set of technologies without implementing a security strategy simultaneously. In fact, we believe that in the next ten years, no IT product will be released without rock solid hooks into the security paradigm. Any provider that hasn't adopted security as part of their technology portfolio will not survive.

Innovation is at the core of business continuity and growth. How is Accedian helping businesses with this?

Accedian has a solid reputation for innovation, and we are absolutely focused on performance

quality and network security capabilities. For 17 years now we have single-mindedly pursued our goal to provide our customers with a real-time view into everything happening on their network – from a microsecond granularity to a macro, or holistic, view of their network and service performance. We know that we have our customers' trust that we are the best at what we do here. And because of that heritage, providing insight into cyber threats and breaches was a natural next step.

Our purpose as a company is to provide the best possible performance and security solutions with the best possible people backing them, so that we can effectively make the technologies that connect people and systems as transparent and effective as possible.

We don't consider it our job to help our customers innovate, we know that they have the edge and expertise to innovate in their respective fields – but we do believe that it's our job to make sure nothing STOPS them from innovating. That's the role we play.

The need for an effective cyber resilience strategy is more important than ever. How does Accedian help?

One of the challenges of the security industry

is that the market is very crowded. There's a lot of noise, a lot of overlapping solutions. Therefore, IT professionals are faced with hundreds of choices that make it difficult to select exactly what she or he needs. They are also faced with constant threats, increasingly sophistication of those threats, and usually, the ask to do more with less resources and potentially less know-how on their teams.

Organisations today are also faced with another reality – it's not a matter of if, but when, they will be breached. In fact, according to the IBM 2022 Cost of a Data Breach Report, 83% of business surveyed at least one data breach. That's a staggering number.

Cyber resilience is about managing that reality. How quickly can an organisation detect, respond to, and recover from a breach. We can see everything on the wire, at the highest level of resolution and in real-time, with prioritised alerts, context and incident correlation. No more long periods of dwell time driving up compliance costs, ransom, and additional havoc wrecked by cyber attackers.

And adding to that, with our unified platform for performance and security, adding in performance monitoring capabilities to network detection and response (NDR) is literally like flipping a switch. We aim for our real-time, highest granularity data insight to unite teams to optimise user experience and strengthen cyber resilience in their organisations, so they can focus on innovation and driving business success.

WE AIM FOR OUR REAL-TIME, HIGHEST GRANULARITY DATA INSIGHT TO UNITE TEAMS TO OPTIMISE USER EXPERIENCE AND STRENGTHEN CYBER RESILIENCE IN THEIR ORGANISATIONS.







an you tell our readers about some of the solutions and partnerships you showcased at GITEX this year?

We are the leading supplier of IT Security and ICT (information, communications, and technology) products, providing technological advancements for more than 20 vendors and collaborating with more than 500 partners to bring the best security solutions (cloud security, email security management and security training) to the Middle East.

The value-added distributor delivers the appropriate solutions to end customers by collaborating with a large network of resellers and system integrators. We offer information security solutions that include network security, cloud security, OT/IoT security, robotic process automation (RPA), and other specialized solutions for cyber security.

In the last 12 months, how has your company performed in the MENA market? Has your company ventured into any new markets/countries?

During the pandemic the market was guite slow, but in the last month activities have really picked up and we have been very active in the GCC. Through our network of partners, we provide value-added services around-the-clock in the Middle East and Indian subcontinent and we have also expanded our business to Saudi Arabia, where we have opened an office recently.

What technologies and IT trends are the forefront of driving innovation for your business?

but after the pandemic, they had to add security into that.

If we look at the whole situation, most of companies went for remote secure access, digitalisation and cloud adoption in the past,

WE ONLY SIGN UP WITH VENDORS AFTER AN EXTENSIVE EVALUATION AND WE PROVIDE SECURITY SOLUTIONS NEEDED FOR DIFFERENT INDUSTRY VERTICALS AND TYPES OF **CUSTOMERS.**

We have training labs providing high end solution training and partner enablement, a dedicated & active 500+ reseller network in the region, a diverse customer experience giving us an edge to understand different industry verticals & their requirements and a strong technical knowledge base & back-end support

We also have excellent recognition with all leading vendors as we promote and market their product and provide local support.

Can you tell our readers what differentiates your company from your market rivals?

We only sign up with vendors after an extensive evaluation and we provide the security solutions needed for different industry verticals and types of customers.

We specialise in high-end enterprise security solutions and deploy them via influential system integrators in the area. We also have a strong track record of providing world-class products and firstrate customer support. Our broad product line has everything a business needs to secure its data. 🙎

www.tahawultech.com NOVEMBER 2022



MANAGING VULNERABILITIES

MAHER JADALLAH, SENIOR DIRECTOR MIDDLE EAST & NORTH AFRICA AT TENABLE, TELLS ANITA JOSEPH WHY VULNERABILITY MANAGEMENT IS VITAL FOR MODERN-DAY SECURITY.

ulnerability Management has become even more crucial today than ever before. Tell us about the evolution of the whole concept of vulnerability

management

In cybersecurity, we recognise that all modern software contains vulnerabilities that require patches to fix the flaws. But that's only part of the story. Security teams also have to consider misconfigurations that

require human intervention to find and fix. We believe these two areas are fundamental for effective vulnerability management. However, securing the modern attack surface needs to go beyond vulnerability management to allow security teams to also fully understand all of the conditions that matter within today's complex and dynamic environments.

Organisations need the ability to see their entire attack surface holistically.

They need to see all of their software vulnerabilities, misconfigurations, who is using what systems and what level of access they have all correlated together, regardless of whether it's happening on a laptop, a container, an application or a programmable logic controller (PLC).

Exposure management goes beyond vulnerability management to give cybersecurity leaders a way to reclaim the narrative from the reactive, headline-





grabbing breaches and attacks. It brings together technologies such as vulnerability management, Web application security, cloud security, identity security, attack path analysis and external attack surface management to help organisations understand the full breadth and depth of its exposures and take the actions needed to reduce them through remediation and incident response workflows.

IT adoption has evolved significantly since the pandemic. So how do you think organisations should rethink their security practices?

When a threat actor evaluates a company's attack surface, they're probing for the right combination of vulnerabilities, misconfigurations and identity privileges that will give them the greatest level of access the fastest.

However, in stark contrast, the security industry as a whole has focused on creating point solutions tailored to address very specific aspects of cybersecurity - vulnerability management, Web application security, cloud security, identity security, and so on. This hodgepodge of technologies,

ONE OF THE MOST COMMON BUT DANGEROUS SECURITY LAPSES IS TO MISCONFIGURE SOMETHING IN THE CLOUD AND MAKE IT INTERNET-FACING.

that all serve a bespoke function, don't allow organisations to see the full scope of their cyber risk. This creates blindspots that threat actors exploit. This has to change.

Modern, proactive cybersecurity requires the ability to: continuously assess the attack surface; understand the interconnectedness of users, assets and systems; and take steps to address vulnerabilities, fix misconfigurations and harden user identities and access privileges long before they're on the radar of an attacker.

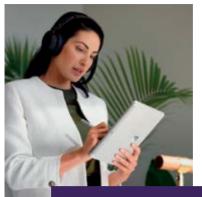
With remote work gaining traction, how do you think one can ensure the safety of all the cloud devices?

One of the most common but dangerous security lapses is to misconfigure something in the cloud and make it Internet-facing. Organisations need to understand that whatever is visible on the internet is likely to be the first point threat

actors will target. They'll look for known but unpatched flaws to leverage and gain entry and from there escalate their access status to dig deeper and compromise further systems. However, with new vulnerabilities being identified every day, the task of remediating everything is not just challenging, but arguably impossible.

Instead, organisations need to understand what systems and data are critical for the business to function. In tandem they need to identify the potential attack paths that exist from external systems to critical assets. The combination of this information illustrates the 'blast radius' from threat actor compromise, allowing security teams to focus efforts on the most damaging risks first. This ensures the vast majority of attack paths are closed off preventing compromise, malware infiltration, and/or exfiltration of data.









Build a secure, productive hybrid workplace

Choose devices that optimize hybrid work

Your teams require different tools to be successful:



Many prefer flexible 2in-1 devices,

while some love their laptops.



Everyone wants accessories that work

seamlessly and make work easier.



Simplify security with zerotouch deployment and

password-free login.

Set your employees up for success

with devices and accessories that enhance productivity, collaboration, and security.

Tel: +973 17700777 | acsales@almoayyedcomputers.com | www.acme.tech

in Almoayyed Computers Middle East (ACME) 📵 almoayyedcomputers

Almoayyed Computers

NEXT-LEVEL CYBERSECURITY

RIK SCHOONIS, TERRITORY CHANNEL MANAGER AT HEIMDAL SECURITY TELLS TAHAWULTECH.COM ABOUT THE COMPANY'S UNIQUE SECURITY POSITIONING IN THE GLOBAL MARKET





ell us about Heimdal Security
and its participation at GITEX.
Heimdal is the representation
of a future approach
to security. We are a
Europe-based security vendor based in
Copenhagen, Denmark, and we have a high

Copenhagen, Denmark, and we have a high adoption rate throughout the world. We combine threat prevention, vulnerability management, access management, and antivirus and e-mail security into a single platform that simplifies IT operations and helps companies stop any cyberattack, keeping critical assets, information and intellectual property safe.

As for GITEX, it felt great to be back on ground after two years of restrictions and online meetings. The event provided a great platform for us to showcase our products and solutions and network with innovative minds in the industry.

Tell us about Heimdal's Threat Prevention capabilities.

Heimdal Threat Prevention scans users'



traffic in real time, blocking infected domains and preventing communication to cybercriminal infrastructures with minimal system footprint. Heimdal Threat Prevention is compatible with any Antivirus or Firewall and can be combined with more Heimdal products to deliver an authentic Endpoint Prevention, Detection and Response solution, in one agent and one platform. What's more, it can be deployed in your environment in less than an hour. Its cloud-native Threat Intelligence safeguards your most precious assets against any type of threat, from human error to full-fledged malware campaigns.

WE BELIEVE THAT CYBERSECURITY CAN BE COMPLICATED ENOUGH AS IT IS, WHICH IS WHY WE BELIEVE OUR CLIENTS SHOULD GET THE BEST TECHNOLOGIES WITHOUT NEEDING TO SACRIFICE TOO MANY MAN-HOURS IN ORDER TO MAKE IT ALL WORK.

What is the company's USP in a market that is crowded and extremely competitive?

We believe that cybersecurity can be complicated enough as it is, which is why we believe our clients should get the best

EVERY SINGLE CYBERSECURITY SOLUTION IN THE HEIMDAL SUITE IS DESIGNED TO SEAMLESSLY

COMMUNICATE WITH EACH OTHER, AS WELL AS INTEGRATE WITH OTHER SECURITY PRODUCTS BEING USED.

technologies without needing to sacrifice too many man-hours in order to make it all work. Every single cybersecurity solution in the Heimdal suite is designed to seamlessly communicate with each other, as well as integrate with other security products you're using. This is how we manage to achieve what we hold as the golden standard in cybersecurity today – unification. All our solutions operate under one convenient roof known as the Heimdal Unified Dashboard, where you get access to all the data you need and have incisive reporting features at your fingertips. \$\mathbb{1}\$

SECURING WORKSPACES

LARA YOUSUF, CHANNEL ACCOUNT MANAGER AT MIMECAST, TELLS VERONICA MARTIN ABOUT GITEX 2022 AND THE COMPANY'S PLANS FOR THE REGION.



hat is the Mimecast key message at GITEX 2022?

GITEX is a forum for

us to showcase our latest technologies, what our customers have brought in terms of developments in the cybersecurity world. It's a chance for us to connect with our partners, with our customers and probably meet new prospects, as well as peers in different cybersecurity organisations. Our main message is how we can help organisations

In the last 12 months, how has your company performed in the MENA market?

Working in cybersecurity you can see

to build a more secure site.

the threat landscape is increasing and email remains the number one attack vector. In the UAE 94% of organisations have been a victim of an email born through attack. Similarly, in KSA, around 90% of organisations have faced similar challenges. In more than 40% of cases this attack is individual. The attack vector and the surface have increased and more so with organisations moving into a hybrid work environment and relying more and more on the digital communications and collaboration tools, which puts organisations in a riskier atmosphere, where they need to make sure that their data, people and communications are secure. Now is the perfect time to enable organisations to be protected in the modern workspace.

WORKING IN CYBERSECURITY, YOU CAN SEE THE THREAT LANDSCAPE IS INCREASING; EMAIL REMAINS THE NUMBER ONE ATTACK VECTOR.

What trends are driving innovation in your business?

It would definitely be ML and AI, as our new platform Mimecast x1 relies specifically on them and it basically leverages the data and allows organisations to learn more about how employees work, as well as educating them on how to be more protected in their workspace, whether they are working from the office or remotely.

What do you think it makes you different from your competitors?

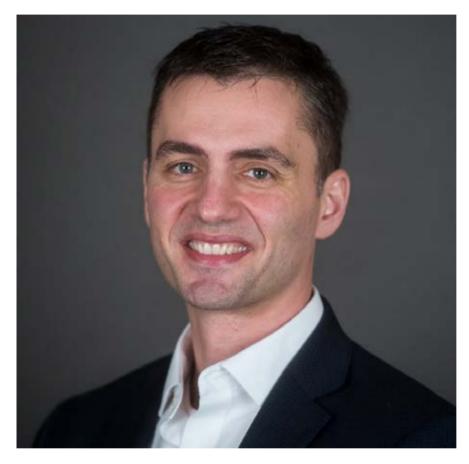
Our key differentiator is the way we approach cybersecurity organisations and our service capability detection. Enterprises need to adopt a more layered security approach when it comes to cyber security. Not only protecting your email, but also your web, domain and making sure that cloud security and email security are working hand in hand, so that you have a more solid security. 1

ORGANISATIONS INCREASING MODERN DATA PROTECTION FOR CLOUD WORKLOADS TO REDUCE SECURITY RISKS

eeam Software, the leader in Modern Data Protection, has released the findings of the company's Cloud Protection Trends Report 2023, covering four key "as a Service" scenarios: Infrastructure as a Service (laaS) Platform as a Service (PaaS). Software as a Service (SaaS), and Backup and Disaster Recovery as a Service (BaaS/DRaaS). The survey found that companies are recognising the increasing need to protect their SaaS environments. For example, nearly 90% of Microsoft® 365 customers surveyed use supplemental measures rather than relying solely on built-in recovery capabilities. Preparing for a rapid recovery from cyber and ransomware attacks was the top cited reason for this backup, with regulatory compliance the next most popular business driver.

Highlights of the report:

- While new IT workloads are launching in the cloud at far faster rates than old workloads are being decommissioned in the data center, a surprising 88% brought workloads from the cloud back to their data center for one or more reasons, including development, cost/performance optimisation and disaster recovery.
- With cybersecurity (including ransomware) continuing to be a critical concern, data protection strategies have evolved, and most organisations are delegating backup responsibilities to specialists, instead of requiring each workload (laaS, SaaS, PaaS) owner to protect their own data. The majority of backups of cloud workloads are now being done by the backup team and no longer require the specialised expertise or added burden of cloud administrators.
- Today, 98% of organisations utilise a cloud-hosted infrastructure as part of



their data protection strategy. DRaaS is perceived as surpassing the tactical benefits of BaaS by providing expertise around Business Continuity and Disaster Recovery (BCDR) planning, implementation and testing. Expertise is recognised as a primary differentiator by subscribers choosing their BaaS/DRaaS provider, based on business acumen, technical IT recovery architects, and operational assistance in planning and documentation of BCDR strategies.

 Unfortunately, as is often the case for new cloud-hosted architectures, some PaaS administrators are incorrectly presuming that the native durability of cloud-hosted services relieves the need for backup: 34% of organisations do not yet back up their cloud-hosted file shares, and 15% do not back up their cloud-hosted databases.

"The growing adoption of cloud-powered tools and services, escalated by the massive shift to remote work and current hybrid work environments, put a spotlight on hybrid IT and data protection strategies across industries," said Danny Allan, CTO and Senior Vice President of Product Strategy at Veeam. "As cybersecurity threats continue to increase, organisations must look beyond traditional backup services and build a purposeful approach that best suits their business needs and cloud strategy. This survey shows that workloads continue to fluidly move from data centers to clouds and back again, as well as from one cloud

to another — creating even more complexity in data protection strategy. The results of this survey show that while modern IT enterprises have made significant strides in cloud and data protection, there is still work to be done."

The Veeam Cloud Protection Trends Report 2023 findings include: Software as a Service (SaaS):

- 90% of organisations realize they need to back up Microsoft 365. The report revealed only 1 in 9 (11%) organisations do not protect their Microsoft 365 data

 a promising majority of 89% use thirdparty backups/BaaS or enhanced tiers of Microsoft 365 for legal hold, or both.
- As data protection strategies have evolved and ransomware continues to be a top concern, most organisations are delegating backup responsibilities to backup specialists, instead of requiring each workload (laaS, SaaS, PaaS) owner to protect their own data. This fuels the progression of backup becoming a conventional component tasked to the traditional backup admin versus the application team.

Infrastructure as a Service (laaS): While organisations of all sizes now embrace hybrid-cloud architectures, it is not a oneway journey to the cloud that reduces the importance of the modern data center.

- 30% of cloud-hosted workloads were from "cloud first" strategies, whereby new workloads are starting in clouds at far faster rates than old workloads are being decommissioned in the data center.
- 98% of organisations utilise a cloudhosted infrastructure as part of their data protection strategy, including cloud-storage tiers, cloud-infrastructure as their disaster recovery site, or the use of BaaS/DRaaS providers.
- 88% of organisations brought workloads from the cloud back to their data center for one or more reasons (development, cost/performance optimisation, or disaster recovery) — highlighting a need for 2023 data protection strategies to ensure consistent protection and the ability to migrate, as workloads move

THE GROWING ADOPTION OF CLOUD-POWERED TOOLS AND SERVICES, PUTS A SPOTLIGHT ON HYBRID IT AND DATA PROTECTION STRATEGIES ACROSS INDUSTRIES.

from data center to cloud, cloud to data center, or from one cloud to another cloud.

 The majority of backups of cloud workloads are now being done by the backup team and no longer require the specialised expertise or added burden of cloud administrators. However, while nearly every organisation acknowledged having long-term regulatory mandates, only half of organisations retain backups of their cloud data for even one year.

Platform as a Service (PaaS): While most organisations initially "lift and shift" servers from the data center to laaS, most agree that running foundational IT scenarios, such as file shares or databases, as native cloud-services is the future for mature IT workloads:

- 76% run file services within cloudhosted servers and 56% run managed file shares from AWS or Microsoft Azure
- 78% run databases within cloudhosted servers and 65% run managed databases from AWS or Microsoft Azure

Backup and Disaster Recovery as a Service (BaaS/DRaaS): Nearly every laaS/SaaS environment also utilises cloud services as part of their data protection strategy in some form.

- 58% of organisations utilise managed backup (BaaS) compared to the 42% that utilize cloud storage as part of their self-managed data protection solution.
 Of special interest, nearly half (48%) started with self-managed cloud storage but eventually switched to BaaS.
- Nearly every organisation (98%) claims to use cloud services as part of their data protection strategy, though that varies from cloud storage as a repository to full-fledged BaaS or DRaaS services.
- BaaS is predominantly sought for gaining operational and economic efficiencies, as well as assuring data survivability from

- disasters and ransomware attacks. It is notable that BaaS is no longer seen as the "tape killer" that early pundits offered, with organisations stating that nearly 50% of their data is still stored on tape during its lifecycle, regardless of their use of cloud-based data protection services.
- DRaaS is perceived as surpassing the tactical benefits of BaaS by providing expertise around BCDR planning, implementation, and testing. Expertise is perceived as a primary differentiator by subscribers choosing their BaaS/DRaaS provider, based on business acumen, technical IT recovery architects, and operational assistance in planning and documentation of BCDR strategies.

This year's report showed a significant shift from last year as customers are increasingly interested in outsourcing their backups and gaining a "turnkey" or "white-glove" level of management service instead of the internal IT staff continuing to manage BaaS-delivered infrastructure. This shift indicates that experience and trust in providers is increasing and could also point to challenges over the past year with the IT talent supply chain.

The Veeam Cloud Protection Trends Report 2023, born from the annual Veeam Data Protection Trends Report, is the result of a third-party research firm that surveyed 1,700 unbiased IT leaders from 7 countries (US, UK, France, Germany, Japan, Australia, New Zealand) on their use of cloud services in both production and protection scenarios to deliver the largest single view into the trajectory of hybrid strategies across the modern IT enterprise in today's cloud-first digital landscape. The broad-based market study was conducted to understand the various perspectives on responsibilities and methodologies related to operating and protecting cloud-hosted workloads, and considerations when using cloud-powered data protection.

SECURING THE DIGITAL WORKSPACE

VERONICA MARTIN CAUGHT UP WITH **HARISH MENON**, CEO AT ACCOPS, TO DISCUSS GITEX 2022 AND THE COMPANY'S PLANS FOR THE REGION.



an you tell our readers about some of the solutions and partnerships during GITEX this year?

It was great to be a part of GITEX and showcase our solutions to customers, partners, and exhibitors. What we bring to the region is primarily a range of information security tooling platforms and virtual desktops. We specialise in providing our customers a secure digital workspace.

In the last 12 months, how has your company performed in the MENA market? Has your company ventured into any new markets/countries, and can you share your overall growth?

Our engineering centre is in Pune, India

and since five years ago, we have expanded globally. Japan is our second biggest market outside of India, followed by the Middle East and Africa. We also have plans to venture North America and Europe. We many promising investments with the government and public sector in Middle East and Africa. We are thrilled to be a part of the growth of the region and we want to



continue showcasing how we can grow with customers here.

Which technologies and IT trends are the forefront of driving innovation for your business?

We specialise in digital workspaces, so primarily what we bring to the region is securing the workspace.

Today users are coming from different locations and aren't just vendors or employees. There are also machines now accessing a corporate network, so the term user has a new definition. It's no longer people, it's also machines. Given that changed dimension, there are a couple of major elements to ensure that people and machines continue collaborating in this digitally transforming world.

Trust is number one. There is a Zero Trust network access framework we work with and consolidate your vendors. You should try to have less vendors in your technology ecosystem because the more vendors you got, the more the complexities you have to work with. That's an area we really focus on because our entire product

IDENTITY WILL BECOME A VERY PRECIOUS THING IN FUTURE AND WON'T BE LIMITED TO JUST WHAT WE SEE.

offers customers to work with less vendors.

The second is learning systems, such as AI and ML that ensure the security threats are proactively defended. We are also propagating the desktop as a service and we believe in the future data won't travel to the endpoint, only images.

Besides, identity will become a very precious thing in future and won't be limited to just what we see. It could be a fingerprint, a retina, so we propagate the messaging of converge identity management.

What do you think it makes your different from your competitors?

I believe that whenever there has been

transformation, which has come globally, you have a frugal engineering, which is a way of staying ahead in this transformative and uncertain world we live in today. We've adopted frugal engineering as a part of our execution process from the time the code is written and after the time the product is sold. That's a very important aspect of how we have developed our products and solutions and because we've used frugal engineering, we are able to offer the best solution to the customer and the most optimised licensing.

This brings us as a very relevant vendor today to companies across the globe and I can give you an example of what happened recently because of the Ukraine Russia war. Out of the blue, we got an inquiry from a customer in Europe wanting to see how his freelancers from Ukraine could collaborate on their portal, but they had to make sure the work they were going to access was secure. Using our technology, we were able to make sure that their work access continued securely, so we more than exceeded the customer's expectations.

EVERY DAY IS PHISHING SEASON!

JOSH GOLDFARB, FRAUD SOLUTIONS ARCHITECT FOR EMEA AND APCJ AT F5, ON WHY YOU CAN'T AFFORD TO IGNORE A WELL-KNOWN AND GROWING MENACE

f a burglar wanted to gain entry to your home, they could force their way in - perhaps by picking a lock, breaking a window, or some other means. If a neighbour heard noises or saw strange activity, they might call the police. This might result in the burglar getting caught, of course.

On the other hand, the burglar could try to convince you to hand over your keys willingly. Perhaps by posing as a delivery or repair person, or inspector, or by telling a plausible story. If the burglar can get their hands on the keys, they can simply walk right in - as if they are doing so legitimately, and no one suspects a thing.

In the digital world, phishing is how burglars (cybercriminals) gain entry to your home (your critical systems and sensitive data). Successful phishing attacks provide attackers with stolen credentials that allow them to simply 'walk into' your business and gain

access to the targets they have set their sights on.

How come phishing is so effective? Well, for starters, phishing attacks have evolved significantly in recent years. Whereas they once were primitive, full of typos, and not particularly convincing, nowadays, even experts have trouble distinguishing phishing emails from legitimate emails. Phishing sites also look remarkably like the legitimate ones they are designed to imitate. It is no wonder so many users are fooled into providing their credentials to the attackers. In other words, handing over their keys willingly.

As many businesses continue to go

through a digital transformation, the use of this method of attack has greatly accelerated, and the resulting damage spreading. An increased online presence means a bigger online attack surface and risk. Attackers don't need to devise complex schemes to force entry into businesses these days - they can merely invest in convincing unsuspecting users to hand over their valid credentials.

That said, what can businesses do to protect their online applications from security and fraud incidents?

Simply rooting out the phishing sites is not enough to combat credential theft. Attackers can create phishing sites with ease. When we take one down, another one pops up elsewhere. This can often devolve into a never-ending battle of attrition that rarely makes our online applications more secure or protects them from fraud.

Instead, if we assume that a certain percentage of our legitimate users will fall prey to phishing attacks and will have their credentials stolen, we can adapt accordingly. When we shift our perspective and take this approach, we realise that identifying and mitigating security and fraud attacks that result from credential theft becomes one of our main focuses. Adapting our approach helps us to protect our online applications from the array of phishing attacks that are likely being launched against them on a regular basis.

There are likely many approaches we can take to mitigating risk due to credential theft. Here are a few of them:

• Eliminate automation. Attackers build



databases of stolen credentials that they amass from a variety of sources, phishing among them. Those stolen credentials are often tested in bulk using bots. The credentials that are valid are then often used to commit Account Takeover (ATO) and manual fraud. Eliminating these automated attacks not only mitigates this risk, it also reduces infrastructure costs going to undesired non-human (bot) traffic.

- Stop ATO. Attackers that can leverage valid stolen credentials to log in to stolen accounts and masquerade as legitimate users can use that access to commit fraud. This manual fraud, of course, results in losses incurred by businesses that fall victim to these incidents. Detecting and mitigating Account Takeover (ATO) stops these fraud losses, saving businesses money.
- Reduce friction. Increased risk of fraud often results in businesses instituting more stringent authentication and Multi-Factor Authentication (MFA) requirements.

Unfortunately, this approach adds friction for legitimate customers without significantly reducing fraud losses.

Attackers are resourceful, motivated, and adept at finding workarounds. If we can reliably identify automation and manual fraud, we can also reliably identify desired legitimate traffic. Once we know the traffic we want, we are less likely to inconvenience legitimate customers and can focus on stopping the attackers instead. 2



Secure Your Digital Future

Simple. Secure. Resilient.



Secure Your Enterprise IT Footprint For A Safer Digital Journey

www.raqmiyat.com UAE | KSA | INDIA

MEDIUM-SIZE BUSINESSES IN UAE CONSIDER USING PIRATED SOFTWARE TO CUT COSTS: KASPERSKY

he latest Kaspersky report reveals 24% of companies in the UAE with 50 to 999 employees are ready to use pirated alternatives of business software to decrease IT spending. Among small businesses (less than 50 employees), only 13% are ready to take this step. This measure can seriously affect corporate cyber safety, since adversaries actively distribute malicious files under the guise of most used software.

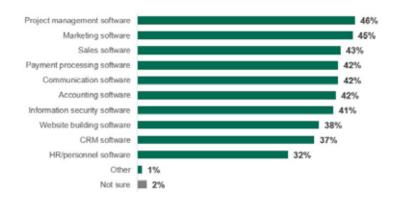
According to Kaspersky Security
Network (KSN), in just eight months the
total number of users who encountered
malware and unwanted software
masquerading as the most popular
software products for small and medium
businesses was 9,685. In general, 4,525
unique malicious or potentially unwanted
files were spread via unofficially
distributed (including pirated) SMBrelated software.

The Kaspersky study aims to explore which crisis management tactics business leaders find most successful, and how some steps can seriously affect a company's cyber resilience. Safe measures such as seeking lower-cost contractors and adopting free alternatives of usual software are most popular with the respondents, gaining 41% and 32% respectively, but 20% of surveyed business leaders would replace their software with a pirated version to cut costs.

As for the type of programs respondents believe they could replace with hacked copies, the majority chose project management, marketing and sales software - 60% even agree to use a pirated cybersecurity software.

"A lack of resources is a common

What types of software would you replace with a pirated alternative?



situation for small and medium businesses but use of a pirated or hacked software should be completely excluded if an organization values its safety, reputation and income. Pirated copies of software usually come with Trojans and miners and do not contain the fixes or patches released by developers to close vulnerabilities that might be exploited by cybercriminals. Official free alternatives are much better options for those who need to save money on IT," said Alexander Shlychkov, Product Marketing Lead at Kaspersky.

To avoid data leakage and financial losses caused by infected software installation, implement the following Kaspersky's recommendations:

- Make sure your employees use standard accounts without admin rights. That will prevent them from accidentally installing a Trojan mistaken for productivity software.
- You can use free security solutions.
 They usually have less functions than paid products but still might be very helpful. Choose a solution based on the independent tests' results,

- and download it directly from the developer's site.
- To avoid paying a hidden miner electricity bills, try to constantly monitor your devices efficiency. If your gadget is slowing down, overheats and makes a lot of noise even when no one is using it, someone might have installed a miner on the device which is overloading the processor and video card. Use a security solution that detects not only malicious programs, but also potentially unwanted installments.
- Update your operating system, security software, browser and all the programs you work with as soon as a new update comes out.
- Implement regular backups of important files in a cloud service and on alternative hardware. That will allow you to have a copy even if ransomware encrypts your data. A security solution with remediation feature will let you roll back actions performed by malware in the operating system, delivering protection against cryptolockers.



Make the most of WiFi 6.

Linksys Atlas Pro 6 with Intelligent Mesh[™] is a dual-band WiFi 6 system that delivers next-level streaming, data traffic and uninterrupted video conferencing to more than 30 devices per node simultaneously.

Access to 160 MHz — the least congested channels available on the 5GHz band — unleashes WiFi 6's incredibly fast connectivity.



Up to 3,5X faster speeds than WiFi 5.

Mesh WiFi 6 delivers true gigabit speeds—up to 5.4 Gbps with 6-stream connectivity—throughout your entire home or business, inside & out.

160 MHz capable.

Access to the least congested channels on the 5 GHz band unleashes the true power of WiFi 6, allowing work-from-home, online learning, streaming & gaming devices to operate simultaneously without reduced bandwidth.

Linksys.com

More WiFi Channels.

Dynamic Frequency Selection (DFS provides access to more channels, reducing interference from neighbouring networks.

Industry-leading technology.

The Qualcomm* Immersive Home 216 Platform transforms home & business WiFi to wired-like stability & speed.

Easy setup & control.

It's simple to set up and lets you manage your network or prioritise devices from anywhere, all with the free Linksys app.

As compared from 802.11ac to 802.11ax.

30+ devices

Capacity per node.



AX5400

Accumulated speed up to 5.4 Gbps.



Covers homes with up to

2-3 bedrooms

per node (±230 m² / 1 floor).



Model# MX5500

Available in 1-, 2- or 3-Pack: MX5501, MX5502, MX5503

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.

