

Security

ADVISOR

MIDDLE EAST

INTERVIEW:

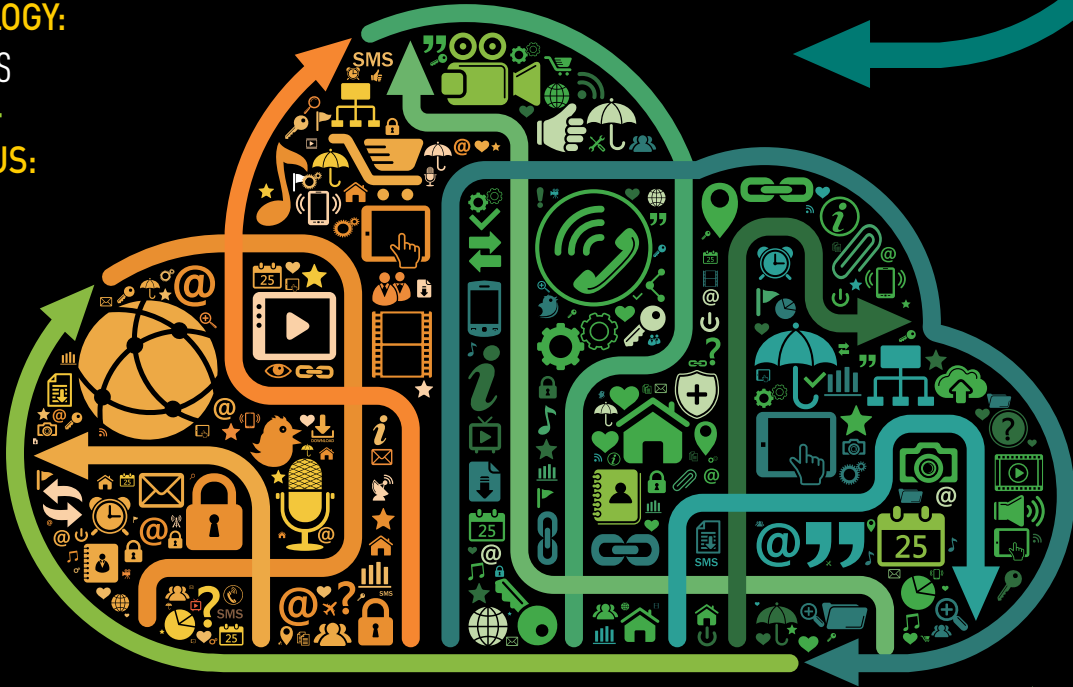
SECLORE

TECHNOLOGY:

SOPHOS

IN FOCUS:

ESET



A HYBRID APPROACH

DOES A HYBRID SECURITY APPROACH ENSURE
MAXIMUM PROTECTION AGAINST AN INCREASINGLY
COMPLICATED ATTACK LANDSCAPE? WE EXAMINE.



Connect to more...

D-Link®

PROFESSIONAL IP SURVEILLANCE SOLUTIONS



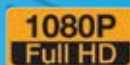
**Making the move to digital technology
at your own pace**

Easy & Pro Series Range | IP Cameras & NVRs | Deep Video Compression | Superior Quality | Video Analytics
Centralized Management | Starlight & Super Starlight

Monitor Your Premises From Anywhere



H.265+



CONTENTS



06 NEWS

Top news & headlines from the world of cybersecurity.

INTERVIEWS

10 Seclore

Vishal Gupta, CEO & Founder, Seclore, explains how the company's device-agnostic, automated range of security solutions makes it the preferred choice for some of the largest enterprises in the world.

18 Micro Focus

Tamer El Refaey – Chief Cyber Security Strategist, Emerging Markets, Micro Focus, on the need for a strong cyber resilience strategy.

26 Spire Solutions

Sanjeev Walia, Founder & President, Spire Solutions, on the cybersecurity landscape and the growth trajectory of the organization.



30 Check Point

Ram Narayanan, Country Manager, Check Point Software Technologies, ME tell us more about cloud security.



AVIENTEK

Distributor of Audio Visual & IT Products

Middle East | India | Africa



ENHANCE YOUR MEETING WITH PROFESSIONAL AV

ARE YOU ON THE RIGHT TRACK ?

- Video Conferencing
- Audio Conferencing
- Wireless Microphones
- Wireless Collaboration
- Interactive Display
- Professional Display
- Camera Extenders
- Video Wall Processors
- Media Streaming
- AV Mounting Systems
- AV Furniture
- AV Distribution Systems
- AV Racks
- Retractable Monitor
- Control Systems



EPSON



logitech®

NEC

ClearOne.

CLEVERTOUCH

DIGIBIRD

DTEN

OPTERNA

PureLink

PureLink

SCREENLINE

SOLTEC

WOLFvision

AVIENTEK LLC: Office#107, API Business Suites, Sheikh Zayed Road, Al Barsha 1, Dubai, UAE. Tel: +971 4 343 6216

AVIENTEK FZE: PO. Box-341290, Dubai Silicon Oasis, Dubai, United Arab Emirates

AVIENTEK TRADING WLL: Office# 26, Building-20, Street-940, Najma, C-Ring Road, Doha, Qatar.

EDITORIAL



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

Anita Joseph
Editor

A HYBRID APPROACH TO SECURITY

Cybersecurity is no longer an option for businesses-what with an increasingly complex and complicated threat landscape and distributed IT environments, companies have realized that a comprehensive, resilient infrastructure is critical to safeguard critical applications.

Hybrid IT can strengthen the IT posture of organizations because it provides them more control over data, helps them make more informed decisions and choose the best place for their data to reside. A hybrid infrastructure calls for a hybrid approach to security as well, helping to consolidate the overall cybersecurity framework.

This is what we've highlighted in this issue-we've spoken to some experts to find out how a hybrid approach to security can act as an effective deterrent for a threat landscape that is sophisticated and unpredictable. I won't spoil the excitement, read our cover

story to find out more.

In addition to this, we have our regular columns and expert insights into the world of cybersecurity now and in future. Not to mention, interviews with cybersecurity leaders such as Seclore, Check Point, Spire Solutions and Micro Focus.

Seclore's Vishal Gupta talks about redefining data security, while Check Point's Ram Narayanan explains in detail what cloud security entails. We also have Sanjeev Walia, Founder & President of Spire Solutions, telling us about the cybersecurity landscape and the

growth trajectory of the organisation. Tamer El Refaey – Chief Cyber Security Strategist, Emerging Markets, Micro Focus, elaborates on the need for a strong cyber resilience strategy for companies to grow and thrive in the midst of a crisis.

So, here's to an engrossing and informative issue-Happy Reading!

HYBRID IT CAN
STRENGTHEN THE
IT POSTURE OF
ORGANIZATIONS.

EVENTS



FOUNDER, CPI MEDIA GROUP
Dominic De Sousa (1959-2015)

Published by
CPI

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

**EDITORIAL
Editor**
Anita Joseph
anita.joseph@cpimediagroup.com

**DESIGN
Senior Designer**
Analou Balbero
analou.balbero@cpimediagroup.com

Registered at
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

**ADVERTISING
Group Sales Director**
Kausar Syed
kausar.syed@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

**DIGITAL SERVICES
Web Developer**
Adarsh Snehan

Reception: +971 4 5682993
Operations: +971 4 5682994
Accounts: +971 4 5682995

Senior Sales Manager
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2021 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.

CHECK POINT SOFTWARE REPORT REVEALS 29% INCREASE IN CYBER-ATTACKS GLOBALLY

MAYA HOROWITZ,
VP RESEARCH AT
CHECK POINT
SOFTWARE



Check Point

Research, the Threat Intelligence arm of Check Point® Software Technologies Ltd., a leading provider of cyber security solutions globally, has released its 'Cyber Attack Trends: 2021 Mid-Year Report' which shows how cyber criminals have continued to exploit the global shift to hybrid working and target organizations across all sectors, including government, healthcare and critical infrastructure.

Organizations have experienced a 29% increase in cyber-attacks globally. The EMEA region showed the highest growth with 36%, followed by the Americas with an increase of 34% with APAC witnessing a 13% growth in attacks. This year has also seen a new 'Triple Extortion' ransomware technique emerge.

"In the first half of 2021, cyber criminals have continued to adapt their working practices in order to exploit the shift to hybrid working, targeting organizations' supply chains and network links to partners in order to achieve maximum disruption," said Maya Horowitz, VP Research at Check Point Software. "This year cyber-attacks have continued to break records and we have even seen a huge increase in the number of ransomware attacks, with high-profile incidents such as Solarwinds, Colonial Pipeline, JBS or Kayesa. Looking ahead, organizations should be aware of the risks and ensure that they have the appropriate solutions in place to prevent, without disrupting the normal business flow, the majority of attacks including the most advanced ones."

FORTINET UNVEILS INDUSTRY'S FIRST HIGH PERFORMANCE NEXT-GEN FIREWALL

Fortinet, a global

leader in broad, integrated and automated cybersecurity solutions, has announced the FortiGate 3500F

Next-Generation Firewall (NGFW) to protect organizations with hybrid data centers against the ever-growing threat landscape and ransomware attacks. FortiGate 3500F offers some of the industry's highest performance numbers, including TLS1.3, with automated threat protection post decryption. Additionally, FortiGate 3500F is built with zero trust network access (ZTNA) capabilities, further delivering consistent security and seamless user experience to any user at any location with its security-driven networking approach.



FortiGate 3500F NGFW helps organizations ensure business continuity and advanced security for hybrid data centers. With the industry's highest Security Compute Rating (SCR) of 6x IPsec, FortiGate 3500F NGFW secures the data center edge, core and interconnect by providing ultra-fast secure data center to data center paths to build disaster recovery sites. It also enables organizations to secure data center to cloud paths for cloud on-ramps with full compliance and controls.

SANS INSTITUTE LAUNCHES INTERACTIVE SUMMER CYBERSECURITY COURSES FOR GULF PROFESSIONALS

SANS Institute, the global leader in cyber

security training and certifications, announced its upcoming live online training program 'SANS Summer Dunes August 2021 Live Online', to be held from 14th – 19th August. Designed to offer flexible access to cyber security training taught by real-world practitioners, the event enables Gulf professionals to protect their assets by learning critical skills in a hands-on labs in a virtual setting.

Expert instructors will help participants develop skills in topics such as network penetration testing, advanced incident response and threat hunting to defend their organisations against ever-increasing cyber threats. 'SANS Summer Dunes August 2021 Live Online' will feature two new GIAC-certified courses:

NED BALTAGI, MANAGING
DIRECTOR – MIDDLE
EAST AND AFRICA AT
SANS INSTITUTE



ICS410: ICS/SCADA Security Essentials, aimed at industrial cybersecurity professionals; and MGT551 Managing a Security Operations Centre (SOC), aimed at those looking to build SOC's.

"Through its ambitious vision, the Gulf is on course to become one of the world's most digitised economies. While a truly networked region will be the catalyst for exponential business and civic progress, these opportunities also mandate the need for vigilant protection of corporate and government networks," commented Ned Baltagi, Managing Director – Middle East and Africa at SANS Institute.

CYBEREASON EXPOSES CHINESE THREAT ACTORS COMPROMISING TELECOMMUNICATIONS PROVIDERS FOR CYBER ESPIONAGE

Cybereason, the leader in operation-centric attack protection, has announced the discovery of several previously unidentified cyber-attack campaigns infiltrating major telecommunications providers across Southeast Asia. Similar to the recent SolarWinds and Kaseya attacks, the threat actors first compromised third-party service providers — but in this case instead of using them to deliver malware through a supply chain attack, the intent was to leverage them to conduct surveillance of their customers' confidential communications.

In the report, titled *DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos*, multiple clusters of

LIOR DIV, CEO & CO-FOUNDER, CYBEREASON



attack activity were identified that have evaded detection since at least 2017 and are assessed to be the work of several prominent Advanced Persistent Threat (APT) groups aligned with the interests of the Chinese government. Cybereason observed a significant overlap in tactics, techniques

MULTIPLE CLUSTERS OF ACTIVITY WERE IDENTIFIED THAT HAVE EVADED DETECTION SINCE AT LEAST 2017.

and procedures (TTPs) across the three operations and assessed that the attackers were likely tasked with parallel objectives under the direction of a centralized coordinating body aligned with Chinese state interests.

BEYONDTRUST INTRODUCES NEW PRIVILEGE MANAGEMENT FOR WINDOWS & MAC

BeyondTrust, the worldwide technology leader in Privileged Access Management (PAM), announced further product enhancements and integrations to its market-leading BeyondTrust Privilege Management for Windows & Mac (PMWM) product. This solution enables a preventative approach to endpoint security, stopping malicious attacks by enforcing passwordless administration, "Just-in-Time" access, and pragmatic application control on endpoints.

"The latest Privilege Management for Windows & Mac releases exemplify our innovative approach to

DAN DEROSA, CHIEF PRODUCT OFFICER AT BEYONDTRUST



Endpoint Privilege Management, by focusing on capabilities related to enabling endpoint security," says Dan DeRosa, Chief Product Officer at BeyondTrust. "With the massive shift of endpoints outside of the traditional perimeter as a result of the remote working expansion, it's more critical than ever to protect them from the threats of ransomware and other threats."

THE SOLUTION ENABLES A PREVENTATIVE APPROACH TO ENDPOINT SECURITY.

MODEE JORDAN USES NUTANIX TO ENABLE SECURE, HIGH-PERFORMANCE EMAIL SERVICES FOR GOVERNMENT EMPLOYEES

ABDALLAH FARRAYIH, HEAD OF OPERATION, MODEE



Nutanix, Inc.

a leader in private cloud, hybrid, and multicloud computing, announced that the Jordanian government entity Ministry of Digital Economy and Entrepreneurship (MoDEE) has successfully deployed Nutanix Hyperconverged Infrastructure (HCI) and Nutanix Prism Pro management solution. The implementation enables secure, high-performance email services for the entire Jordanian government and provides high-availability for over 53,000 mailboxes with the ability to effortlessly expand capacity as required. The solution has also reduced infrastructure costs, and IT management overheads.

"Nutanix stood out for its ability to offer the most compute resources and storage at a more attractive price point and in a small form factor. They convincingly demonstrated how data migration and expansion could be effortlessly accommodated and offered us the freedom to use any of the most popular hypervisors," said Abdallah Farrayih, Head of Operation, MoDEE. "When you consider that we need to reliably deliver email services for over fifty thousand users, the lower resource requirements, lower size and thereby power consumption, and simplified management benefits that are made possible by Nutanix are all exponentially amplified," Farrayih added.

TENABLE HELPS ORGANISATIONS DISRUPT ATTACKS WITH NEW ACTIVE DIRECTORY SECURITY READINESS CHECKS

RENAUD DERAISON,
CO-FOUNDER AND
CHIEF TECHNOLOGY
OFFICER, TENABLE.



In the wake

of a growing number of both ransomware and sophisticated attacks, Tenable, Inc., the Cyber Exposure company, has developed 10 foundational configuration checks for its solutions, including Tenable.io, Tenable.sc and both Nessus Professional and Nessus Essentials, that assess Microsoft Active Directory security readiness and align remediation efforts based on the threat landscape. These checks leverage Tenable's expertise in securing Active Directory environments through Tenable.ad and are available immediately for existing customers at no extra charge.

"We're seeing the weaponisation of Active Directory by bad actors virtually every time a new ransomware attack or hack makes the headlines. Securing Active Directory is one of the most critical steps virtually any organisation should take to build stronger cyber defences and a solid foundation for their digital business", said Renaud Deraison, Co-Founder and Chief Technology Officer, Tenable. "We're helping to address this growing crisis with new Active Directory checks that make it easier than ever for customers to understand what steps they must take immediately to get their Active Directory security in order and disrupt bad actors' go-to attack paths".

The Active Directory Security Readiness Checks are now generally available in Tenable.sc, Tenable.io, Tenable.ep, Nessus Professional and Nessus Essentials.

COHESITY APPOINTS GREGG PETERSEN AS MEA LEAD

Cohesity has appointed Gregg Petersen

as regional director for its operations in the Middle East and Africa (MEA) region. Petersen will focus on empowering regional businesses in UAE, Saudi Arabia, Qatar, Egypt, and South Africa to easily and effectively back up, manage, protect, and derive value from their data through Cohesity's next-gen data management solutions.

Petersen, a prominent figure in the MEA IT industry, brings 14 years of relevant experience to Cohesity, including his most recent role at Rackspace. He will work closely with channel

GREGG PETERSEN



and ecosystem partners as customers in the MEA region embrace modern, cloud-native data management solutions.

Petersen will also work closely with global technology alliance partners including Cisco, HPE, and Pure Storage and hyperscale cloud providers such

as AWS, Microsoft Azure, and Google Cloud, along with an expanded set of local distribution and reseller partners, service providers and global systems integrators (GSIs).

**PETERSEN
BRINGS 14 YEARS
OF RELEVANT
EXPERIENCE TO
COHESITY.**

MIMECAST JOINS XDR ALLIANCE AS FOUNDING MEMBER



JULES MARTIN,
VICE-PRESIDENT
ECOSYSTEM &
ALLIANCES AT
MIMECAST

Mimecast Limited, a leading email security and cyber resilience company, announced it has joined Exabeam's XDR Alliance™ as a founding member. The alliance is a partnership of leading cybersecurity industry innovators committed to an inclusive and collaborative extended detection and response (XDR) framework and architecture. The goal of the XDR Alliance is to foster an open approach to XDR which is essential to enable organizations everywhere to protect themselves against the growing number of cyberattacks, breaches, and intrusions.

"We are thrilled to

be a founding member and inaugural email security partner in the XDR Alliance," said Jules Martin, vice president ecosystem & alliances at Mimecast. "We see collaboration in security being essential in keeping our customers safe, and leveraging the members' interconnected, best in class cybersecurity solutions, which allows joint customers to benefit greatly."

Collaboration is at the core of

Mimecast's industry leading cyber resilience ecosystem, which includes Exabeam plus 60 other partners, and supports the open framework that are engineered to underpin threat sharing, control points and remediation capabilities which are fundamental to the modern enterprise.

**THE ALLIANCE IS
A PARTNERSHIP
OF LEADING
CYBERSECURITY
INNOVATORS
COMMITTED TO AN
INCLUSIVE XDR
FRAMEWORK.**

SOPHOS ACQUIRES REFACTR TO OPTIMIZE MANAGED THREAT RESPONSE

Sophos, a global leader in next-generation cybersecurity, announced that it has acquired Refactr, which develops and markets a versatile DevSecOps automation platform that bridges the gap between DevOps and cybersecurity. Based in Bellevue, Washington, Refactr launched in 2017 and is privately held.

With Refactr's platform, DevOps teams can augment existing continuous integration, continuous delivery and continuous deployment (CI/CD) workflows, and cybersecurity teams can leverage the platform's visual drag and drop builder. Refactr has leading customers in both the private and government/public sectors, including the Center for Internet Security and the

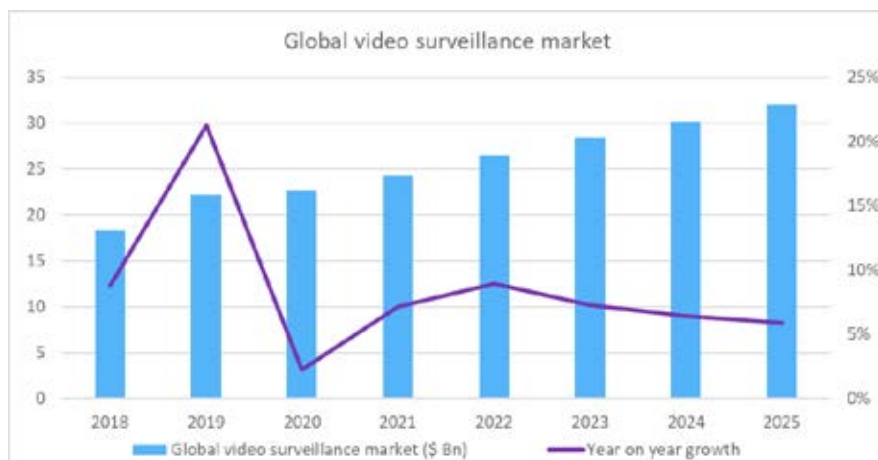
JOE LEVY, CHIEF
TECHNOLOGY
OFFICER, SOPHOS



U.S. Air Force's Platform One.

Sophos is optimizing Refactr's DevSecOps automation platform to add Security Orchestration Automation and Response (SOAR) capabilities to its Managed Threat Response (MTR) and Extended Detection and Response (XDR) solutions. The SOAR capabilities will also help automate Sophos' Adaptive Cybersecurity Ecosystem, which underpins all of Sophos' product solutions, services, threat intelligence, and data lake.

TOTAL VIDEO SURVEILLANCE MARKET REVENUES TO HIT \$24.2BN IN 2021



Global video surveillance market revenues are set to reach \$24 bn by the end of 2021 according to Omdia's latest Video Surveillance and Analytics Intelligence Database.

This marks a quick recovery for the video surveillance market as demand that was suppressed in 2020 will return and revenues will be bolstered by projects that were postponed in 2020 due to COVID getting the greenlight in

2021. Omdia forecasts that total video surveillance market revenues will grow to \$31.9bn by 2025 with a total CAGR of 7.1% between 2020-2025.

Omdia expects average selling prices of video surveillance equipment to increase in the short term as US-China geopolitical tension and supply chain constraints from the COVID-19 pandemic increases pressure of vendor margins.

QUALYS COLLABORATES WITH RED HAT TO ENHANCE SECURITY FOR RED HAT ENTERPRISE LINUX COREOS & RED HAT OPENSIFT

SUMEDH THAKAR



Qualys, Inc.,

a pioneer and leading provider of disruptive cloud-based IT, security and compliance solutions, has announced it has collaborated with Red Hat to drive greater security for both the container and host operating system for Red Hat OpenShift.

Teaming with Red Hat, Qualys is offering a unique approach providing a containerized Qualys Cloud Agent that extends security to the operating system. The Cloud Agent for Red Hat Enterprise Linux CoreOS on OpenShift combined with the Qualys solution for Container Security provides continuous discovery of packages and vulnerabilities for the complete Red Hat OpenShift stack. Built on the Qualys Cloud Platform, Qualys' solution seamlessly integrates with customers' vulnerability management workflows, reporting and metrics to help reduce risk.

"As security teams look to support modern applications built on cutting edge technology like Red Hat OpenShift, they need to secure both the running container images and the underlying OpenShift cluster," said Sumedh Thakar, president and CEO of Qualys. "By collaborating with Red Hat, we have built a unique approach to secure Red Hat Enterprise Linux CoreOS that provides complete control over containerized workloads enhancing Qualys' ability to help customers discover, track and continuously secure containers," he added.

REDEFINING DATA SECURITY

VISHAL GUPTA, CEO & FOUNDER, SECLORE, EXPLAINS HOW THE COMPANY'S DEVICE-AGNOSTIC, AUTOMATED RANGE OF SECURITY SOLUTIONS MAKES IT THE PREFERRED CHOICE FOR SOME OF THE LARGEST ENTERPRISES IN THE WORLD.



What is the biggest challenge faced by encryption and rights management technologies today?

Encryption and even rights management technologies have been tough for users to adopt. They require complicated setups of key and software agents and lots of user education over a period of time. This becomes cumbersome to manage. Often, enterprises have had to hire armies to manage encryption/rights management technologies as they become key and policy management nightmares.

Overall, I believe that a lack of automation at the user and security administration levels has been the biggest stumbling block. Users are forced to make decisions such as what to protect, how to protect, what policy to apply, how to monitor, when to change the policy and when to raise an alarm, while security administrators are busy defining and managing security policies and user permissions and rights.

This combination of clunky user experience and high overheads has been the adoption bane in the encryption and rights management world.

Emails are the most common source of data breaches today. Are existing email gateways and encryptions enough to secure them?

The focus with most email security systems today is threat protection i.e., how we prevent hackers from infiltrating the enterprise. Today, the biggest risks arise from the lack of data protection, i.e., how we prevent confidential information from being exfiltrated or misused by internal or external actors. This non-linear focus on threat protection leaves the goal of data protection unachieved by present-day email security systems.

Therefore, the need today is to combine the best threat protection systems like

SECLURE'S EMAIL PROTECTION CAPABILITIES ARE COMPLETELY DEVICE-AGNOSTIC SO THEY WORK WITH ANY DEVICE WHICH COULD BE CREATING OR CONSUMING ENTERPRISE EMAILS.

anti-malware, anti-phishing, APT, etc. with the best data protection systems like encryption, rights management, and data-centric audits. This combination can help enterprises continue using email as the dominant method for both internal and external collaboration.

What is Seclore's approach to email security? Can you tell us more about the Seclore Email Protector and its key features?

Seclore's approach to email security is based on 4 key principles:

Automation – The best products are the ones which we don't have to 'use' at all

User experience – The user experience must be seamless and should encourage security-conscious behavior and not try to bypass the system across personal devices like mobile phones and corporate devices.

Visibility – Users and enterprise security professionals appreciate the visibility of what is happening to their emails within and outside of the enterprise.

Bullet-proof Security – The security of emails and documents should not be dependent on complicated and faulty key management, endpoint agents, and insecure infrastructure.

With built-in capabilities to

automatically protect emails from official computers, personal phones and web interfaces, as well as applications AND integration with leading DLP and email security systems, Seclore eliminates the need for user participation or awareness. The user experience is seamless without the need to download/install clunky agents and extends to all devices and operating systems. The enterprise and the users get visibility into WHO is using the information shared via email, WHAT is each person doing, WHEN and from WHERE. This visibility is extremely important for privacy compliance and breach investigations. Granular controls and dynamic policy management allows for highly confidential information to be shared with people while still allowing for remote destruction, should the need arise.

These capabilities have made Seclore the data protection solution of choice for some of the largest enterprises in the world.

Emails on mobile phones are even more vulnerable to breaches and attacks than the ones accessed on laptops. How does Seclore Email Protector address this problem?

Seclore's email protection capabilities are completely device-agnostic so they work with any device which could be creating or consuming enterprise emails. The device itself need not be under enterprise control for "Seclored" emails to be created or consumed on it.

The biggest challenge for security teams in enterprises when it comes to emails on personal devices has been the lack of control over these devices. Users have specific preferences on the devices they want to use and for enterprises to even gain visibility to the devices being used is tough. Seclore solves this problem by relieving the enterprise of exercising control over user devices while still ensuring that enterprise emails are secured and compliant. This is a first in the email security world.

Aspects such as email attachments & archiving are very often ignored, even in the most comprehensive of email security frameworks. How different is Seclore's email protection solution in this regard?

Historically, long-term information governance and retention have always conflicted with encryption and rights management technologies. This creates challenges in archiving, search and indexing, and the discovery of emails. However, Seclore's rich integration and interfaces allow email archives to store unprotected copies of the information for easy search and discovery. Ready connectors allow DLP and other discovery systems to be able to "peek" inside 'Seclored' emails on the fly.

All the above makes email archiving, discovery, and DLP inspection seamless for enterprises as they seek to deploy Seclore's email security solutions.

Does Seclore provide on-premise deployments and cloud options? How would you describe Seclore's own security infrastructure?

Seclore is flexible when it comes to provisioning. Large enterprises and defence agencies use Seclore in a completely on-prem model and even in air-gapped networks. Seclore is also available in a completely cloud-hosted, managed model which enterprises can start using in less than 24 hours from the time the decision is made.

Seclore has taken extreme measures to ensure that its system and cloud infrastructure is secure. Now, with the SolarWinds and Kaseya breaches, enterprises are and should be concerned about the security of security products.

Seclore has a fundamental, built-in, security measure within its system, i.e., the content and its key never travel together. This is unlike most encryption technologies and provides an in-built security measure



SECLORE HAS A FUNDAMENTAL, BUILT-IN, SECURITY MEASURE WITHIN ITS SYSTEM, I.E., THE CONTENT AND ITS KEY NEVER TRAVEL TOGETHER. THIS IS UNLIKE MOST ENCRYPTION TECHNOLOGIES AND PROVIDES AN IN-BUILT SECURITY MEASURE IN THE SYSTEM.

in the system. This means that even if an enterprise's complete email infrastructure or the complete cloud infrastructure (e.g., M365) is compromised, the data will still be secure.

Beyond this, Seclore invests heavily in its security infrastructure to be SOC2 compliant and GDPR compliant and the underlying technology is subjected to more than 500 VAPT assessments in any year using the most advanced tools.

For enterprises and agencies concerned about hosting their security technologies with third parties/cloud, Seclore provides a completely on-prem offering that assumes no connectivity to the Internet even for upgrades and is regularly deployed in air-gapped networks.

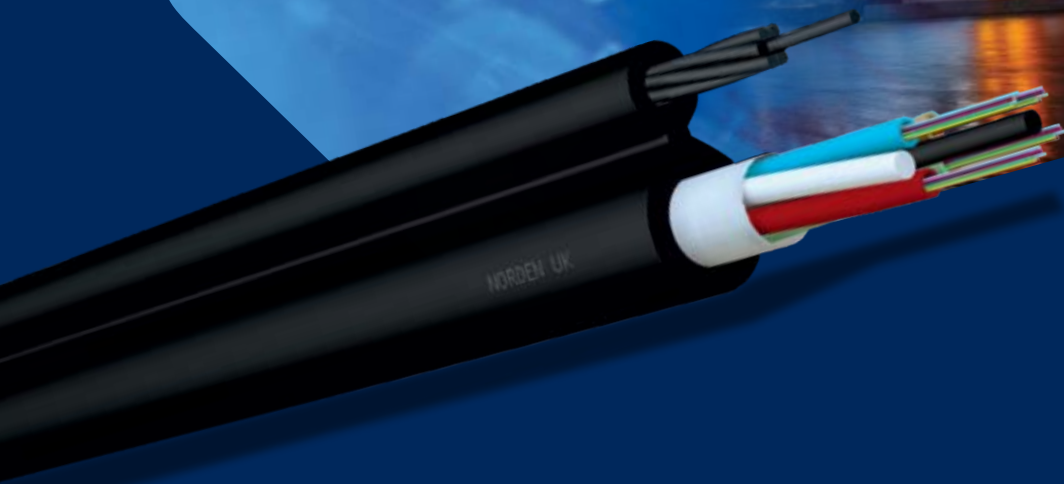
What enterprises and customers currently use Seclore?

The largest enterprises in the financial services, manufacturing, and government use Seclore to protect their data. From large global enterprises like American Express and Applied Materials to large organisations like RAK Bank, Qatar Islamic Bank, Saudi Telecom, ICICI Bank, and Allianz have chosen Seclore to protect their most confidential information. Do visit the Seclore website to hear some of the customer stories. 📖



Reliable fast connection for all...

DIELECTRIC SELF-SUPPORTING FIGURE 8-AERIAL CABLE



Dielectric Self-supporting figure 8-Aerial cable from Norden ensures protection from UV rays and other harsh environment factors. The lightweight wires also offer a good bend resistant performance making it more durable and reliable. The cables are made of standard galvanized steel and are designed for medium span aerial installations. They have ultraviolet and harsh external environment protection. Up to 12 fibres are there in each jelly filled plastic compound tube, which are stranded around a FRP strength member, water blocking tape and covered by a PE outer sheath. The upper part of figure 8 has seven number messenger wires made of stranded galvanized steel wire with PE outer sheath. They have small diameter, light weight, good bend resistance performance. The messenger cables support the fibre cables to withstand the tensile force for aerial installations. The PE outer sheath gives excellent environment and ultraviolet protection to the cable.



Norden Communication UK Ltd
Unit 13, Baker Close, Oakwood Business Park
Clacton-on-Sea, Essex, CO15 4BD, United Kingdom
Tel: +44 [0] 1255 474063, E-mail: support@norden.co.uk



www.nordencommunication.com

SONICWALL: RECORD 304.7M RANSOMWARE ATTACKS ECLIPSE 2020 GLOBAL TOTAL IN JUST 6 MONTHS



Bill Conner, president & CEO, SonicWall

In the first half of 2021, ransomware attacks skyrocketed, eclipsing the entire volume for 2020 in only six months, according to the mid-year update to the 2021 SonicWall Cyber Threat Report published today. In a new paradigm for cybercrime, SonicWall is analyzing how threat actors are using any means possible to further their malicious intent.

With high-profile attacks against established technology and infrastructure, ransomware is now more prevalent than ever. Through the first half of 2021, SonicWall recorded global ransomware volume of 304.7 million, surpassing 2020's full-year total (304.6 million) — a 151% year-to-date increase.

"In a year driven by anxiety and uncertainty, cybercriminals have continued to accelerate attacks against innocent people and vulnerable institutions," said SonicWall president & CEO Bill Conner. "This latest data shows that sophisticated

threat actors are tirelessly adapting their tactics and embracing ransomware to reap financial gain and sow discord. With remote working still widespread, businesses continue to be highly exposed to risk, and criminals are acutely aware of uncertainty across the cyber landscape. It's crucial that organizations move toward a modern Boundless Cybersecurity approach to protect against both known and unknown threats, particularly when everyone is more remote, more mobile and less secure than ever."

Ransomware running rampant

After posting record highs in both April and May, SonicWall recorded another new high of 78.4 million ransomware attacks in June 2021 alone. Ransomware volume showed massive year-to-date spikes in the U.S. (185%) and the U.K. (144%). Accounting for 64% of all recorded ransomware attacks, Ryuk, Cerber and SamSam were the top three ransomware families in the first half of the year, as recorded by SonicWall Capture Labs.

The top five regions most impacted by ransomware in the first half of 2021 were the United States, United Kingdom, Germany, South Africa, and Brazil.

"The continued rise of ransomware, cryptojacking and other unique forms of malware targeted at monetization, along with their evolution of tactics, are evidence that cybercriminal activity always follows the money and rapidly adapts to new opportunities and changing environments," said SonicWall Vice President of Platform Architecture Dmitry Ayrapetov.

In line with spikes in global data, SonicWall Capture Labs threat researchers also

recorded alarming ransomware spikes across key verticals, including government (917%), education (615%), healthcare (594%) and retail (264%) organizations.

Patented RTDMI finding, blocking more never-seen-before variants than ever

In the fight against known and unknown threats, SonicWall's patented Real-Time Deep Memory Inspection™ (RTDMI) identified record numbers of never-before-seen malware, posting a 54% year-to-date increase over the first half of 2020.

RTDMI technology blocks more advanced and unknown malware compared to traditional behavior-based sandboxing methods, and with a lower false-positive rate. This can be seen in the latest ICSCA Labs Advanced Threat Defense (ATD) Q2 test results, where the SonicWall Capture Advanced Threat Protection (ATP) service with RTDMI detected 100% of previously unknown threats with zero false positives across 33 consecutive days of testing.

In its most recent test administered in the second quarter of 2021, ICSCA conducted a total of 1,144 tests against Capture ATP, with a mixture of 544 new and little-known malicious samples and 600 innocuous applications. Capture ATP correctly identified 100% of malicious samples while allowing all clean samples through. It was the sixth consecutive ICSCA ATD certification for Capture ATP, and second 'perfect score' in as many quarters. "Third-party validation is hard earned, particularly in today's fast-moving threat landscape," said SonicWall Vice President of Software Engineering & Threat Research Alex Dubrovsky. "Consecutive perfect certifications is a testament to the SonicWall team and our continued quest

to arm organizations with intelligence and technology that help protect them from the most dangerous cyber threats.”

Malware continues to fall, non-standard port attacks down

Last year, SonicWall recorded a drop in global malware attacks, a trend that continued in the first half of 2021 with a 24% drop in malware volume worldwide. As threat actors become more sophisticated — using ransomware, cryptojacking and other types of cyberattacks to launch surgical strikes — the need for “spray-and-pray” malware attempts has lessened, decreasing overall volume.

Malware attacks via non-standard ports also fell in 2021 after hitting record highs in 2020. These attacks, which aim to increase payloads by bypassing traditional firewall technologies, represent 14% of all malware attempts in the first half of 2021, down from 24% year to date.

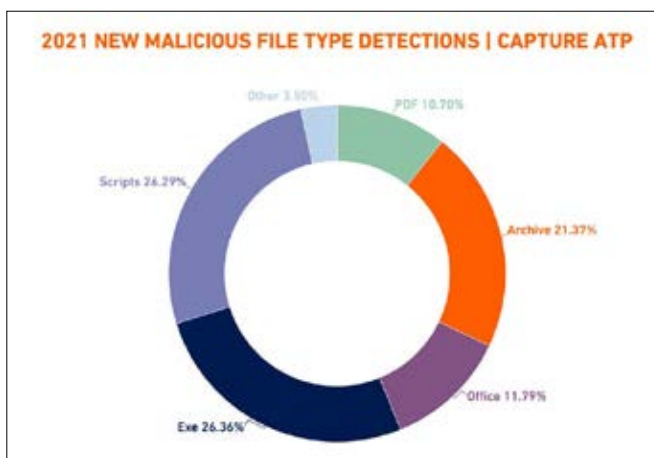
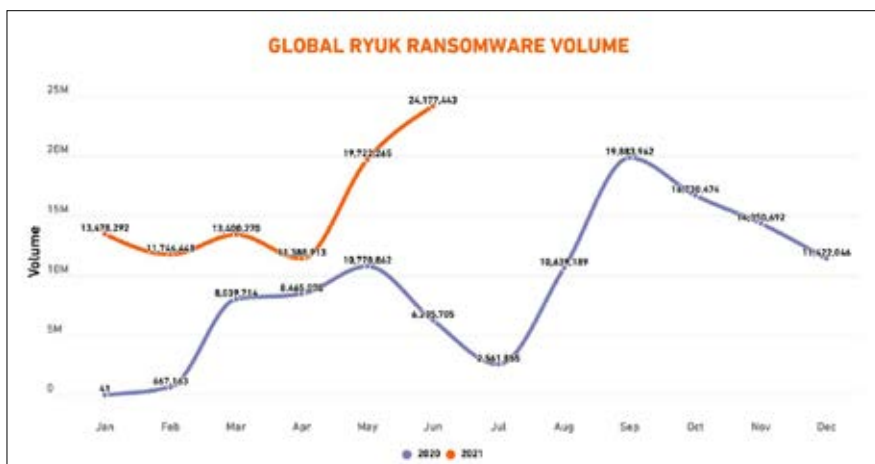
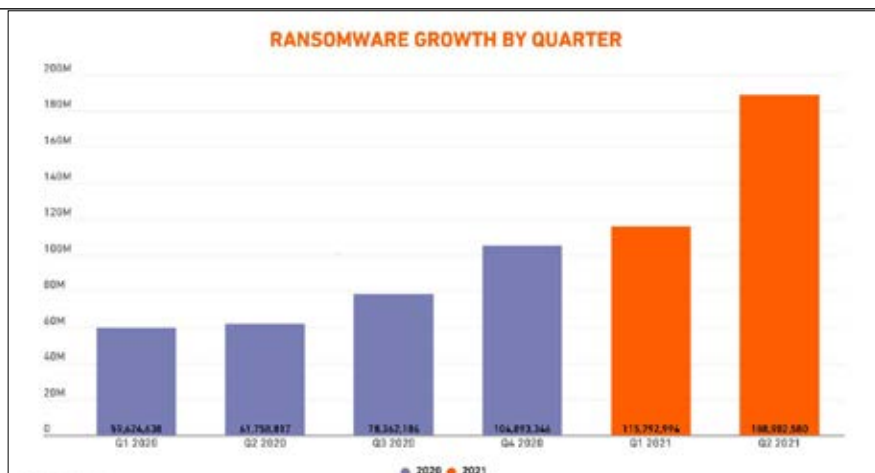
Cryptojacking malware remains a concern

After having made an unexpected revival in 2020, crypto jacking malware continued to climb through the first half of 2021 as cryptocurrency prices remain high. From January to June, SonicWall threat researchers recorded 51.1 million cryptojacking attempts, representing a 23% increase over the same six-month period last year.

Europe was particularly ravaged, recording a 248% year-to-date rise in cryptojacking malware. This increase highlights the volatile shifts of a market cybercriminals have come to leverage due to their high desire for online anonymity when it comes to lucrative payouts.

IoT vector continues to serve threats

Last year, employees packed their belongings and went home in droves, introducing millions of new devices to the network and millions of openings for cybercrime. This year, Internet of Things (IoT) malware attacks have continued to increase, rising 59% year-to-date globally,



This includes cross-vector, threat-related information shared among SonicWall security systems, including firewalls, email security devices, endpoint security solutions, honeypots, content filtering systems and the SonicWall Capture Advanced

a trend stemming back to 2018.

While the U.S. saw a slightly smaller 15% year-to-date increase in IoT malware, Europe and Asia also saw alarming rises of 113% and 190%, respectively, in IoT malware volume.

SonicWall Capture Labs threat researchers collect and analyze threat intelligence data from 1.1 million sensors in over 215 countries and territories.

Threat Protection (ATP) multi-engine sandbox; SonicWall internal malware analysis automation framework; malware and IP reputation data from tens of thousands of

firewalls and email security devices around the globe; and shared threat intelligence from more than 50 industry collaboration groups and research organizations.

LATEST HP CYBERSECURITY THREAT REPORT REVEALS HACKERS SHARING COMPUTER VISION TOOLS TO SUPERCHARGE CAPABILITIES

HP WOLF SECURITY THREAT RESEARCH TEAM FINDS INCREASING CYBERCRIME SOPHISTICATION AND A BOOM IN MONETIZATION AND HACKING TOOLS, WHILE END USERS ARE STILL VULNERABLE TO OLD TRICKS

HP Inc. has released its latest global Threat Insights Report, providing analysis of real-world cybersecurity attacks and vulnerabilities. The research shows a significant increase in the frequency and sophistication of cybercrime activity, including a 65% rise in the use of hacking tools downloaded from underground forums and filesharing websites from H2 2020 to H1 2021.

The researchers noted hacking tools in wide circulation were surprisingly capable. For example, one tool can solve CAPTCHA challenges using computer vision techniques, namely optical character recognition (OCR), in order to perform credential stuffing attacks against websites. More broadly, the report found that cybercrime is more organized than ever, with underground forums providing a perfect platform for threat actors to collaborate and share attack

tactics, techniques and procedures.

"The proliferation of pirated hacking tools and underground forums are allowing previously low-level actors to pose serious risks to enterprise security," says Dr. Ian Pratt, Global Head of Security, Personal Systems, HP Inc. "Simultaneously, users continue to fall prey to simple phishing attacks time and time again. Security solutions that arm IT departments to stay ahead of future threats are key to maximizing business protection and resilience."

Notable threats isolated by HP Wolf Security included:

Cybercriminal collaboration is opening the door to bigger attacks against victims: Dridex affiliates are selling access to breached organizations to other threat actors, so they can distribute ransomware. The drop in Emotet activity in Q1 2021 has led to Dridex becoming the top malware family isolated by HP Wolf Security.

Information stealers delivering nastier malware: CryptBot malware – historically used as an infostealer to siphon off credentials from cryptocurrency wallets and web browsers – is also being used to deliver DanaBot – a banking trojan operated by organized crime groups.

VBS downloader campaign targeting business executives: A multi-stage Visual Basic Script (VBS) campaign is sharing malicious ZIP attachments named after the executive it's targeting. It deploys a stealthy VBS downloader before using legitimate SysAdmin tools to "live off the land", persisting on devices and delivering malware.

From application to infiltration: A résumé-themed malicious spam campaign targeted shipping, maritime, logistics and related companies in seven countries (Chile, Japan, UK, Pakistan, US, Italy and the Philippines), exploiting a Microsoft Office vulnerability to deploy the commercially-available Remcos RAT

and gain backdoor access to infected computers.

The findings are based on data from HP Wolf Security, which tracks malware within isolated, micro-virtual machines to understand and capture a full infection chain and help to mitigate threats. By better understanding the behavior of malware in the wild, HP Wolf Security researchers and engineers are able to bolster endpoint security protections and overall system resilience.

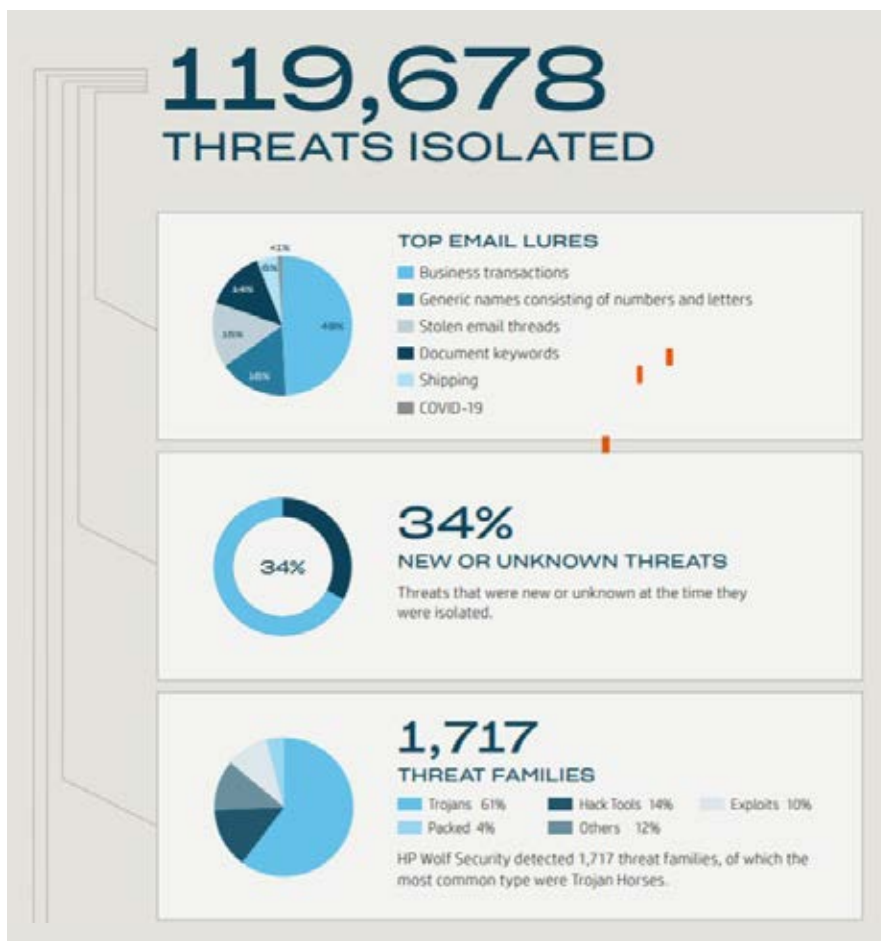
"The cybercrime ecosystem continues to develop and transform, with more opportunities for petty cybercriminals to connect with bigger players within organized crime, and download advanced tools that can bypass defenses and breach systems," observes Alex Holland, Senior Malware Analyst, HP Inc. "We're seeing hackers adapt their techniques to drive greater monetization, selling access on to organized criminal groups so they can launch more sophisticated attacks against organizations. Malware strains like CryptBot previously would have been a danger to users who use their PCs to store cryptocurrency wallets, but now they also pose a threat to businesses. We see infostealers distributing malware operated by organized criminal groups – who tend to favor ransomware to monetize their access."

Other key findings in the report include:

75% of malware detected was delivered via email, while web downloads were responsible for the remaining 25%. Threats downloaded using web browsers rose by 24%, partially driven by users downloading hacking tools and cryptocurrency mining software.

The most common email phishing lures were invoices and business transactions (49%), while 15% were replies to intercepted email threads. Phishing lures mentioning COVID-19 made up less than 1%, dropping by 77% from H2 2020 to H1 2021.

The most common type of malicious attachments were archive files (29%),



spreadsheets (23%), documents (19%), and executable files (19%). Unusual archive file types – such as JAR (Java Archive files) – are being used to avoid detection and scanning tools, and install malware that's easily obtained in underground marketplaces.

The report found 34% of malware captured was previously unknown¹, a 4% drop from H2 2020

A 24% increase in malware that exploits CVE-2017-11882, a memory corruption vulnerability commonly used to exploit Microsoft Office or Microsoft WordPad and carry out fileless attacks.

"Cybercriminals are bypassing detection tools with ease by simply tweaking their techniques. We saw a surge in malware distributed via uncommon file types like JAR files – likely used to reduce the chances of being detected by anti-malware scanners,"

comments Holland. "The same old phishing tricks are reeling in victims, with transaction-themed lures convincing users to click on malicious attachments, links and web pages."

"As cybercrime becomes more organized, and smaller players can easily obtain effective tools and monetize attacks by selling on access, there's no such thing as a minor breach," concludes Pratt. "The endpoint continues to be a huge focus for cybercriminals. Their techniques are getting more sophisticated, so it's more important than ever to have comprehensive and resilient endpoint infrastructure and cyber defense. This means utilizing features like threat containment to defend against modern attackers, minimizing the attack surface by eliminating threats from the most common attack vectors – email, browsers, and downloads." 📌

CYBER RESILIENCE- THE KEY TO SUSTAINED BUSINESS GROWTH

TAMER EL REFAEY – CHIEF CYBER SECURITY STRATEGIST, EMERGING MARKETS,
MICRO FOCUS, ON THE NEED FOR A STRONG CYBER RESILIENCE STRATEGY.



What is Cyber Resilience and why is it so important today?

Cyber Resilience

refers to an organisation's ability to respond effectively to advanced cyber and deliver intended business outcome(s) continuously, despite adverse events. Until COVID-19 struck, the crisis management plan of most organisations took into account only natural disasters, however, in the days following the pandemic and the accelerated digital transformation that followed, they recognised the need for a robust cyber resilience strategy that would help them bounce back swiftly from any kind of volatility. Today, it is well-known that cyber resilience is an invaluable asset for businesses hoping to survive and thrive, as it increases the business value of organisations and powers growth.

What are the essentials of a strong cyber resilience strategy?

A good cyber resilience strategy

must act as a “shock absorber” that prevents the crash and fall of business operations and growth plans in times of crisis. In order to do this, it must integrate three crucial capabilities: Protection, Detection and Evolution.

To protect, a cyber resilience strategy must seamlessly incorporate cybersecurity throughout the organisational security framework, so as to detect changing risk patterns and adapt to the evolving threat landscape. It should also extend complete protection across the board, securing not only data, but also the systems and applications of an organisation. Identity management plays a key role here, in ensuring that only authorised users have access to sensitive information and that their digital activity can be traced. A strong cyber resilience strategy must also detect vulnerabilities in the entire digital infrastructure including applications and guarantee privacy and the highest levels of security.

The second aspect of a good cyber resilience strategy is detection: the ability to identify a malicious attack when it happens. This is more challenging than it sounds, because cyber criminals are becoming more and more sophisticated and hide themselves in more clever ways so that they can attack with greater force. Here, it must be remembered that advanced threats don’t always originate outside. In fact, some of the more serious ones happen within an organisation. Wherever it begins, threat actors use the time between breach detection and containment to steal and destroy data, and also attack the entire IT network of an organisation, without anyone noticing.

To be able to detect attacks and

vulnerabilities on time, companies must fully understand their data ecosystem: what the data contains and where it resides. This is an important step in managing sensitive information and tackling issues such as non-compliance and/or theft. Security teams must also understand the behaviour patterns of individual users and recognise what constitutes “normal” behaviour, so that anything “abnormal” or “suspicious” can be quickly identified.

It is a fact that most security teams struggle with detection because there is so much data generated and so many solutions available, that may lead to multiple “false positives,” which make it difficult to determine what and where the actual threat is. That is why it is important for a good cyber-attack detection solution to evaluate every alert and add necessary context and to provide security teams with high quality leads to respond accordingly.

Evolution is another crucial aspect of a robust cyber resilience strategy—the ability to continuously evolve its security stance to stay ahead of threats. Hackers are well aware that no attack should be repeated because there will certainly be a fix for anything that has happened until then. A cyber-resilient organisation will be able to predict new attack patterns and put up a solid defence before it becomes a full-blown crisis. Thanks to concepts like unsupervised machine learning and security orchestration and automation, organizations can cope with the ever-changing attack landscape.

How does Micro Focus help businesses strengthen their cyber resilience infrastructure?

Micro Focus has a suite of data

A GOOD CYBER RESILIENCE STRATEGY MUST ACT AS A “SHOCK ABSORBER” THAT PREVENTS THE CRASH AND FALL OF BUSINESS OPERATIONS AND GROWTH PLANS IN TIMES OF CRISIS.

security products that strengthen cyber resilience and help organisations adopt a zero-trust approach, combining data security with information governance use cases for buyers and customers. Some of our products include Smart Cipher, CyberRes Data Security solutions, File Analysis Suite, Content Manager, Voltage Data Privacy and Protection solutions.

For instance, CyberRes Data Security solutions provide an end-to-end data-centric approach to enterprise data protection, thereby enhancing the cyber resilience infrastructure of organisations. The Voltage Data Privacy and Protection platform allows data-centric protection and the flexible implementation of different kinds of data in any language and region, with accuracy and scalability.

Our passion is to help customers add value to their business by strengthening their cyber resilience infrastructure. Our solutions help businesses fight even the most advanced of threats and keep the lights on while growing and thriving at all times. 🌟

DEFENDERS BENEFIT FROM AN 'AIR TRAFFIC CONTROL SYSTEM' THAT SEES ALL NETWORK ACTIVITY, REVEALS UNKNOWN AND UNPROTECTED ASSETS, AND EXPOSES EVASIVE MALWARE MORE RELIABLY THAN INTRUSION PROTECTION SYSTEMS (IPS).

Joe Levy chief technology officer, Sophos

SOPHOS ACQUIRES BRAINTRACE TO BOOST ADAPTIVE CYBERSECURITY ECOSYSTEM

IT PROVIDES VISIBILITY INTO SUSPICIOUS NETWORK TRAFFIC PATTERNS, ADDING NOVEL THREAT INTELLIGENCE TO SOPHOS' FAST-GROWING MANAGED THREAT RESPONSE & RAPID RESPONSE SERVICES, XDR TECHNOLOGY & DATA LAKE.

Sophos, a global leader in next-generation cybersecurity, has announced that it has acquired Braintrace, further enhancing Sophos' Adaptive Cybersecurity Ecosystem with Braintrace's proprietary Network Detection and Response (NDR) technology. Braintrace's NDR provides deep visibility into network traffic patterns, including encrypted traffic, without the need for Man-in-the-Middle (MitM) decryption. Located in Salt Lake City, Utah, Braintrace launched in 2016 and is privately held.

As part of the acquisition, Braintrace's developers, data scientists and security analysts have joined Sophos' global Managed Threat Response (MTR) and Rapid Response teams. Sophos' MTR and Rapid Response services business has expanded rapidly, establishing Sophos as

one of the largest and fastest-growing MDR providers in the world, with more than 5,000 active customers.

Braintrace's NDR technology will support Sophos' MTR and Rapid Response analysts and Extended Detection and Response (XDR) customers through integration into the Adaptive Cybersecurity Ecosystem, which underpins all Sophos products and services. The Braintrace technology will also serve as the launchpad to collect and forward third-party event data from firewalls, proxies, virtual private networks (VPNs), and other sources. These additional layers of visibility and event ingestion will significantly improve threat detection, threat hunting and response to suspicious activity.

"You can't protect what you don't know is there, and businesses of all sizes often miscalculate their assets and attack surface, both on-premises and in the

cloud. Attackers take advantage of this, often going after weakly protected assets as a means of initial access. Defenders benefit from an 'air traffic control system' that sees all network activity, reveals unknown and unprotected assets, and exposes evasive malware more reliably than Intrusion Protection Systems (IPS)," said Joe Levy, chief technology officer, Sophos. "We're particularly excited that Braintrace built this technology specifically to provide better security outcomes to their Managed Detection and Response (MDR) customers. It's hard to beat the effectiveness of solutions built by teams of skilled practitioners and developers to solve real world cybersecurity problems."

Sophos will deploy Braintrace's NDR technology as a virtual machine, fed from traditional observability points such as a Switched Port Analyzer (SPAN) port or a network Test Access Point (TAP) to inspect both north-south traffic at boundaries or east-west traffic within networks. These deployments help discover threats inside any type of network, including those that remain encrypted, serving as a complement to the decryption capabilities of Sophos Firewall. The technology's packet and flow engine feeds a variety of machine learning models trained to detect suspicious or malicious network patterns, such as connections to Command and Control (C2) servers, lateral movement and communications with suspicious domains. Since Braintrace built its NDR technology specifically for predictive, passive monitoring, its engine also provides intelligent network packet capture that IT security administrators and threat hunters can use as supporting evidence during investigations. The novel NDR analysis and prediction technique is patent pending.

Sophos plans to introduce Braintrace's NDR technology for MTR and XDR in the first half of 2022. 📌



SECURITY-THE HYBRID WAY

HYBRID CLOUD INFRASTRUCTURE IS THE TREND NOW. IN FACT, RESEARCH SHOWS THAT AROUND 40% OF BUSINESSES NOW USE HYBRID CLOUD AND THAT THIS FIGURE IS EXPECTED TO RISE BY THE END OF THE YEAR. THEREFORE, IT FOLLOWS THAT SECURING THE HYBRID CLOUD REQUIRES A HYBRID APPROACH, FOR MAXIMUM EFFECTIVENESS. SO, HOW DOES IT HAPPEN? WE SPEAK TO THE EXPERTS TO FIND OUT.

A hybrid approach to security is one that tightly integrates SaaS solutions with an enterprise's existing IT infrastructure. How will this approach ensure maximum security in a space where hacking is getting extremely sophisticated?

ACCELERATED MULTI-CLOUD ADOPTION IS RENDERING TRADITIONAL PRIVATE NETWORKS LESS RELEVANT AS THERE'S LESS NEED TO BACKHAUL TRAFFIC BACK TO CORPORATE DATA CENTERS.

Alain Penel
Regional Vice-President, Middle East & Pakistan at Fortinet



As organizations continue to accelerate their digital innovation initiatives, it is important to adopt an effective security design as new network edges are introduced to the security infrastructure – from data center, LAN, SASE and more.

One of the most profound changes lately has been the increased adoption of cloud-based infrastructures, SaaS applications and services, and the need to provide fast, flexible and secure connections to these resources to any user on any device in any location. We've seen a greater appreciation for a hybrid approach and we are now seeing companies creating a mix of on-prem and cloud environments. Accelerated multi-cloud adoption is rendering traditional private networks less relevant as there's less need to backhaul traffic back to corporate data centers. Indeed, remote workers, branch offices and headquarters locations are increasingly directly connecting to multiple clouds and SaaS providers.

This new distributed network, including the new home office and transformed branch office, has added another layer of complexity. The model moving forward focuses on the user or the entity sitting on some local area network (LAN), reaching across a wide area network

(WAN) to access resources from multiple clouds. As the platform, infrastructure and software become more distributed and disaggregated, it's clear that security and networking have to be integrated and automated across the LAN, WAN and cloud edges. In addition, security should come in multiple form factors and consumption models to suit an organization's unique requirements.

Amit Hooja, NetGraph
CEO, NetGraph



With digital transformation becoming the cornerstone of most organizations, increasing work from home environments, stupendous loads of data being transferred in today's world is also an environment where the number of data security attacks have not only increased, but have also become more advanced. This calls for an even greater need for organizations to ensure that their data is protected to ensure that they can run their businesses unhindered.

Although a lot of SaaS is being increasingly incorporated in most business processes, what we are seeing are increased specializations that are arising both as App based and or API, where certain business processes are better handled by specialized companies. However, both service

providers as well as end-users must be able to understand the pros and cons of the vendors they work with.

One of the biggest challenges is integrating SaaS apps within existing IT infrastructure, as more often they are geared to be specialized problem solvers. Having said that, Most SaaS companies are better equipped to handle the security events and avert sophisticated hacks.

Integration across disparate platforms may require several protocol conversions at the data layer and hence opens up doors for hackers to get in. For SaaS integrations to be effective they must implement security at multiple layers including IP restrictions, API security keys, and must have the right processes to ensure that data flow needs are adequately monitored for proper usage, while any abnormal data selections must generate appropriate alerts.

Most SaaS platforms are web delivered and removes the need of installation of any client level software. It is however, very critical that organizations are aware of the need to have regular updates and patches.

As a part of our Managed Security Service offerings at NetGraph, we

FOR SAAS INTEGRATIONS TO BE EFFECTIVE THEY MUST IMPLEMENT SECURITY AT MULTIPLE LAYERS INCLUDING IP RESTRICTIONS, API SECURITY KEYS AND MUST HAVE THE RIGHT PROCESSES TO ENSURE THAT DATA FLOW NEEDS ARE ADEQUATELY MONITORED FOR PROPER USAGE.

constantly review the integration architectures for any security loop holes, provide SaaS vendor security audits and ensure that there are no leakages at the partner level. We also tackle monitoring for data access usages and build patterns on right use of data.

Rohit Bhargav
Practice Head - Cloud & Security,
Cloud Box Technologies



Cyberattacks have evolved dramatically in the past couple of decades regarding their capabilities, scope, fallout, number of targets. CIOs and CISOs are now pressured to prioritize cybersecurity and shift budget to acquiring additional security solutions making sure that they are resilient to cyberattacks.

Testing the cybersecurity posture of organizations is becoming a top priority, it triggered an increased demand for the latest and most comprehensive testing solutions. The three pillars under Gartner Breach and Attack simulations are insider threat, lateral movement and data exfiltration using continuous and consistent testing. There are no siloed environments. We are using SaaS business application in business and it needs a solution that takes 360-degree approach to protect all the 3 verticals keeping data protection at the core.

[illegible]

threats in the network. This ability can be leveraged best when organisations use on-premises DNS servers to block access to domains based on alerts from the threat intel platform and when they further improve the threat assessment model based on the wide range of threat data available in the cloud.

Hybrid solutions also offer granularity and visibility over the organisational network. User activities within the on-premises network are continuously shared with the SaaS component of the solution, and indicators of compromise detected by the SaaS tool are immediately forwarded to the on-premises SOC. Based on these inputs, the organisation's security infrastructure (on-premises or in the cloud), including IAM, endpoint security, and SIEM solutions, triggers the automated incident response.

Preventing today's sophisticated threats involves strengthening the defenses of three components: users, processes, and technology. The hybrid approach is key to ensure that organisations are "incident-response-ready" for both known and unknown attacks. 📌

TESTING THE CYBERSECURITY POSTURE OF ORGANIZATIONS IS BECOMING A TOP PRIORITY, IT TRIGGERED AN INCREASED DEMAND FOR THE LATEST AND MOST COMPREHENSIVE TESTING SOLUTIONS.



Sanjeev Walia

UNDERSTANDING CYBERSECURITY

SANJEEV WALIA, FOUNDER & PRESIDENT, SPIRE SOLUTIONS, ON THE CYBERSECURITY LANDSCAPE AND THE GROWTH TRAJECTORY OF THE ORGANIZATION.

How has the pandemic impacted the cybersecurity industry? Research and statistics show that the pandemic has accelerated digital transformation on one hand and introduced many critical cybersecurity challenges to governments and enterprises on the other.

Some organizations quickly recognized cybersecurity as a pain

point and have been addressing it proactively to ensure business or service continuity. While others are slowly accepting this reality with the help of lots of education and awareness on the types of risks their organizations may be vulnerable to.

Now that the people, processes, data, and technology are distributed everywhere, more so due to trends like work from home, CISOs have a

much harder task in hand so they are proactively seeking collaboration with solution providers. Also, the board and broader C-suite are now keenly participating in cybersecurity discussions, a change that was much needed.

Are there any new cyberattacks/ threat trends that organizations in the region must be aware of, especially in the last year since the pandemic?

We believe that the types of risks and number of attacks will continue to be on the rise as cybercriminals are constantly changing their tactics, techniques, and procedures and finding innovative ways to fulfill their motives.

Endpoints, networks, and humans are being targeted using various methods such as malware, ransomware, phishing, social engineering, and more. Brand and VIP impersonation is also on the rise.

There may not be a silver bullet perse, but areas such as security data lakes, data analytics, automation, threat hunting, threat intelligence, attack path visualization, human risk management, and SOC optimization will help CISOs in getting an edge over threat actors.

Have you recently launched any new products or made any announcements?

We have had several positive developments over the last few months such as exclusive partnerships with the likes of XM Cyber for attack path visualization and security validation platform; Outthink for cybersecurity human risk management; and Nemesysco for layered voice analysis for personality testing.

Additionally, we launched Spire Data - our bespoke big data and analytics business unit – as we believe that heightening security is directly dependent on data and analytical ability.

What industry events are you partaking in this year and what are your key objectives?

We have been supporting GISEC since its inception and concluded this year's edition successfully as their



Official Distribution Partner. Towards the end of the year, we will be at @Hack in Saudi Arabia as one of their first Strategic Partners. @Hack is held in partnership with the iconic

Blackhat and Saudi Federation For Cybersecurity, Programming, and Drones (SAFCSP). GITEX is also on the cards.

Our primary objective for these events is to show solidarity with the Middle East & Africa's fight against cybercrimes. Our primary expectation from events like these is a good quality audience to showcase our product capabilities to customers, connect with new technology partners, and reconnect with our channel partner ecosystem.

Is there anything else you would like to add?

Cybersecurity for the community is a collective responsibility and a regional priority so we welcome customers, technology partners, channel partners, media, and generally the whole cybersecurity ecosystem to reach out to us for any possible collaboration. 🙋

WE BELIEVE THAT THE TYPES OF RISKS AND NUMBER OF ATTACKS WILL CONTINUE TO BE ON THE RISE AS CYBERCRIMINALS ARE CONSTANTLY CHANGING THEIR TACTICS, TECHNIQUES & PROCEDURES AND FINDING INNOVATIVE WAYS TO FULFILL THEIR MOTIVES.

MIMECAST LAUNCHES AI- ENABLED SOLUTION FOR EVASIVE EMAIL THREATS

■ THE MIMECAST CYBERGRAPH™ SOLUTION USES AI TO HELP IMPROVE DETECTION AND REDUCE RISK

Mimecast Limited, a leading email security and cyber resilience company, today announced the Mimecast CyberGraph™ solution, a new add-on for Mimecast Secure Email Gateway (SEG) that is engineered to use Artificial Intelligence (AI) to help detect sophisticated phishing and impersonation attacks. CyberGraph creates an identity graph which is built to store information about relationships between all senders and recipients. The graph is designed

to detect anomalies and leverages machine learning technology to help organizations stay one step ahead of threat actors by alerting employees to potential cyber threats.

"Phishing and impersonation attacks are getting more sophisticated, personalized and harder to stop. If not prevented, these attacks can have devastating results for an enterprise organization," said Josh Douglas, VP, Product Management for Threat Intelligence at Mimecast. "Security controls need to be constantly updated and improved to outsmart threat

CYBERGRAPH LEVERAGES OUR AI AND MACHINE LEARNING TECHNOLOGIES TO HELP KEEP EMPLOYEES ONE STEP AHEAD WITH REAL-TIME WARNINGS, DIRECTLY AT THE POINT OF RISK.

actors. CyberGraph leverages our AI and machine learning technologies to help keep employees one step ahead with real-time warnings, directly at the point of risk. What makes this exciting is that we are embedding the technology for existing email security customers, they do not need to look for other vendors to fill the gap with technologies that only work to solve part of this challenge.”

The workplace is always the top target of cybercriminals, but in the remote working era, the problem has intensified. “The State of Email Security Report” found that email threats rose by 64% and employees are clicking on three times as many malicious emails as they had before the COVID-19 pandemic. Security controls need to evolve to help evade cybercriminals’

relentless and crafty approach. CyberGraph includes three key capabilities engineered to help prevent cyber threats:

Receivers embedded trackers useless – During the reconnaissance phase of an attack, threat actors embed trackers into emails that communicate with an illegitimate remote server, disclosing important information that can be used to create a targeted social engineering attack. CyberGraph is built to block this communication, mask the email recipient’s location, and prevents attempts to understand engagement levels with the email content.

Uses machine learning to protect from targeted email threats – CyberGraph is designed to create an identity graph by learning

about relationships and connections between all senders and recipients. This intelligence is combined with the outputs from machine learning models to detect anomalies that could be indicative of a malicious email.

Engages users with contextual, dynamic warning banners – CyberGraph is engineered to engage users at the point of risk with color-coded banners that indicate the potential nature of a threat. Users are empowered by seeing whether an email is safe or potentially nefarious. CyberGraph is built to “crowd-source” threat intelligence, which helps to reinforce the machine learning model. As the risk associated with any given delivered email changes, banners embedded in any similar emails are updated with the latest information, providing ongoing engagement and protection for users. 🔒



Josh Douglas, VP, Product Management
for Threat Intelligence at Mimecast

SECURING THE CLOUD

ANITA JOSEPH CAUGHT UP WITH **RAM NARAYANAN**, COUNTRY MANAGER, CHECK POINT SOFTWARE TECHNOLOGIES, MIDDLE EAST, TO FIND OUT MORE ABOUT CLOUD SECURITY.



Ram Narayanan, Country Manager, Check Point Software Technologies, Middle East

What are some of the security risks of cloud computing? What would you say is the biggest threat

faced by businesses in the region.

Cloud computing security is an organization's approach to protecting the cloud-based resources. This includes both security solutions deployed to protect the organization's cloud deployment and the policies and procedures put in place to define how cloud-based systems and data are protected. However, cloud-based environments differ from the on-premises ecosystems that organizations are accustomed to protecting. These differences create various cloud security challenges and threats such as misconfiguration of the cloud platform followed by unauthorized cloud access, insecure interfaces and hijacking of accounts. We are now experiencing the 5th generation of cyberattacks: large scale, multi-vector, mega attacks targeting businesses, individuals, and countries. Businesses are trying to protect their IT environments against current attacks with traditional security technologies. They are stuck in the world of 2nd and 3rd generation security, which only protects against viruses, application attacks, and payload delivery. Although there is a rise in cyber attacks in general such as phishing attacks, spear phishing, man in the middle (MitM) attacks, denial of service or distributed denial of service (DDoS), ransomware is emerging as one of the biggest threats to enterprise cybersecurity.

Tell us more about Check Point Software Cloud Security. How is it different from the other cloud security offerings in the market?

Check Point Software Technologies offers broad and deep multi-layer security to protect customers at all stages of their cloud journey. Through the unified platform of Check Point CloudGuard we offer consolidated security, threat prevention and posture management across all public,

private and hybrid cloud environments, assets and workloads from foundational cloud network security and continuous compliance, through cloud workload and cloud applications security (WAAP) for containers and serverless functions, as well as cloud intelligence and threat hunting. Aligned with the agile nature of cloud development and deployment, Check Point CloudGuard delivers the ultimate solution for both cloud security practitioners and cloud DevOps:

Check Point Cloud Guard Network Security for advanced threat prevention and automated cloud network security through a virtual security gateway, with unified security management across all multi-cloud and on-premises environments.

Check Point CloudGuard Security Posture Management, which automates governance across multi-cloud assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks.

Check Point CloudGuard Workload Protection, which provides seamless vulnerability assessment, and delivers full protection of modern cloud workloads, including serverless functions and containers, from code to runtime – automating security with minimal overhead.

Check Point CloudGuard Application Security, which automates application security and API protection with AppSec powered by contextual AI, and stops attacks against your web applications with a fully automated, cloud native application security solution.

Check Point CloudGuard Cloud Intelligence, which provides cloud native threat security forensics through rich, machine learning visualization, giving real-time context of threats and anomalies across your multi-cloud environment.

What are some of the other cybersecurity products and solutions that Check Point Software offers?

Check Point Software Technologies offers a complete security architecture defending enterprises from networks to mobile devices in addition to the most comprehensive and intuitive security management. Our mission is to provide any organization with the ability to conduct their business on the internet with the highest level of security. Check Point Software has taken over 80 products and technologies and organized them into three main pillars:

Check Point Harmony protects remote employees, their devices and their internet connectivity from malicious attacks, while ensuring secure, remote

**CHECK POINT OFFERS
A COMPLETE SECURITY
ARCHITECTURE
DEFENDING
ENTERPRISES FROM
NETWORKS TO
MOBILE DEVICES, IN
ADDITION TO THE MOST
COMPREHENSIVE AND
INTUITIVE SECURITY
MANAGEMENT.**

Zero-Trust access at any scale to any corporate application,

Check Point Quantum which is the most complete network security solution for every organization, perimeter, and datacenter, encompassing IoT Nano-Security to Terabit super-networks.

Check Point CloudGuard sets the gold standard for securing critical cloud workloads, both public and private. It offers cloud posture management, serverless security, and a new generation of Web Application Firewalls powered by contextual AI that secures APIs, Web applications as well as hosted and on premise web servers.

Check Point Software Infinity-Vision is our unified management platform which controls Check Point Software Harmony, Check Point CloudGuard and Check Point Quantum. Powered by the world's largest threat intelligence network, Check Point Infinity-Vision centrally manages organizations' security architectures to mitigate attacks effectively in real time, close security gaps, and reduce total cost of ownership. It consolidates management of multiple security layers, providing superior policy efficiency and enabling teams to manage the security of the entire enterprise through a single pane of glass, spanning networks, cloud, mobile, endpoint, and IoT devices.

How is Check Point Software positioning itself in today's fast-growing, changing and evolving market? What is your approach and strategy here?

Check Point Software Technologies is making Internet communications and critical data secure, reliable and available everywhere. The focus is on real customer needs and to develop new and innovative security solutions that redefine the security to ensure that they are effectively protecting their assets and data from 5th generation cyber attacks. Automation is key – it is important to ensure the ease of use and support for automation at every stage of the security and development process. The earlier organizations enable security in the development cycle the more they can reduce the risk and cost of mistakes. We address organizations' most imminent cyber security needs based on three core principles:

Prevention-first approach - deploy pre-emptive user protections to eliminate threats before they reach the users.

Gold Standard Management – single pane of glass to manage the entire security estate.

Consolidated Solution - realize complete, pre-emptive protection against the most advanced threats while achieving better operational efficiency. 🏠

ESET CEMENTS 'CHAMPION' STATUS IN CANALYS GLOBAL CYBERSECURITY LEADERSHIP MATRIX 2021

THE 2021 CYBERSECURITY LEADERSHIP MATRIX ASSESSED 19 CYBERSECURITY VENDORS ON THEIR GLOBAL CHANNEL AND MARKET PERFORMANCE OVER THE LAST 12 MONTHS.



Ignacio Sbampato, ESET

ESET, a global leader in cybersecurity, has achieved 'Champion' status for the third year in a row in the latest Global Cybersecurity Leadership Matrix from Canalys, improving upon its 2020 matrix position with a focus on investment in enterprise services and partner training.

Canalys is a leading global technology market analyst firm with a distinct channel focus, and strives to guide clients on the future of the technology industry and to think beyond the business models of the past.

The 2021 Cybersecurity Leadership Matrix assessed 19 cybersecurity vendors on their global channel and market performance over the last 12 months. The Leadership Matrix combines partner feedback from Canalys' Vendor Benchmark tool with an independent analysis of each vendor's

momentum in the channel based on their investments, strategy, market performance and execution.

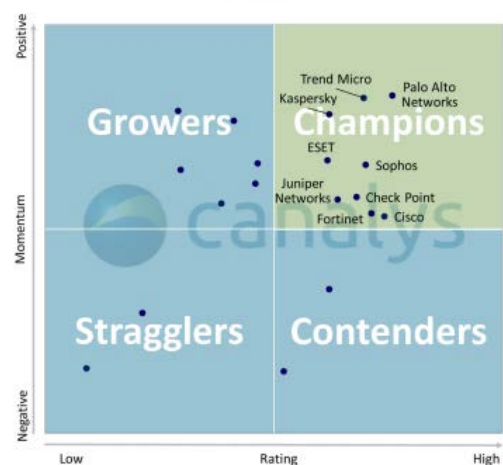
According to Chief Analyst Matthew Ball at Canalys, "ESET's technical support, account management and overall ease of doing business was rated the highest by its partners. It continued to invest in increasing its presence in enterprise accounts and enhanced its Global Managed Service Provider Program with the release of its EMA2 marketplace platform."

ESET MSP Administrator 2 (EMA2) is a license management system for managed service providers (MSPs) that both extends access to ESET's more advanced portfolio and integrates with third-party tools through an application programming interface.

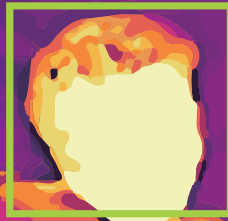
ESET was awarded Champion status with eight other vendors. Champions have the highest scores in the Canalys Vendor Benchmark and exhibit common characteristics, including making improvements to and simplifying channel processes, and demonstrating commitment to growing partner-generated revenue. Champions must also show that they are making sustainable investments in the future of their channel models, including channel programs and initiatives.

Ignacio Sbampato, chief business officer at ESET, commented: "Since our inception we have kept the same values and approach towards the channel, continuously improving our resources and tools to help our partners develop their Cybersecurity business and protect their customers from all types of threats and we are proud to see they continue to recognize the quality of our products and services. It is rewarding to know that our partners rate us highly and value the investments we have made in our platforms and systems. A safer internet experience for all is central to our core mission, and without a strong relationship with partners we would not have been able to achieve this." 🏆

Global Cybersecurity Leadership Matrix
June 2021



36.5° C



Hikvision Temperature Screening Thermal Solutions

SAFER, FASTER, SMARTER



Contact-free



Multi-person detection



1s measurement



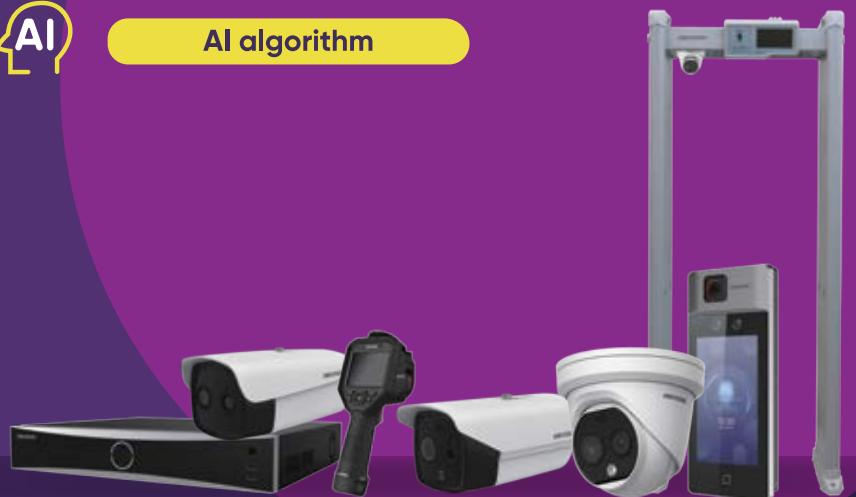
AI algorithm

Thermographic
Cameras

MinMoe Terminals

Metal Detector Door

DeepinMind NVRs



Temperature Screening
Thermal Cameras

For more information, please scan the QR-Code to visit
our Temperature Screening Thermal Solution page.

HIKVISION

www.hikvision.com



Hossam Seif El Din, General Manager
IBM in the Middle East and Pakistan

DATA BREACH COST HITS RECORD HIGH DURING PANDEMIC: IBM REPORT



AVERAGE COST PER DATA BREACH INCIDENT IN THE UAE
AND SAUDI ARABIA STANDS AT \$6.93 MILLION.

BM Security has announced the results of a global study, based on in-depth analysis of over 500 real-world data breaches occurring over the past year across 17 countries, including the Middle East region, and among 17 different industries. According to the study, the Middle East region is the second highest average breach cost amongst the 17 regions studied.

The study on organizations surveyed in the Kingdom of Saudi Arabia (KSA) and the United Arab Emirates (UAE) suggests that security incidents became more costly and harder to contain due to drastic operational shifts during the pandemic. The financial impact of these security incidents in the Middle East has risen by 6% over the past year and has reached the highest cost in the report's 8-year history in the region. These data breaches cost companies studied in the region \$6.93 million per breach on average, which is higher than the global average of \$4.24 million per incident.

Businesses were forced to quickly adapt their technology approaches last year, with many companies encouraging or requiring employees to work from home, and 60% of organizations moving further into cloud-based activities during the pandemic. The new findings released today suggest that security may have lagged behind these rapid IT changes, hindering organizations' ability to respond to data breaches.

The annual Cost of a Data Breach Report, conducted by Ponemon Institute and sponsored and analyzed by IBM Security, identified the energy sector, financial services, and healthcare as the top three

BUSINESSES WERE FORCED TO QUICKLY ADAPT THEIR TECHNOLOGY APPROACHES LAST YEAR, WITH MANY COMPANIES ENCOURAGING OR REQUIRING EMPLOYEES TO WORK FROM HOME AND 60% OF ORGANIZATIONS MOVING FURTHER INTO CLOUD-BASED ACTIVITIES.

industries per record cost of a data breach in the Middle East region. The study also found that breaches cost companies surveyed in Saudi Arabia and the UAE \$194 per lost or stolen record on average. While phishing attacks were the most common root cause of breaches that target organizations in the region, followed by stolen user credentials such as name, email and password.

"The rapid adoption of digitization in the Middle East has made the region an attractive target for a wide array of cyber threats, and this has also been intensified by the pandemic," says Hossam Seif El Din, General Manager IBM in the Middle East and Pakistan. "As cybercriminals became increasingly sophisticated, IBM is uniquely prepared to support complex security challenges for governments and businesses of all sizes and across all industries in our region".

Businesses That Modernized Had Lower Breach Costs

While certain IT shifts during the pandemic increased data breach costs, organizations surveyed in Saudi Arabia and the UAE who said they did not implement any digital transformation projects to modernize their business operations during the pandemic actually incurred higher data breach costs. The cost of a breach was 10% higher than average at organizations that had not undergone any digital transformation due to COVID-19.

Companies studied that adopted a zero-trust security approach were better positioned to deal with data breaches. This approach operates on the assumption that user identities or the network itself may already be compromised, and instead relies on AI and analytics to continuously validate connections between users, data and resources. Organizations in KSA and UAE with a mature zero trust strategy had an average data breach cost of \$5.6 million – which was \$2.4 million lower than those who had not deployed this approach at all.

Methodology and Additional Data Breach Statistics

The 2021 Cost of a Data Breach Report from IBM Security and Ponemon Institute is based on in-depth analysis of real-world data breaches of 100,000 records or less, experienced by over 500 organizations worldwide between May 2020 and March 2021. The report takes into account hundreds of cost factors involved in data breach incidents, from legal, regulatory and technical activities to loss of brand equity, customers, and employee productivity. 🔑

RANSOMWARE, PHISHING, ZERO TRUST AND THE NEW NORMAL OF CYBERSECURITY



BABUR NAWAZ KHAN,
TECHNICAL MARKETING
ENGINEER, A10 NETWORKS

When the COVID-19 pandemic struck, cyber criminals saw their opportunity, and they took it. With corporate offices, government agencies, schools, and universities shifting from in-person to remote work models, and even many healthcare interactions moving online, the rushed nature of the transition led to inevitable cyber security gaps. Consumer broadband and personal devices undermined the corporate security stack; unsafe user practices and overlooked security patches opened ample vulnerabilities throughout the environment.

Meanwhile, an anxious and often confused public proved easy prey for phishing attacks. The impact was all too predictable: phishing attacks, DDoS attacks, and ransomware attacks all spiked. Eighty percent of firms saw an increase in incidents in 2020, and the COVID-19 pandemic was blamed for a 238 percent rise in cyber attacks on banks. Phishing has jumped 600 percent since the end of February 2020.

Why Ransomware Attacks and Costs are Soaring

The pandemic-driven surge in ransomware was immediate and dramatic. Ransomware attacks rose 148 percent in March 2020, with average payments up 33 percent to \$111,605 compared with Q4 2019—and reaching \$170,000 by Q3 2020.

While the rise in ransomware strikes likely resulted in part from greater opportunities for hackers, combined with the increased effectiveness of phishing attacks targeting news-obsessed users, a change in tactics may also have played a role. While earlier attacks generally focused on the traditional encryption-payment-decryption ransomware model, hackers are now seeking to increase their returns through data exfiltration, stealing data and offering it for sale on the black market.

For ransomware victims such as government agencies, corporations, healthcare systems, and universities, the growth in data exfiltration can compound the already considerable damage of a ransomware attack beyond the ransom itself, potentially including violations of customer privacy, the loss of corporate data, and massive regulatory fines. Add to this hidden costs such as system downtime, reduced efficiency, incidence response costs, and brand and reputation damage—bringing total global costs to more than \$1 trillion each year.

Taking Data Protection Inside the Perimeter with Zero Trust

In the era of public cloud, mobility, and work-from-home, the notion of perimeter security has quickly become outdated. It's not just that the attack surface has changed; organizations have also gained a new understanding of the identity of potential attacker, including trusted insiders who don't even realize that they're abetting a crime. It's common

IT'S NOT JUST THAT THE ATTACK SURFACE HAS CHANGED; ORGANIZATIONS HAVE ALSO GAINED A NEW UNDERSTANDING OF THE IDENTITY OF A POTENTIAL ATTACKER, INCLUDING TRUSTED INSIDERS WHO DON'T REALIZE THAT THEY'RE ABETTING A CRIME.

to think of an internal threat actor as a disgruntled employee or spy undermining cyber security with ill intent, but it's even more common for a well-meaning employee to inadvertently open the door to hackers through poor password hygiene, nonsecure practices, or the ever-popular phishing lure.

While awareness and education can help lessen the risk of successful phishing and ransomware attacks, a single moment of inattention and carelessness can be enough to devastate the business. It's safer to assume that anyone, even a trusted user with a heart of gold, can pose a security risk, and design your cyber defense strategy accordingly. Hence the rise of Zero Trust—the notion that we shouldn't trust anything or anyone, inside or outside the network, with access to our computer systems. In practice, this means measures such as:

Moving beyond the idea of inside versus outside and redesigning cyber defense in terms of secure micro-parameters, with multiple points of network defense

Implementing the ability to control, inspect, and restrict network traffic traveling in any direction—north-south or

east-west—within your organization

Subjecting users to checks and balances, each time they cross into a different area of the network or try to access a new set of resources, to verify their need and privileges

Ensuring timeliness and preventing excess privileges from accumulating by periodically revoking and refreshing access and credentials

Continuously monitoring who's accessing what and the level of risk these activities might present

Why SSL Inspection is Critical for Zero Trust

As organizations move to implement Zero Trust, they quickly run into the issue of visibility in a world of pervasive TLS/SSL encryption. To enable fast threat detection and response times, it's essential to be able to decrypt, inspect, and re-encrypt network traffic quickly and efficiently at scale without impairing cost or adding complexity. A centralized, dedicated SSL decryption capability makes it possible to provide visibility into network traffic for each element of the cyber security stack without the inefficiencies and performance penalties of device-by-device decryption and re-encryption. Similarly, a centralized approach to management can help organizations ensure consistent and efficient policy enforcement across the security infrastructure.

As a strategy rather than a product category, Zero Trust implementation requires more than simply plugging in a new box. Rather, it represents a new way of thinking about cyber security, embodied in evolving approaches to management, automation, auditability, resiliency, and integration. By approaching Zero Trust in this way, organizations can mitigate the security risks endemic in the new normal, and better protect their business from threats of all kinds. 📌

NETSCOUT REPORTS 5.4 MILLION ATTACKS IN H1 OF 2021

ADVERSARIES WILL NEVER TURN DOWN AN OPPORTUNITY FOR INNOVATION—AND THE PANDEMIC PROVIDED AN ENORMOUS ONE.

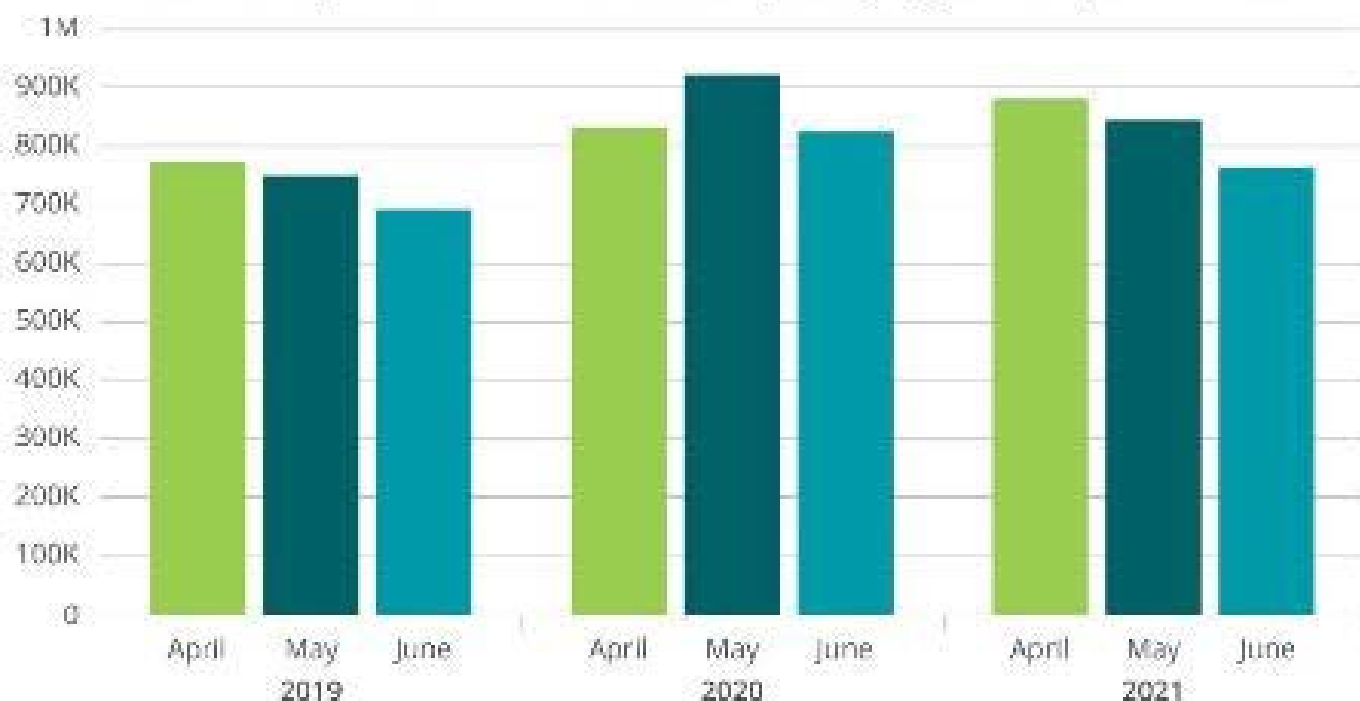
THE PANDEMIC'S LONG TAIL OF CYBERTHREAT INNOVATION WILL LIKELY CONTINUE WELL INTO 2021 AS CYBERCRIMINALS DISCOVER AND WEAPONIZE NEW ATTACK VECTORS THAT EXPLOIT PANDEMIC-RELATED VULNERABILITIES.

According to research from NETSCOUT's ATLAS Security Engineering and Response Team (ASERT), threat actors launched approximately 5.4 million Distributed Denial-of-Service (DDoS) attacks in the first half of 2021, an 11 percent increase from the same time period in 2020, putting the world on track to hit close to 11 million DDoS attacks in 2021. But Q2's numbers do show some signs of abatement:

ASERT observed 2,488,048 attacks in the second quarter, a 13 percent decrease compared with the first quarter's extraordinary number of 2,863,882.

The second quarter 2021 numbers also decreased by 6.5 percent

Second-quarter DDoS attack frequency by month, 2019 – 2021



compared with the same period in 2020.

In June, monthly DDoS attack numbers dropped below 800,000 for the first time since March 2020, to 761,914.

Second Quarter 2021

Total attacks: 2.48 million

Max size: 530 Gbps

Max throughput: 391 Mpps

Average duration: 59 minutes

But although attack frequency has dropped, we are nowhere near the attack numbers that were considered normal prior to the onset of the COVID-19 pandemic. To put things in perspective, we pulled data from the before the pandemic: 2019. In comparison, the second quarter

numbers from 2021 showed a continued high level of activity:

- 13 percent more attacks in 2021 than 2019
- The lowest monthly number of attacks for Q2 21 came in June, with 761,914 attacks. That low number nonetheless topped the high-water mark of Q2 2019: April's 755,748 attacks.

Several other things jumped out from our review of both quarterly and first-half statistics for 2021.

- The top five DDoS attack vectors seen in the first half of 2021 were TCP ACK, DNS amplification, TCP SYN, TCP RST, and TCP SYN/ACK amplification.
- Attackers continue to find value in pouring on faster, more difficult-to-mitigate attacks. Adversaries ratcheted

up throughput considerably, with the max throughput recorded increasing by 65 percent compared with Q1 2020.

- When it comes to attack duration in Q2 2021, attacks of five to ten minutes continued to top the list, used by 38 percent. We also saw a slight increase in attacks lasting between 10 minutes and an hour compared with Q1 duration numbers.

Adversaries will never turn down an opportunity for innovation—and the COVID-19 pandemic provided an enormous one. As such, the pandemic's long tail of cyberthreat innovation will likely continue well into 2021 as cybercriminals continue to discover and weaponize new attack vectors that exploit pandemic-related vulnerabilities. 🗝

DEMOCRATIZING SECURITY INTELLIGENCE WITH FORCEPOINT “DIM”

DIM IS A MODULAR SOLUTION THAT PROVIDES AUTOMATED INGESTION OF SECURITY FINDINGS FROM MULTIPLE HETEROGENOUS SOURCES AND AUTOMATED EXPORT TO MULTIPLE HETEROGENOUS DESTINATIONS.

A recent survey of cybersecurity and IT professionals uncovered that 78% of organizations use more than 50 different cybersecurity products to address their security goals and protect their resources. Within a few days another survey further highlighted that 86% of organizations rely on up to 20 security vendors. I’m not going to debate if these numbers are too big or just right: every company has a different security posture, a different perception of risk and a unique perimeter made of on-premise and cloud services.

The problem with an ever-growing array of security products and vendors is that, despite the numerous standards currently available in modern cybersecurity, security findings identified by one product are typically not available across all products, and findings are even less likely exchangeable across solutions from different vendors. This is why organizations buy SIEM tools to receive, aggregate and correlate findings and alerts.

End result, organizations end up building small ecosystems of great point products that could deliver better protection if only security insights identified by each product were shared automatically and in a timely fashion

across all components securing the different layers of the technology stack.

More importantly, it should be possible for developers within the organization to plug into this intelligence stream by integrating further sources, automating the exchange of intelligence with third party products. Ideally this should be done with a clean set of APIs that provides the ability to ingest/export data and perform queries and lookups against the entire intelligence vault.

To help address all these issues, Forcepoint has developed a free and open-source product to help the developer community increase security efficacy of their organizations.

Dynamic Intelligence Manager

Forcepoint Dynamic Intelligence Manager (DIM) is a modular solution that provides automated ingestion of security findings from multiple heterogenous sources and automated export to multiple heterogenous destinations, so that organizations can easily leverage a varied selection of intelligence and make it available across formats and products to their security devices and applications.

In the first release DIM handles the following elements:

- > IPv4 addresses, single entries and

DIM WAS BUILT WITH MODERN ORGANIZATIONS IN MIND: IT DOES THE JOB AUTOMATICALLY, WITH MINIMAL RESOURCES, IN A COMPLETELY TRANSPARENT WAY AND WITH THE ABILITY TO SCALE WITHOUT THE USUAL MIX OF UPDATES AND UPGRADES.

entire ranges.

- > Domain names, wildcard supported (e.g. *.badsite.com)

- > URLs

and provides several default modules that customers can use to import security intelligence from:

- > any custom source over the network (CSV, TXT formats) or uploading files locally in air-gapped scenarios

- > any TAXII feed serving intelligence in the STIX format (2.0)

- > Amazon GuardDuty

The entire list of elements stored into DIM is made available to:

- > Forcepoint Secure Web Gateway, to protect all users across the organization against web-based threats

- > Forcepoint Next Generation Firewall, to secure the network traffic of users, devices and workloads either on-premise or across cloud providers

- > any 3rd party product, using the DIM Lookup module which provides a secure API endpoint to check against DIM if a given element is known

Let's look at the cool features!

Dynamic Intelligence Manager was built with modern organizations in mind: it does the job automatically, with minimal resources, in a completely transparent way and with the ability to scale without the usual mix of updates and upgrades.

First of all DIM runs on any docker host (with just 2GB RAM and 2 vCPU) taking installation complexity out of the equation. The docker image is provided free of charge, with no registration necessary and it's only 70 MB in size! If you were to use it 24x7 for an entire year on AWS (using an EC2 micro instance) the TCO would only be around \$50.

All modules are installed using the UI of DIM itself: you click on the "Marketplace" tab and click to install the module. In a few instants a container for the module is deployed and the module is available for configuration: after that the module is ready to go and will keep working at recurring intervals as set by the user. Anytime Forcepoint creates new modules, they show up automatically in the Marketplace: you don't need to go

through updates and upgrade to add new functionalities.

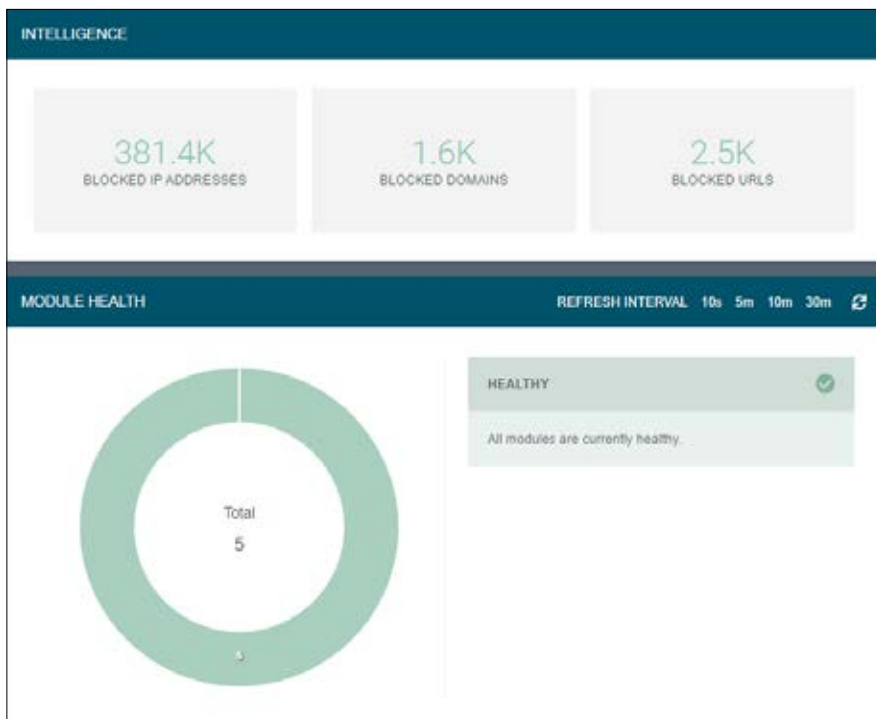
But did I not mention how DIM is developer friendly? Developers can build custom modules simply following the public DIM documentation. DIM is language agnostic and modules can be written in any language as long as they abide to the API contracts. All modules developed by Forcepoint are written in Go or Python, due to ease of development, performance and reusability and then built into docker images for portability.

Organizations with extremely tight security policies might want to look under the hood before running a new tool in their infrastructure. No problem! Source code of all modules used by DIM is publicly available inside Forcepoint's GitHub and can be inspected before DIM is deployed. Furthermore, DIM is licensed with an Apache 2.0 license, which allows developers to build on top of our work. More importantly: there is no tracking or telemetry in place so your intelligence and the use you make of it stays private.

Last, if you have been using something similar in the past, you might have witnessed false positives triggered by automated tools that went a bit too far. DIM comes with a Safelist feature which enables users to define known safe elements (e.g. your corporate domains, public IPs of your workloads and resources across geographical locations) and elements in the Safelist will be filtered out before the export takes place, so that no downward product will ever receive false positives.

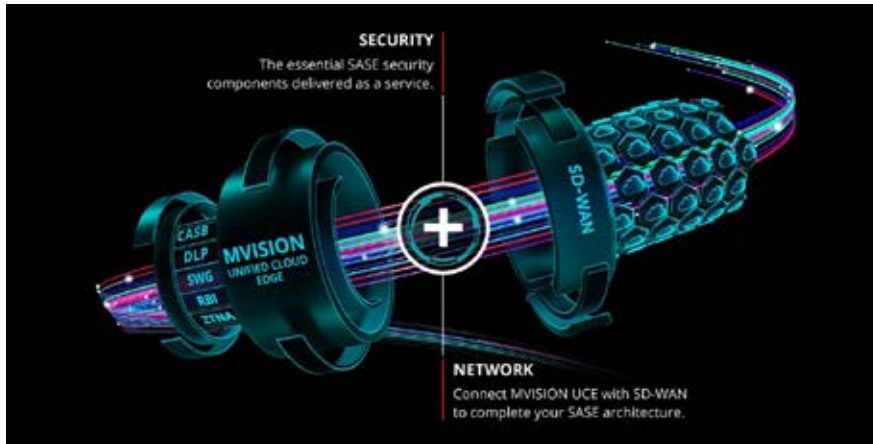
What's Next

Forcepoint is actively developing Dynamic Intelligence Manager, so that new intelligence types and modules can be available to users to further enhance their intelligence vault built on DIM. For example, we are working to ingest, store and export SNORT signatures and SHA256 file hashes with the same ease of use currently available for all other intelligence types. 🧑🏻



MCAFEE ENTERPRISE INTRODUCES MVISION PRIVATE ACCESS

MVISION PRIVATE ACCESS DISRUPTS THE ZERO TRUST NETWORK ACCESS (ZTNA) MARKET BY MAKING DATA-CENTRICITY A CORE CAPABILITY OF GRANULAR “ZERO TRUST” ACCESS TO PRIVATE APPLICATIONS.



McAfee Enterprise has announced MVISION Private Access, an integrated approach to enable granular ‘Zero Trust’ access and extend data and threat protection capabilities to private applications hosted across hybrid IT environments.

“As private applications increasingly move to the cloud, organizations are rapidly adopting Zero Trust Network Access due to its security and flexibility advantages compared to VPN,” said Christopher Rodriguez, research director, IDC Network Security. “However, organizations need to recognize that private applications are just as likely to pose a data theft risk as SaaS apps, and that this risk needs to be mitigated.”

MVISION Private Access disrupts the Zero Trust Network Access (ZTNA) market by making data-centricity a core capability of granular “Zero Trust” access to private applications, whether in customer data centers, or hosted in private, public or hybrid cloud environments, from any location and

device. The solution provides complete coverage across managed and unmanaged devices and performs continuous risk assessment by deriving enhanced device posture information through McAfee Enterprises endpoint security technology.

MVISION Private Access provides secure, ubiquitous access to private resources from any remote location and device, and secures remote workforce collaboration with:

- **Integrated data loss prevention (DLP) and industry-leading Remote Browser Isolation (RBI):** Enables advanced threat protection and complete control over data collaborated through private access sessions, preventing inappropriate handling of sensitive data, blocking files with malicious content and securing unknown traffic activity to prevent malware infections on end-user devices.

- **UCE Convergence:** Integrates with MVISION UCE, which includes Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG) to offer unified visibility, granular access control, end-to-end data protection and advanced threat protection

from a unified cloud management console. This seamlessly provisioned private access, along with other security capabilities through the same service edge, establishes the security foundation for Secure Access Service Edge (SASE) deployments.

- **Granular controls for Unmanaged Device Access:** Frictionless support for unmanaged devices, including the ability to move beyond simple access and posture concepts into full session control. MVISION Private Access enables sophisticated policy options that enable organizations to tailor policy to address their desired threat and data posture, even addressing session residence, cookie theft/replay, copy/paste and preventing lateral movement of threats.

- **Endpoint Security and Posture Assessment:** Extended context from McAfee Enterprise endpoints, powered by proactive threat intelligence from 1 billion sensors to evaluate device and user posture, which informs a risk-based zero trust decision in real-time.

- **Hyper Scale Service Edge:** Cloud-grade, intelligently peered PoP architecture with 99.999% availability that provides blazing-fast, direct-to-app access and seamless user experience beyond that delivered by traditional VPNs.

MVISION Private Access also further integrates with IAM (Identity and Access Management) and MFA (Multi Factor Authentication) solutions, enabling strong authentication options for application access and supplementing context-based access controls. This eliminates the risk of threat actors infiltrating corporate networks using compromised devices or user credentials, preventing an attack from propagating a network. 🛡️

17-21 OCT 2021

DUBAI WORLD TRADE CENTRE



GITEX
TECHNOLOGY
WEEK

X



عالم الذكاء الاصطناعي
EVERYTHING



**Fintech
SURGE.**
فنتك سيرج

**FUTURE
BLOCKCHAIN
SUMMIT**
قمة مستقبل البلوك تشين

ماركيتنغ مانيا
**Marketing
Mania**

17-20 OCT 2021

WHERE BUSINESS,
INNOVATION,
AND THE FUTURE
WILL BE DECIDED

140 COUNTRIES PRESENTING THEIR TECHNOLOGIES,
MAKE SURE YOU'RE THERE TOO

SECURE YOUR SPACE NOW: marketing@gitex.com

#GITEX2021
GITEX.COM

Gold Sponsor



5G Innovation Partner

Bronze Sponsor



VIP Majlis Sponsor



Platinum Sponsor



نيوم NEOM

Conference Sponsor



Headline Sponsor
Xlabs



Headline Sponsor
Xlabs



Supporting
Sponsor Xlabs



Supported by



Organised By





Security-Driven Networking, everywhere you need it.

Protect the possibilities
with Secure SD-WAN.

