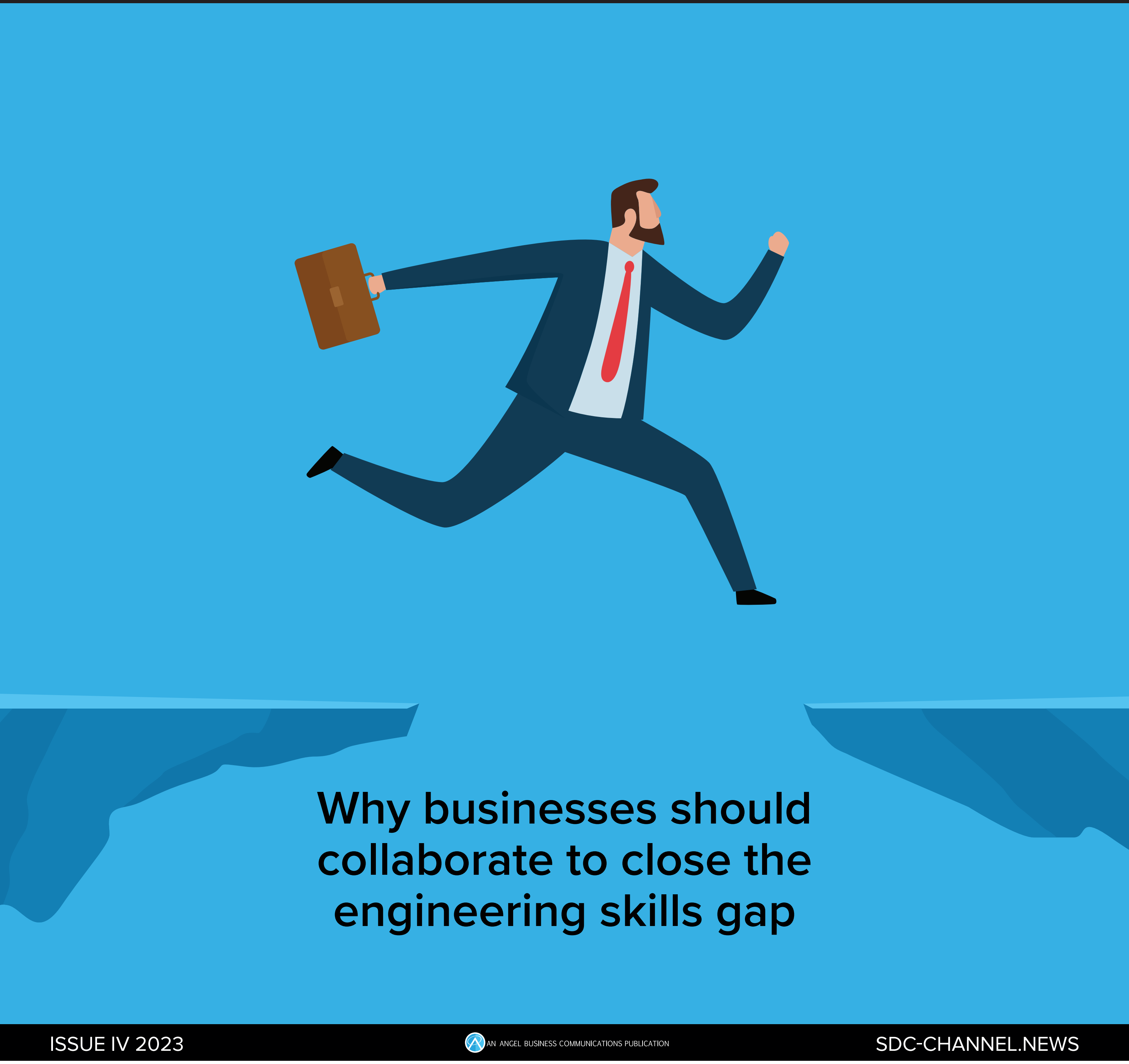
SDC CHANNEL INSIGHTS
SUSTAINING DIGITAL EXCELLENCE



Why businesses should collaborate to close the engineering skills gap

ISSUE IV 2023
AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION
SDC-CHANNEL.NEWS

INSIDE

News Review, Features
News Analysis, Profiles
Research Review
and much more...

CLOUD SECURITY AND RUNTIME ANALYSIS

Cloud computing helps companies implement technology more efficiently so they can achieve goals faster

PAVING THE WAY FOR SECURITY RESILIENCE

With so many cybersecurity solutions available on the market, customers can be left feeling underwater

HOW MSSPS CAN TACKLE RANSOMWARE

Ransomware is now a top threat, with the commercialisation of these attacks via Ransomware-as-a-Service

CLOUDBILLING

CLOUDBILLING
Manage the complexities of multi-cloud solutions
Automate billing and kickstart your BI strategy
CloudBilling Company Timeline
CLOUDBILLING
Get in touch!
Grow your
in the

We help service providers in maximizing their cloud profitability

Spot opportunities

Supercharge your business with our billing dataset. Compare client data, uncover insights, and seize opportunities.

Streamline your financial operations

Seamlessly connect and streamline multiple processes simultaneously. Your employees will love you for that.

Unlock the Power of Managed Services

Say goodbye to manual processes. We're here to take the load off your shoulders. Just tell us your needs and watch the magic happen!

"With CloudBilling, **80% of manual billing efforts are eradicated.**"
Jamie Sinclair - ANS

CLOUD NATION ANS wortell

☎ (+31) 035 524 8909
✉ sales@cloudbilling.nl
in /company/cloudbilling/
🌐 www.cloudbilling.nl

SCAN FOR A DEMO

VIEWPOINT

By Phil Alsop, Editor

Cybersecurity – the challenge continues

Which is more secure – physical paperwork, contained in a file, locked in a cabinet, locked in an office room, locked in a building patrolled by security guards OR a digital file, stored on a computer connected to the rest of the world? The answer would seem to be obvious. Ah, but ask a different question: Which of the above two scenarios better provides dynamic, 24x7x365 access to data crucial to the successful running of your digital business? And the answer changes. And here, in a nutshell, we have not so much a dilemma for organisations, rather an acknowledgement that the safest way to do business is also the slowest and most painful way to interact with employees, suppliers and customers. And the best way to do business in the digital age comes with a new level of risk – the connected world's major strength to enable modern enterprises to be fast, agile, scalable is also its major weakness as it allows so-called 'bad actors' undreamt of (potential) access to other people's money.

This issue of SDC Channel Insights is almost entirely related to cybersecurity. It's a constantly evolving topic, responding to the new ways in which the criminals attack organisations for financial gain, and has come a long way in a short space of time as a result. Looking ahead, perhaps the major concern is the potentially alarming skills gap that is developing within this technology sector. There aren't enough cybersecurity professionals available to do all the jobs required of them as of now; and it would appear that this situation is only going to get worse.

Step forward two possible solutions. The first is AI and automation. It is already doing an increasing amount of the cybersecurity heavy lifting, and will only do more and more of it in future.

The second is the Channel. More and more end users are realising that they do not have the necessary in-house cybersecurity expertise – either because they can't find suitable individuals and/or they cannot afford the cost. However, a Managed Security Services Provider (MSSP) can step up to the plate and provide multiple organisations with the technology solutions they require to keep safe.

Hopefully, the articles in this issue will provide some great knowledge and insight to help Channel organisations to create and develop their own cybersecurity offerings, which will play a critical role in safeguarding so many, as we all become more and more dependent on digital services.

SDC CHANNEL INSIGHTS

Angel BUSINESS COMMUNICATIONS

Editor
Philip Alsop
+44 (0)7786 084559
philip.alsop@angelbc.com
Sales Manager
Peter Davies
+44 (0)2476 718970
peter.davies@angelbc.com
Director of Logistics
Sharon Cowley
+44 (0)1923 690200
sharon.cowley@angelbc.com

Design & Production Manager
Mitch Gaynor
+44 (0)1923 690214
mitch.gaynor@angelbc.com

Publisher
Jackie Cannon
+44 (0)1923 690215
jackie.cannon@angelbc.com

Circulation & Subscriptions
+44 (0)1923 690214
circ@angelbc.com

Directors
Scott Adams: CTO
Sukhi Bhadal: CEO
Stephen Whitehurst: Chairman

Published by:
Angel Business Communications
6 Bow Court
Burnsall Road
Coventry CV5 6SP

T: +44 (0)2476 718970
E: info@angelbc.com

Published by: Angel Business Communications Ltd, 6 Bow Court, Burnsall Road, Coventry CV5 6SP
T: +44 (0)2476 718970 E: info@angelbc.com

SDC-Channel Insights is published four times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication.

CONTENTS

28

NEWS

07

SDC CHANNEL INSIGHTS

Editor
Philip Alsop
+44 (0)7786 084559
philip.alsop@angelbc.com

Sales Manager
Peter Davies
+44 (0)2476 718970
peter.davies@angelbc.com

Director of Logistics
Sharon Cowley
+44 (0)1923 690200
sharon.cowley@angelbc.com

Senior B2B Event & Media Executive
Mark Hinds
+44 (0)2476 718971
mark.hinds@angelbc.com

Design & Production Manager
Mitch Gaynor
+44 (0)1923 690214
mitch.gaynor@angelbc.com

Marketing & Logistics Executive
Eve O'Sullivan
+44 (0)2476 823 123
eve.osullivan@angelbc.com

Publisher
Jackie Cannon
+44 (0)1923 690215
jackie.cannon@angelbc.com

Circulation & Subscriptions
+44 (0)1923 690214
circ@angelbc.com

Directors
Sukhi Bhadal: CEO
Scott Adams: CTO
Stephen Whitehurst: Chairman

Angel BUSINESS COMMUNICATIONS

Published by:
Angel Business Communications Ltd
6 Bow Court, Burnsall Road, Coventry CV5
6SP
T: +44 (0)2476 718970
E: info@angelbc.com

MSPs are continuing to show unprecedented growth rates for third straight year

Service Leadership, Inc.®, a ConnectWise solution, has released the findings of its Service Leadership Index® 2023 Annual IT Solution Provider Industry Profitability Report™, recognised worldwide as the "IT solution provider industry encyclopedia of performance".

THE SERVICE LEADERSHIP Index® is the leading source of empirical data on IT solution providers (TSPs) performance worldwide. 2023 marks the 18th year of benchmarking to objectively identify best practices and set the bar for TSP owners and executives, including in 102 countries. It also provides an unequalled depth of insight and analysis to companies seeking to maximise growth, profitability, and stock value.

Having spent the last 12 months continually evaluating the performance of TSPs, the report reveals another impressive year of revenue and profitability growth with average approximate valuations being the highest on record. This is the third consecutive year that best-in-class managed service providers (MSPs) had over 20% adjusted EBITDA (earnings before interest, taxes, depreciation, and amortization) which is unprecedented and speaks to the high performance of the industry since 2020. This was also the sixth consecutive year that best-in-class VARs improved their profit performance (16.1% adjusted EBITDA). "2022 was an impressive year for TSPs across all Predominant Business Models™ continuing the trend for the third straight year with record revenue and profitability growth," said Peter Kujawa, VP & GM, Service Leadership, Inc. "Both best-in-class MSPs and VARs have continuously improved their profitability for three or more years. The TSP industry is healthy, despite recessionary fears."

The report also includes three new special sections:

- Financial performance for three geographic regions – APAC, EMEA and North America
- Profitability correlation of five key Operational Maturity Level™ Traits
- Declining services gross margin trend and recommendations for improvement

These special sections, and the report overall, will help TSPs worldwide understand how to drive better financial performance.

Modern applications need modern approaches

CISCO APPDYNAMICS has released a report titled, "The Age of Application Observability." The report provides insights into the challenges UK IT teams face managing application performance within increasingly complex multi-cloud and hybrid IT environments.

In a rapidly evolving IT landscape, the report found that 86% of technologists identify a pressing need to shift from traditional monitoring approaches to advanced observability solutions.

This change is being driven by the complexities tied to the rising adoption of cloud-native technologies, economic barriers slowing down cloud migration, and the persistence of hybrid and on-premises environments.

Notably, more than half (53%) of organisations are already looking into these next-gen solutions, with an overwhelming 82% marking observability as a strategic focal point.

This research has taken into account the perspectives of over 1,140 IT professionals across 13 global markets, including the UK. It highlights how the convergence of cloud-native technology adoption with on-premises technology is urging a more adaptive approach in the IT sector.

Key UK-centric insights from the report include:

- 86% of technologists claim that observability with business context will enable them to be more strategic and spend more time on innovation.
- 67% report that leaders within their organization do not fully understand that modern applications need modern approaches and tools to manage availability, performance and security.

On average, technologists report that 52% of their new innovation initiatives are being delivered with cloud-native technologies, and they expect this figure to climb to 61% within the next five years.

That means that the majority of new digital transformation programs will be built on cloud native technologies by 2028.

Half of zero trust programmes risk failure

CISOs consider zero trust a hot security ticket, but organisations run the risk of leaving gaps in their security infrastructure.

PLAINID has published the findings of its CISO Zero Trust Insight survey. The study, which questioned 200 CISOs and CIOs, revealed that the majority of respondents are on the road to implementing a zero trust framework in an effort to increase their overall security risk posture. However, only 50% said that authorisation makes up their zero trust programme - potentially exposing their infrastructure to threat actors.

Robust security cannot begin without first implementing Authentication Historically, a zero trust framework was focused on solving the challenges associated with authentication, end point and network access security. However, identity related breaches have increased exponentially, and the convergence of identity and access management with traditional security has accelerated the need for new technical capabilities for enterprise authorisation and access controls.

Authorisation is a broad and complex challenge requiring a solution that can provide a multitude of capabilities such as policy management, governance, control and policy enforcement across a disparate computing environment.

Ultimately, to provide the most secure digital end user experience, authorisation policies must allow for risk-based decision making in real time. This extends the zero trust philosophy from time of authentication through to the final access point and target data set.

The survey results reflected that only 31% of respondents said they have sufficient visibility and control over authorisation policies intended to enforce appropriate data access. Additionally, 45% of respondents indicated a lack of sufficient technical resources as a challenge in optimising enterprise authorisation and access control.

Essentially, organisations may have implemented a form of zero trust but they do not have the complete tool set or the on-staff expertise and knowledge to have true visibility and control of their network.

Building without the right expertise can create gaps in your security - Buy vs Build

Organisations are finding themselves building their own homegrown solutions, which can appear cost effective. However, this leaves gaps within the overall security posture if not developed, deployed, and maintained properly – resulting in higher operational costs and enterprise risk over time.

In response to the survey, 41% of respondents said they use homegrown solutions (OPA-based) to authorise identities. Moreover, 40% of respondents also said they use a homegrown solution (fully custom) to authorise identities. Without true zero trust, organisations run the risk of leaving gaps in their security infrastructure. Security must remain a fluid and ever-evolving technology as cyber adversaries will repeatedly re-strategise and evolve to breach organisations and when there is a will, there is a way. Next generation authorisation can be the differentiator between a headache for security teams and a full-blown breach. It is never a discussion of if but when hence why having homegrown solutions that are not built with the evolved threat landscape in mind and without the technical staff capable of maintaining, there may be a false layer of confidence that could lead to a betrayal of trust from partners and customers when their data is stolen.

As the demand for risk-based authorisation and identity aware security rises, the deficiencies of legacy homegrown authorisation engines are exposed. The demands from business stakeholders to keep pace with digital initiatives, while ensuring the highest levels of security and user experience, is driving change to adopt next generation enterprise authorisation solutions.

Security threats are a guarantee and are constantly evolving

Implementing an end to end zero trust architecture is a strategy that requires building a reference architecture that seeks to harden every threat vector possible. The next frontier is addressing the portion of the user journey post authentication, and beyond the borders of network access security. Next generation authorisation is poised to provide identity aware security at every layer of an enterprise computing infrastructure, while also providing central policy visibility, manageability, and policy governance.

“Zero trust must treat all identities as potential threats. While zero trust boosts higher levels of confidence, it’s imperative to pair it with a comprehensive authorisation framework,” said Oren Ohayon Harel, CEO and co-founder of PlainID. “Enterprises today need continuous evaluation and validation across all tech stack interaction to mitigate data breach impacts”.

Carbon calculator helps with sustainability objectives

AI-informed dashboard is designed to give clients access to standards-based greenhouse gas emissions data and help manage cloud carbon footprint.

IBM has launched a new tool to help enterprises track greenhouse gas (GHG) emissions across cloud services and advance their sustainability performance throughout their hybrid, multicloud journeys. Now generally available, the IBM Cloud Carbon Calculator – an AI-informed dashboard – can help clients access emissions data across a variety of IBM Cloud workloads such as AI, high performance computing (HPC) and financial services.

Across industries, enterprises are embracing modernisation by leveraging hybrid cloud and AI to digitally transform with resiliency, performance, security, and compliance at the forefront, all while remaining focused on delivering value and driving more sustainable business practices. According to a recent study by IBM, 42% of CEOs surveyed pinpoint environmental sustainability as their top challenge over the next three years. At the same time, the study reports that CEOs are facing pressure to adopt generative AI while also weighing the data management needs to make AI successful.

The increase in data processing required for AI workloads can present new challenges for organisations that are looking to reduce their GHG emissions. With more than 43% of CEOs surveyed already using generative AI to inform strategic decisions, organisations should prepare to balance executing high performance workloads with sustainability.

To help clients respond to these challenges, the IBM Cloud Carbon Calculator is designed to quickly spot patterns, anomalies and outliers in data that are potentially associated with higher GHG emissions. Based on technology from IBM Research and through a collaboration with Intel, the tool uses machine learning and advanced algorithms to help organisations uncover emissions hot spots in their IT workload and provide them with the insights to inform their emissions mitigation strategy[2].
“As part of any AI transformation roadmap, businesses must consider how to manage the growth of data across cloud and on-premises environments. This is especially critical today as we see organisations face increasing pressure from investors, regulators, clients to reduce their carbon emissions,” said Alan Peacock, General Manager, IBM Cloud. “For IBM, reducing environmental impact to help create a more sustainable future is a top priority and we are committed to helping clients achieve both sustainability and business goals. With the AI-enabled IBM Cloud Carbon Calculator, we’re helping clients better understand the greenhouse gas emissions associated with their IT workloads and giving them the insights to adjust their strategies and further their sustainability objectives.”

Clients are already using the IBM Cloud Carbon Calculator to address their sustainability goals. This includes e.tres, an Argentinian ecommerce platform, who is using the dashboard to measure greenhouse gas emissions.

“The way people shop is changing, and we’re committed to helping our customers deliver frictionless online shopping experiences backed by high levels of sustainability.

As we help our customers power their digital businesses with our innovative e-commerce platform, sustainability is at the centre of everything we do, with our e3Eco solution. With the IBM Cloud Carbon Calculator, enabled by AI, we can boost the sustainability of our clients’ operations, their technology and logistics shipments, so any ecommerce portal can become sustainable by measuring and offsetting greenhouse gas emissions.” said Diego Gorischnik, CEO of e.tres.

The IBM Cloud Carbon Calculator is designed to give clients access to standards-based GHG emissions data for IBM Cloud workloads with just a few clicks. Its capabilities include:

- **Track emissions across various workloads down to the cloud service level for enterprise accounts:** By helping deliver access to detailed GHG emissions data for their workloads on IBM Cloud, the tool is designed for clients to visualise and track GHG emissions associated with individual cloud services and locations, in accordance with the Greenhouse Gas Protocol. Clients can use filters to see emissions profiles across locations and a variety of services – starting with commonly used classic and cloud native infrastructure services, with more service coverage planned quarterly.
- **Identify GHG emissions hot-spots and opportunities for improvement:** Clients can analyse emissions by month, quarter and year, enabling enterprises to gain a regular view of progress towards targets. Having access to emissions trends and patterns helps to uncover anomalies and hotspots, and clients can use the insights they gained to adjust their strategies in near real time to optimise workloads across locations and ultimately help reduce emissions.
- **Leverage data for GHG emission reports:** Clients can access the output and audit trails generated by the IBM Cloud Carbon Calculator to help meet their reporting needs. Additionally, enterprises can integrate their emissions data into the IBM Envizi ESG suite3, which can help enhance their ability to conduct further analysis and reporting.

Data centres ‘underprepared’ for forthcoming legislation

The data centre industry is ‘underprepared’ for the forthcoming regulatory changes and new reporting thresholds, despite monitoring requitements starting in May 2023, according to Stephen Lorimer, Group Technical Director at Keysource.

SPEAKING at an event recently, Steve discussed The European Parliament’s review of the European Commission’s Energy Efficiency Directive (EED) recast since last year, with the directive set to be signed into law this year. He reminded the audience that in May 2024, the EED will require data centres in the EU with an annual energy use of over 2780 MWh to publicly report their energy performance.

“There will be an increased requirement on enterprises and data centre operators to publish energy action audit plans publicly, but they need to act quickly as the reporting period began in May 2023. So, in real terms you should have started!” urged Steve. “Reporting demands will require colocation operators to source capacity and throughput data from their customers and data centre operators will need to move quickly to examine their ability to comply and ultimately create a strategy to comply with the new reporting thresholds and establish a data collection and management processes for the required information.”

He went on to say that, “The new thresholds for reporting from Article 11 and 11A have changed and due to the global nature of the industry, will likely cover nearly all data centre operators. This involves reporting on annual incoming and outgoing data traffic, the amount of data stored and processed within the data centre, in addition to the temperature set points, power, water, and carbon usage effectiveness; energy reuse factor; renewable energy use and their cooling effectiveness ratio.”

“At Keysource we welcome greater transparency for the data centre industry. In order to comply with our climate change targets our industry needs to be accountable and these regulations will help to ensure everyone is working toward Net Zero. There will also be a number of benefits associated with the new regulatory changes such as cost savings, and a potential for increased investment as investors will be able to make better ROI predictions using historic data. We are working with a number of clients to help them prepare and to maximise the potential benefits,” Stephen concluded.

IT professionals required to do more with less as security threats remain major concern

IT SECURITY remains a top priority for most UKI professionals as revealed by Logicalis’ 2023 IT Survey.

The survey finds 71% of IT professionals list security as their top priority for the year. The independent UK & I survey, which canvassed the opinions of over 1000 IT professionals from across the UK & Ireland, unveils businesses are grappling with tightening IT budgets, changing IT priorities, and elevated concerns over security threats and technical skills shortages.

During uncertainty, digital transformation remains a key driver of innovation and security. In an environment of escalating cyber threats that come with significant costs, investing in cybersecurity has become an essential requirement across all market conditions. Just under half (47%) of respondents identify security threats as their biggest challenges in 2023, followed closely by technical skills and resourcing (46%).

These concerns are interrelated, as gaps in critical skills exacerbate security vulnerabilities. As a result, IT leaders are increasingly levering the technical skills of external IT specialists to pursue digital strategies. In line with this, Logicalis’ 2023 CIO Survey revealed that while a third of CIOs already work with outsourced IT and managed services, 74% expect to increase this spending in the year ahead.

Amid prevailing economic instability, 36% of IT professionals cite budgetary pressure as another major concern. The percentage of respondents expecting a decrease in their IT budgets has risen from 16% in 2022 to 25% in 2023. There is still a notable 35% seeing an increase (down from 51%), while 40% anticipate no change. IT teams are facing mounting pressure to bolster security while operating with limited budgets. Amid the rise in high-profile security threats, IT security is dominating organisations’ IT strategies. As we progress through the second half of 2023, the rapid pace of technological advancements shows no signs of slowing.

80 per cent of businesses claim AI is their biggest cyber threat

Four in five (80 per cent) of cybersecurity leaders claim that AI is the biggest cyber threat to their business, according to new research from RiverSafe, a leading cybersecurity professional services provider.

THE FINDINGS were revealed in the AI Unleashed: Navigating Cyber Risks Report, a survey of 250 cybersecurity leaders conducted by independent polling agency Censuswide, which detailed the rising threat of AI in cybersecurity. The research uncovered the preparedness of organisations and their plans to improve cyber posture to cope against AI-powered threats.

It was found that 81 per cent believe that the risks of artificial intelligence are more of a threat than the benefits it brings, suggesting that more must be done to improve confidence towards the development of AI.

Matthew Scott, Police and Crime Commissioner, Kent said: “Nearly 40% of businesses reported a cyber attack in 2022* and we know digitally-enabled crime accounts for more than half of all offences. There are clear benefits to AI but that cannot come without proper checks and balances and a legal framework to protect businesses and the economy. It is vital that government, policing, security services and business work together to boost prevention, education, and protection in what is a rapidly developing industry.”

Just over three quarters (76 per cent) said that the implementation of AI in their business has been halted due to the cyber risk it poses, while 14 per cent do not feel confident in their organisation’s ability to protect against AI-driven cyber-attacks, requiring the evolution of cyber defences to adapt. Suid Adeyanju, CEO at RiverSafe, said: “AI has taken over in recent months, forcing governments, regulators and businesses to rapidly develop responses to inbound AI threats, adding additional pressure to security teams. AI-enabled attacks themselves are still evolving which requires businesses to constantly review and update their cybersecurity measures to ensure that they are sufficiently protected.”

“Moving forward, security teams must ensure the safe development of AI for their organisation while maintaining their security posture for the evolving threat that AI poses. Balancing these two aspects is key to unlocking the potential of AI as a positive business tool.”

Worryingly, under half of businesses (45 per cent) said they have a system in place to review security risks posed by immediate suppliers, indicating heightened threats within the supply chain posed by the emerging threat of AI.

Oseloka Obiora, CTO at RiverSafe commented: “Innovation is a core goal for the UK and becoming a leader in the development of emerging technologies such as AI is important. Government and industry should embrace the benefits that AI brings, but this must be balanced out by mitigating the risks.” “It is especially concerning to see the lack of visibility that many businesses have over their supply chain, presenting unmonitored entry points for threat actors. This is an area that security teams must address to better protect themselves and their customers, particularly given the added fears that AI-powered threats pose.”

Data breach cost averages £3.4 million

UK organisations that extensively use security AI and automation reduced data breach costs by £1.6m on average.

IBM Security has released its annual Cost of a Data Breach Report, which reveals that UK organisations pay an average of £3.4m for data breach incidents. The study also finds that the use of artificial intelligence (AI) and automation have the biggest impact on UK businesses' speed of breach identification and containment, reducing the average breach lifecycle by 108 days compared to studied organisations that haven't deployed these technologies.

According to the 2023 study, organisations that deployed security AI and automation extensively – meaning throughout security operations, and within several different toolsets and capabilities – paid an average of £1.6 million less in data breach costs than organisations that didn't leverage these technologies. Yet, only 28% of UK organisations surveyed are currently deploying security AI and automation extensively, with a further 37% not yet adopting these technologies.

This year's report shows a decrease in the total average cost of a data breach in the UK from £3.8 million in 2022 to £3.4 million today - but this is still a 9% increase since 2020. Martin Borrett, Technical Director, IBM Security UK & Ireland, said: "With a 108-day average reduction in the breach lifecycle, security AI and automation may be the driving force needed to help defenders bridge the speed gap with attackers. The slight decline from last year in the overall cost of a data breach in the UK suggests the powerful impact security AI and automation may already be having on early adopters."

The 2023 Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by 553 organisations globally between March 2022 and March 2023. The research, sponsored and analysed by IBM Security, was conducted by Ponemon Institute and has been published for 18 consecutive years.

Some additional key UK findings in the 2023 IBM report include:

- **Industry Impacts –** The UK industries with the highest average cost of data breaches were financial services (£5.3 million), services (£5.2 million) and technology (£4.9 million).
- **Initial attack vectors –** Stolen or compromised credentials was the most common entry point for attackers at 13%. Malicious insiders were the most expensive initial attack vector (£3.9 million), followed by business email compromise (£3.86 million) and phishing (£3.85 million). Globally, the 2023 IBM Cost of a Data Breach Report found:
- **Security investment divide –** The global average cost of a data breach reached an all-time high of $4.5 million this year – yet while 95% of those surveyed have experienced more than one breach, only 51% plan to increase their security investments.
- **The Cost of Silence –** Ransomware victims in the study that involved law enforcement saved $470,000 in average costs of a breach compared to those that chose not to involve law enforcement. Despite these potential savings, 37% of ransomware victims studied did not involve law enforcement in a ransomware attack.
- **Detection Gaps –** Only one third of studied breaches were detected by an organisation's own security team, compared to 27% that were disclosed by an attacker. Data breaches disclosed by the attacker cost nearly $1 million more on average compared to studied organisations that identified the breach themselves.
- **Breaching Data Across Environments –** Nearly 40% of data breaches studied resulted in the loss of data across multiple environments including public cloud, private cloud and on-premises – showing that attackers were able to compromise multiple environments while avoiding detection. Data breaches studied that impacted multiple environments also led to higher breach costs ($4.8 million on average).
- **Critical Infrastructure Breach Costs Break $5 Million –** Critical infrastructure organisations studied experienced a 4.5% jump in the average costs of a breach compared to last year – increasing from $4.8 million to $5 million – $590K higher than the global average.

Ransomware attacks up 221% year-on-year

Ransomware attacks continue to hit record levels with 434 attacks in June 2023, a 221% increase on the same period last year (135 attacks – June 2022), according to the latest analysis from NCC Group's Global Threat Intelligence team.

JUNE'S high levels of activity has been driven by Clop's exploitation of the MOVEit file transfer software vulnerability, consistently high levels of activity by groups such as Lockbit 3.0, and emergence of several new groups since May.

Threat actors

Russian-speaking threat actor Clop was responsible for 90 of the 434 attacks (21%) in June, following its exploitation of an SQL injection vulnerability in MOVEit file transfer software, CVE-2023-34362, allowing the group to use this flaw to escalate privilege and steal sensitive data. It follows a quiet period for Clop in May, when it was responsible for just 2 attacks.

LockBit 3.0, the most active threat actor of 2023 so far, was responsible for 62 of the attacks, a fall of 21% from 78 attacks in May. 8base, a new threat actor discovered in May, stepped up activity with 40 attacks (9%) in June – making it the third most active threat group in June.

Other notable activity included 17 attacks from Rhysida and 9 attacks from Darktrace, two ransomware-as-a-service (RaaS) groups that were first observed in May 2023.

Regions

North America was the most targeted region, accounting for more than half of the attacks in June with 222 victims (51%) – the exact same total as May. Europe (27%) and Asia (9%) followed with 116 and 40 victims respectively.

Sectors

Industrials was the most targeted sector in June, representing 143 of the total attacks (33%), followed by Consumer Cyclicals (12%) with 52 attacks, and Technology (11%) with 48 attacks.

Spotlight: Clop and the MOVEit vulnerability

In June, threat actor Clop's exploitation of a vulnerability in Progress Software's MOVEit file transfer app, which is used by thousands of organisations around the world, made international headlines. A number of organisations whose supply chains use the MOVEit app suffered a data breach as a result, with customer and/or employee data being stolen.

This vulnerability has been abused to compromise MOVEit MFT servers and exfiltrate data and is currently tracked as CVE-2023-34362. Targets included big name brands, with attacks against well-known publishers, accounting firms, consultancies, large energy companies and colleges, amongst others. Over the last two years, Clop has abused four vulnerabilities in appliances that would either lead to the deployment of Clop ransomware or exfiltration of the victim organisation's data.

Matt Hull, Global Head of Threat Intelligence at NCC Group, said: "The considerable spike in ransomware activity so far this year is a clear indicator of the evolving nature of the threat landscape. The better known players, such as Lockbit 3.0, are showing no signs of letting up, newer groups like 8base and Rhysida are demonstrating what they're capable of, and Clop have exploited a major vulnerability for the second time in just three months."

"It's imperative that organisations should remain vigilant and adapt their security measures to stay one step ahead. We strongly advise any organisation using MOVEit File transfer software to apply the recent patch, given this vulnerability is being actively exploited."

KEVLARR

DMARC MANAGEMENT FOR MSPs. FROM CHALLENGE TO OPPORTUNITY

Organisations are becoming increasingly aware of the risks associated with inadequate protection against cyber attacks.

Simultaneously, the government is proactively crafting new legislation aligned with NIS2 directive. MSPs will also fall under this egislation, where safeguarding your clients digital identity plays a significant role.

Start protecting your email identity by simply testing your domains protection against impersonation at

kevlarr.io/email-test

Intelligent AI filtering

highly reduce the time needed for DMARC report analysis by applying our AI driven smart filters

Highly optimized DMARC implementation wizard

leverages our expertise and years of experience in the field ofDMARC management to guide you through the process with a step-by-step wizard.

Seamless integration

Capability provided by our API first approach as well as the white labeling capabilities of our dashboard.

WWW.KEVLARR.IO

Why businesses should collaborate to close the engineering skills gap

It's no secret that the technology industry is facing a significant skills gap in UK engineering. A recent report published by the Institution of Engineering & Technology uncovered that as many as 49% of engineering businesses were coming up against challenges when searching for skilled workers, leading to a six-figure shortfall of engineers that has cost the economy £1.5 billion per annum.

By Bev Markland, Chief People Officer at Agilitas

TODAY, engineering leaders are imploring the UK government to take action, requesting a re-examination and refreshed school curriculum that include more of a focus on engineering with a clear gender balance to encourage young girls to consider the sector as a career choice. Until these issues are addressed, however, technology businesses need to step up and take action to close the skills gap.

Identifying the Skills Gap

Defined as the misconnect between employee skill sets and what is required to complete their job effectively, the skills gap is a growing concern. This is especially true as the skill sets that workers need continue to evolve over time in our dynamic and fast-paced business environment, with previously manual tasks becoming automated and other external factors impacting workplaces. In fact, 56% of hiring managers stated that technological advancements, such as artificial intelligence, will significantly change the skills they require from candidates.

As a result, technology companies must begin to identify the skills necessary to remain competitive in the market. They need to pinpoint any workforce gaps or skill shortages, before developing strategies to fill those gaps. This involves defining the specific skill sets associated with each role to hire and retain the right talent.

Promoting Learning and Development

The World Economic Forum recently reported that more than half of all employees worldwide need to upskill or reskill by 2025 in order to embrace new responsibilities driven by automation and emerging technologies.

With that in mind, businesses should consider investing in educational initiatives that promote engineering as a viable career choice. Partnering with academic institutions, offering scholarships, and supporting engineering-focused programs are great ways to attract more students to pursue engineering careers and bridge the skills gap from an early stage.

Learning and Development (L&D) initiatives, such as a strategic workforce education program, also enable employees to keep their skills up to date and further their careers while meeting the industry's changing demands. Furthermore, implementing workforce education programs that promote upskilling and reskilling within an organisation will help close skills gaps and prepare companies for future advancements.

Research demonstrates that organisations that invest in the critical practices that drive L&D success are 59% more likely to experience growth, are 27% more cost-efficient, and consistently deliver higher engagement, retention, and leadership scores. Companies must therefore create a solid L&D infrastructure, content, and organisation strategy roadmap.

In addition, establishing comprehensive in-house training programs enables businesses to upskill their existing workforce. By offering tailored engineering training, employees can acquire the necessary knowledge and expertise to excel in their roles, contributing to a more skilled engineering workforce in the future.

At Agilitas, we are continuously promoting L&D opportunities to encourage our employees to either attain formal qualifications or to attend in-house training and employee wellbeing workshops, all of which are aimed at developing engagement, retention and leadership.

Encouraging a Gender Balance

Women remain a minority in both STEM education and careers, representing only 28% of engineering graduates, 22% of artificial intelligence workers and less than one-third of the global technology sector employees. Now is the time to rethink if the broad subject area of engineering is to appeal to more women.

Several strategies have been used to encourage young women to consider engineering as a viable career option, including outreach programs aimed at students, mentoring programs, information sessions, workshops and summer camps. In line with this, we have enrolled six of our female employees to shortly embark on a STEM three-day course run by a local university.

Another initiative that has seen success is Sheffield’s Women in Engineering Society, which brings thought-provoking and informative material to secondary and primary schools. They are making engineering and science exciting for schoolchildren while simultaneously degendering the field.

Investing in Outsourcing

For businesses, investing in education and training will significantly help to cultivate an educated engineering workforce, with opportunities to leverage outsourcing for technical training to achieve this goal more efficiently. Offering scholarships and grants to aspiring engineering students can also reduce the financial barriers to education, enabling talented individuals from diverse backgrounds to pursue engineering careers. Companies can also consider Research and Development Funding which fosters innovation within the engineering field. Not only does this lead to advancements in technology, but it also attracts top talent to participate in cutting-edge research, thereby enhancing the overall quality of the engineering workforce.

It is estimated that companies spend an average of 26% of their training budget on external (outsourced) suppliers and approximately 64% on internal resources. This highlights the resources available to outsource technical training to specialised providers with in-depth knowledge and expertise in the specific engineering domain, ensuring that the training delivered is high quality and covers all relevant aspects.

Outsourced training also helps workers keep updated on advancements, helping companies maintain a competitive edge in the market. Furthermore, setting up an in-house training program can be expensive and time-consuming, whereas outsourcing technical training allows businesses to focus on their core business activities while leaving the training responsibilities to external experts.

Furthermore, investment in education and training will create a solid and educated engineering workforce. At the same time, businesses can benefit from outsourcing technical training to specialised providers to ensure their employees have the knowledge and skills required to excel in engineering. This collaboration can lead to a more competent, innovative, and efficient engineering ecosystem.

Building a Brighter Future

The engineering skills gap continues to challenge UK businesses, impacting the economy and hindering their growth in the technology sector. As engineering leaders urge the government to take action, companies must collaborate to address this challenge. By embracing proactive measures and launching L&D initiatives, these organisations can play a pivotal role in closing the engineering skills gap. A well-educated, diverse, and skilled engineering workforce will drive growth and innovation, and fortify the UK’s position as a leader in the technology sector for years to come.

Cloud security and runtime analysis - why speed matters

Cloud computing helps companies implement technology more efficiently so they can achieve their goals faster. Gartner estimates that spending with cloud service providers (CSPs) will reach nearly $600 billion this year, as companies run to add more innovation to their business approach. However, cloud computing maintains risk as well. The very reasons that we value the cloud - speed, efficiency, scale - are also prized by threat actors looking to make a buck.

By Crystal Morin, Cybersecurity Strategist, Sysdig

A METRIC we can use to represent this environmental risk is dwell time - that is, how long an attacker spends within a victim's IT network before being detected. For on-premises deployments, this is measured in days. Mandiant estimates that threat actors spend an average of 16 days within the network before they are detected and removed. In the cloud, the risk timescale is vastly different. In our 2023 Global Cloud Threat Report, the Sysdig Threat Research Team reported that threat actors went from initial access to attack mode in just 10 minutes. Dwell time in either environment may include the attacker getting the lay of the land, looking for valuable data or additional privileges, and taking actions such as exfiltrating data or deploying malware. Dwell time is when attackers are the most stealthy and where they are looking to maximise their return on investment.

With your customers' proprietary data and business financials at stake and so little time to mitigate the risks, how do you help them proactively prepare for cloud security attacks and stay ahead of attackers?
Spot the problem, before it becomes a problem
One of the greatest struggles with cloud security

is how to spot potential attackers in the first place. Fortunately, from the get-go CSPs have provided services like AWS CloudTrail which logs all data pertaining to what, where, and when activity is taking place in a cloud environment. There was an initial challenge, however, in that security professionals were not familiar with these tools and did not make use of them effectively. As cloud security processes matured, these became the standard first step in defensive security tooling.

This maturity and ubiquity has not gone unnoticed by threat actors either. In response, attackers look for ways to hide their actions within legitimate traffic and activity, and there are several common methods that have developed. One is the use of an AWS Virtual Private Cloud (VPC) to obfuscate the attacker's existence in a victim network. A VPC spoofs the IPs that end up in the victim's CloudTrail logs, which makes attacker activity appear to be benign behaviour. This technique bypasses any typical security measures that rely on spotting threat actor activity based on abnormal source IP addresses, and makes it harder for defenders to differentiate an attacker IP from normal IP addresses used in the internal network. An attacker can even prepare their AWS VPC with their own AWS account, not needing to have initial access to a victim environment and anonymise any request to publicly reachable service endpoints.

Attackers can also hide themselves from logging services like CloudTrail by calling on AWS S3-compatible services rather than using S3 itself because the latter services do not get captured in CloudTrail logs. In the SCARLETEEL operation, the attacker used the S3-compatible Russian service mail.ru when exfiltrating data. In this case, CloudTrail logs will not suffice and more is needed to stop these attacker techniques.

Lastly, using cloud services like AWS CloudFormation can help attackers get past defences too. CloudFormation allows you to model, provision, and manage AWS and third-party resources by treating infrastructure as code, making it an essential tool for those running AWS installations. It is also able to manipulate roles and policies outside of traditional mechanisms, which makes it ideal for attackers to abuse. Using CloudFormation's AssumeRole command, attackers can try to add more privileges to an account and move laterally to use or implement other services. Spotting attackers using this tool is tricky when it may also be heavily used for any internal management workflows.

Real-time and runtime security

Cloud threat detection systems can help customers protect themselves against these kinds of attacks because relying solely on the native logging and alerting tools provided by the CSPs just isn't enough. Cloud threat detection should be near real-time so your customers' security teams get alerts instantaneously, rather than getting those alerts after multiple actions have taken place. Once you understand how fast attacks take place, the need for runtime security becomes apparent. In Sysdig TRT's research on more than 13,000 container images publicly available on DockerHub, 819 were secretly malicious. Of these malicious images, only 60 percent were identified using vulnerability scanning, and 69 percent were found using static analysis alone. Ten percent of malicious images were still not detected when we combined vulnerability scanning and static analysis. That ten percent of the malicious images were only identified when the container was actually implemented and running.

> Attackers can also hide themselves from logging services like CloudTrail by calling on AWS S3-compatible services rather than using S3 itself because the latter services do not get captured in CloudTrail logs

If you can't spot that a container houses a threat before you implement it in your cloud environment, then you are providing an attacker with an initial access vector as soon as that container goes live. In our 2023 Cloud-Native Security and Usage Report, we found that 72 percent of containers live less than five minutes, but the threat report confirms that this is all the time that is needed for an attacker to obtain initial access and make moves inside your cloud environment. Looking to runtime security and using tools such as Falco are therefore an essential piece of a speedy and proactive cloud defence. The open source project Falco is now part of the Cloud Native Computing Foundation (CNCF) and provides runtime insight into cloud-native environments running containers, Kubernetes, hosts and cloud services. Using Falco, your customers can get the insights they need to secure their cloud and container environments early against attacks that take place at runtime and that would otherwise be missed.

CSPs deliver huge amounts of data to those that use them. Picking out potential threats and issues can be difficult if you do not know where to look for obfuscated attacker activities. However, this level of runtime insight can be used alongside other existing defensive cloud services to spot threats that cross over between different levels of cloud infrastructure and that would be missed by any single cloud logging service. Correlating information from multiple cloud detection services and understanding them in context is necessary to spot threat actor behaviour against the backdrop of your typical cloud environment usage. Truly understanding this complexity is where you can provide advice and guidance to your customers on how to architect cloud security and beat runtime threats.

Three key cyber resilience messages that channel partners need

Pretty much every CISO will believe that cyber threats are the number one challenge facing their organisations. It's not surprising, of course they would - they have a vested interest and their jobs depend on it. They are not the only ones in the C-suite worried about cyber vulnerabilities because CEOs also rank cyber threats very highly.

By JT Lewis, Director of Channels EMEA and APJ at Infinidat

CYBER-ATTACKS rank in second place amongst the most serious of all possible economic, social, political, business, and environmental threats. This is according to PwC's 24th Annual Global CEO Survey. Within the UK CEO subset, the level of threat was deemed very high - 91% of CEOs said that cyber protection was their key priority.

Many channel partners are well aware of what the threat of a cyber-attack means in terms of a market opportunity and have rightly been investing in their cybersecurity operations. They appreciate that enterprises do not always have the internal cyber-skills to ensure a rapid bounce back if they encounter an attack and even if they could afford to buy in the necessary skillsets, recruiting those people is another matter. It is why 'cybersecurity as a service' is now one of the fastest growing new business areas within the enterprise IT channel. It is also one of the most valuable subsets of an industry worth US$2 trillion, based on estimates published by McKinsey.

As with all developing industries, education will inevitably be an important component of any cybersecurity managed service provision and this includes helping end user enterprises to appreciate the need for cyber resilient storage. Here are 3 key messages that every channel vendor needs to be sharing with their CISO and CISO client base, to help them understand what's at stake and how they can protect their organisations.

#1 Not if, but when...

It's mind-blowing to think that every 39 seconds, an organisation somewhere in the world suffers a cyberattack. If intrusion attempts are happening with such frequency, it's no wonder that CEOs are scared. The question is not if your enterprise will suffer a cyberattack, but when and how often. And if penetrating the firewall is a given, this also means it's highly likely that primary and secondary data being stored by an enterprise will be compromised at some point too.

#2 Cyber criminals are patient beasts

There's a perception that cyber attackers have a smash and grab mentality, but the statistics tell a different story. When cyber attackers target an enterprise, they don't immediately pounce, but wait for a while before demanding a ransom. Sometimes they will have planned their eventual move for over 6 months. Research conducted by the Ponemon Institute verifies this, suggesting that the average number of days before a data breach is identified can be as high as 287. It means the hackers have a much greater chance of their ransomware demands being met because without the right controls in place, the data stored can be fully compromised. In that timeframe, data could have been exposed to all kinds of criminal activity.

#3 Prevention is always better than cure

Data is one of an enterprises most important strategic assets and why McKinsey has coined the phrase 'data-driven enterprise.' It describes an organisation with data embedded into every decision, interaction and process. If effective cyber security is about being ready to thwart the problems that arise from a security breach, what should enterprises be doing differently to protect their data? It means thinking beyond the traditional toolkits of firewalls or cyber management software and being ready with an antidote to stop the damage from spreading.

Time to protect data, but how? Key ingredients of cyber resilient storage

Today's cybercriminals are technology experts. They are highly skilled at exploiting data vulnerabilities inside enterprises that do not understand the importance of cyber resilient storage and have left either primary storage infrastructure or secondary/backup/disaster recovery storage exposed. Maybe even both.

When it comes to securing an enterprise's data storage, there are some essential ingredients to building a storage cyber defence strategy that channel partners should understand. These include ensuring the immutable nature of the data, recovered from a copy you can trust. Air-gapping to separate the management and data planes to protect the data. A secure forensic environment, to analyse the data thoroughly and ensure the fastest recovery speeds possible is critical. Each of these elements needs explaining to enterprise end users.

Immutable snapshots are like the vital 'secret sauce' of storage cybersecurity. They allow the end user to effectively roll back the clock and recover guaranteed, uncorrupted copies of their data, before the execution of any malware or ransomware code introduced by an attacker. Immutable snapshots ensure data integrity because they prevent data copies from being altered or deleted by anyone. Even internal systems administrators are locked out of immutable snapshots manipulation. It means that the enterprise can be confident that any disruption or damage caused by the intrusion can be kept to an absolute minimum.

Logical air gapping adds a further layer of security, by creating a safe distance between the storage management layer and the immutable snapshots. There are three types of air gapping. Local air gapping keeps the data on premises, remote air gapping makes use of a remotely hosted system and hybrid air gapping combines the two.

Fenced forensic environments help speed up the recovery process by providing a secure area to perform a post-attack forensic analysis of the immutable snapshots. The purpose here is to carefully curate data candidates and find a known good copy. The last thing an enterprise wants to do after an attack is to start restoring infected data that has malware or ransomware infiltrated within it. Once the forensic analysis is complete, it is safe to restore a copy to primary storage systems.

The right cyber storage resilience solution is part of a "set it and forget it" process. Once the immutable snapshots, logical air gapping, fenced forensic environment and cyberattack recovery processes have been established, the whole restoration will progress like clockwork. This is all part of being an agile enterprise, one that's cyber resilient as well as cyber secure. Significantly very few enterprise storage vendors can offer this level of cyber resiliency on primary data, which if part of an overall cybersecurity as a service offering, would become an important differentiator for a channel vendor.

It is clear that all channel partners have an important role in educating their enterprise customers that securing primary and secondary storage is an essential part of their overall corporate cyber resilience strategy. Data is one of the most important strategic assets an enterprise owns and critical to long term business success. Yet too many enterprises have not fully integrated a cyber storage resilience program. It's a fantastic business opportunity for channel partners and those who are early to market with a strong cyber resilient storage offering will reap plentiful rewards.

Security risk mitigation and the growth opportunity it presents for the Channel

According to the Fortinet 2023 Work-from-Anywhere global study, 60% of companies surveyed are accommodating employees working from home, and 55% are embracing a hybrid work strategy. For the global workforce, this paints a positive, more flexible picture when it comes to balancing home and work demands; for businesses, this presents an opportunity to create a compelling employer brand. However, while the advantages seem plentiful, there are also some important threats that need to be addressed, which is where I see a major growth opportunity for the Channel.

By Erik Nicolai, CEO, Workspace 365

THE SAME Fortinet report found that organisations consider the insecurity of home and remote networks to be their top security risk (41%) when deploying a working from home strategy. This is followed by employees using company laptops for personal reasons (38%), not following security protocols when outside of the office (30%), and unknown users sharing the home network (24%). The report suggests that organisations want to be able to establish consistent policies across all locations, including remote working, however, the complexity and confusion surrounding what vendors can offer combined with the additional investment leaves business leaders and CTOs scratching their heads.

Many of these firms have already invested substantially into IT architecture and infrastructure, however, these systems rarely present a unified, standardised approach to security, meaning it's difficult to put in place measures that will consistently and reliably ensure a company's security, wherever their employees are, and whatever device they're using.

The need for a standardised approach to security

For the Channel, this challenge (and opportunity) is very real. With clients now looking for ways to maximise their current tech investments, rather than reinvest in alternatives, how can resellers add value while delivering the heightened levels of security needed with hybrid workforces?

Working with our long-term Channel partners, we've developed a platform that provides the highest levels of security, while integrating with all major applications, such as SharePoint and Microsoft 365. As well benefitting from a single sign on, the platform uses multifactor authentication provided by Azure. Only after employees have passed these identification

tests will they gain access to their unified digital workplace.

Furthermore, using this standardised approach to security, employees are prevented from uploading or downloading malicious files, as well as being alerted if malicious files are found in applications, such as SharePoint and OneDrive. Additional protection includes not showing images directly in the email app to prevent any potential risk resulting from harmful code.

This file server integration means that existing IT deployments, such as Citrix and OneDrive, remain functional, however, rather than juggling a myriad of different layers of security from a broad supply of vendors, businesses benefit from a standardised approach to security.

For the Channel, this move towards a unison of applications rather than 'yet another deployment', is a critical selling point, and major value add for their clients.

The importance of adaptive security

When we talk about working from home, what we really mean is working from anywhere; from a café, from a beach hut, from a train, and with that comes the likelihood that employees will be accessing workstreams and applications on a range of different devices, depending on what's most suited to where they are, in that moment.

This poses a different type of security threat, for example, let's consider an employee working from their mobile phone on a train. Not only is this not a private or secure location – anyone could be viewing their content – it is also a device that's unlikely to have the same level of security as a company laptop.

By deploying technology that adapts to different devices and environments to deliver the right level of security, businesses can limit the risk. This could mean sensitive documents or folders are inaccessible when working from a mobile or tablet or from insecure locations.

Likewise, if the WiFi in a certain public place or different country does not meet the security requirements set, or their IP testing doesn't match, then employees will only be able to access predefined areas of their digital workspace, until they are deemed to be in a suitably secure location or environment.

For the Channel, it's important to highlight these, often neglected, areas of security and risk to customers, while offering a solution that is ISO-compliant and backed by annual Penetration testing.

Role-based security layer

Isolating accessibility based on specific roles is another key area of growth for security when it comes to hybrid workforces. This conditional access layer allows a business to specify which groups of people can access specific data sets or folders. Not only does this increase productivity, it also ensures sensitive information can only be accessed by predetermined people or roles within the business.

Value add for businesses, growth for the Channel

With figures from the Fortinet report revealing that 37% of organisations are planning to significantly increase their security budget in response to supporting the company's long-term 'work from anywhere' policy, there's a clear opportunity for the Channel to help direct and inform that spend.

While companies are openly looking to invest, the challenge for resellers is to show how that outlay can enhance rather than replace existing IT deployments. Offering a value add proposition, that provides one overarching security standard, while driving increased productivity and collaboration amongst hybrid and global workforces is the core differentiator, and is what will truly set partners apart from the competition.

Working with the Channel

Workspace 365 works with Channel partners to deliver highly secure digital workspaces for businesses operating hybrid workforces. Its platform has been designed to intuitively adapt security levels depending on the device and location being used to access work applications and documents.

These Channel partnerships have helped inform the approach we take to security, with key outcomes being our continuous monitoring to ensure we stay ahead of potential threats, and proactively conducting annual audits and assessments to identify and address any potential vulnerabilities and weaknesses in the platform.

How MSSPs can cost effectively tackle ransomware

Ransomware is now regarded as a top threat, with the commercialisation of these attacks via Ransomware-as-a-Service and nation state sponsored attacks seeing threat actors refine their attack capabilities.

By Matthew Rhodes, Regional Director for MSSPs at Logpoint

Following a brief hiatus earlier this year, attacks are now on the rise again, with the Mid-Year Cyber Threat Report recording almost 90million attacks during Q2 2023, up 74% compared to the first quarter.

It turns out the ransomware window ie the time from compromise to the deployment of ransomware and encryption of data has shrunk. It now stands at 4.5 days compared to 5 days in 2021. Meanwhile, attacker dwell time on networks has halved from 22 days to just 11. So, attackers are getting in, obtaining the data they want, and getting out much faster.

There's also been a significant shift in ransomware practices. Rather than encrypting the data in exchange for a ransom, many operators are now stealing data and threatening to leak it, leading to a rise in extortion-based attacks. Reports suggest that non-encryption ransomware attacks were up 25% between April and June of this year and the attack against the MOVEit file sharing protocol by the Clop group is a perfect example of how devastating these can be.

Struggling to keep up

Defences, however, are not keeping pace. According to the MSSP Automation and Integration report, 65% of businesses saying SOC operations are losing time due to inefficient processes, 57% saying the Mean Time to Detect (MTTD) and MTTR are below goals, and 35% saying they do not have the best process or tools for building detection patterns. This presents MSSPs with a clear opportunity, with many organisations now turning to the channel to provide access to the latest technology to counter the ransomware threat.
The faster infiltration we're seeing with ransomware attacks requires faster detection and defence, which is why it's imperative that monitoring covers the entire information estate, from email to endpoints. Endpoint Detection and Response (EDR) is a tool

that can help here as it continuously monitors all endpoint devices for threats that may get past traditional defence mechanisms such as anti-virus, anti-malware and firewalls. Analysis is carried out in real-time and incident response is carried out automatically to speedily mitigate threats and minimise the impact of an attack. EDR can therefore dramatically improve detection, reduce dwell time and increase Mean Time to Response (MTTR).

Yet many businesses cannot afford to invest in EDR, lack the expertise or resource to manage it. This makes it a prime technology for MSSPs to consider, with many looking to add it to their portfolio over the next 12-24 months, according to the report. The difficulty lies in being able to integrate such technologies with their current offerings. MSSPs don't want to have to bolt together different technologies and dedicate the manpower to managing and customising these, all of which leads to higher overhead costs.

Integrating EDR

Monitoring end user devices, networks, applications, and firewalls is complex and even more so when using point solutions which have different ways of working. Over time, the addition of numerous technologies to the security stack has inevitably lead to siloed operations. Those overseeing these technologies then have to resort to swivel chair monitoring, logging into and reviewing alerts across numerous user interfaces. As these standalone technologies are not integrated, bringing together this information then requires the manual correlation of events and alerts.

A lack of interoperability can often be the reason a customer chooses to outsource to an MSSP due to the complexity involved but it can equally be an issue for the MSSP too. Increasingly, MSSPs are looking at how they can simplify the stack and this is now front of mind when it comes to investing in new technologies. So, when it comes to developing a ransomware-ready solution, MSSPs pre-integrated technologies and one example of this is virtual EDR integrated within the Security Incident and Event Management (SIEM).

A converged SIEM (sometimes referred to as a next generation SIEM) extends the traditional functionality of the SIEM by incorporating additional, complementary tool sets. Adding in EDR, for instance, sees log source analysis also incorporate EDR monitoring so that issues can be captured even earlier. Using agents deployed on the endpoints, data is fed back to the SIEM rather than a separate EDR server so that the EDR operates as another log source. This then means there is no need to extrapolate the threat data to explore the potential impact of a threat. Because this data is compared against the tactics, techniques and procedures (TTPs) outlined in the MITRE ATT&CK framework, this provides a more comprehensive form of monitoring across the network and its endpoints, reducing MTTD and MTTR. The convverged SIEM can also integrate other threat hunting technologies such as Security Orchestration Automation and Response (SOAR) and User Entity and Behaviour Analytics (UEBA). SOAR brings together data from disparate sources and then uses automation to ingest and analyse alerts. It can prioritise threats, make recommendations and carry out automated actions including automated response through the use of pre-built and customised playbooks. Post-incident, it can also provide automated case management and reporting.

UEBA works by building baseline parameters of 'normal' behaviours that are tailored to each individual user. When behaviours then stray outside of these parameters, these are automatically flagged to security analysts for their review. So in the case of a ransomware attack, the exfiltration of data via a particular endpoint which went against that user's usual work pattern would trigger an alert.

A combined effort

But integration doesn't just reduce complexity, it also paves the way for the MSSP to take a less reactive and more proactive stance. Rather than being alert and event driven, the MSSP can offer more proactive services such as threat hunting and emerging threat detection. This is because assimilating these tools together enables far more effective endpoint interrogation and faster threat detection and incident response (TDIR). The event logs and flat files capture behaviour from systems and applications hosted on servers enabling forensic investigations and threat hunting to be carried out by the IR team. This means that, in the event of an attack, the logs can be used to determine how the attack gained access and moved across the network during the investigation.

As those endpoint logs and telemetry are being fed into the SIEM they can be enriched using contextual information from the MITRE ATT&CK framework to see which tactics, techniques and procedures were used. They can also be configured with compliance standards to save time and resources during audits. MSSPs can and should be looking to extend their capabilities to address the ransomware threat but what they don't want to end up with is a bloated resource-hungry stack. They need to expand their offerings but also need to reduce complexity so at some point have to adopt a convergent approach and combine functionality.

Convergence of complementary technologies promises to greatly emancipate MSSPs as they'll no longer be as restricted when it comes to choosing which technologies to offer. Combining multiple threat hunting solutions over a single platform, for instance, ensures the MSSP remains competitive while gaining from much better network visibility, control and lower maintenance demands by using one solution - benefits they can then pass on to their customers.

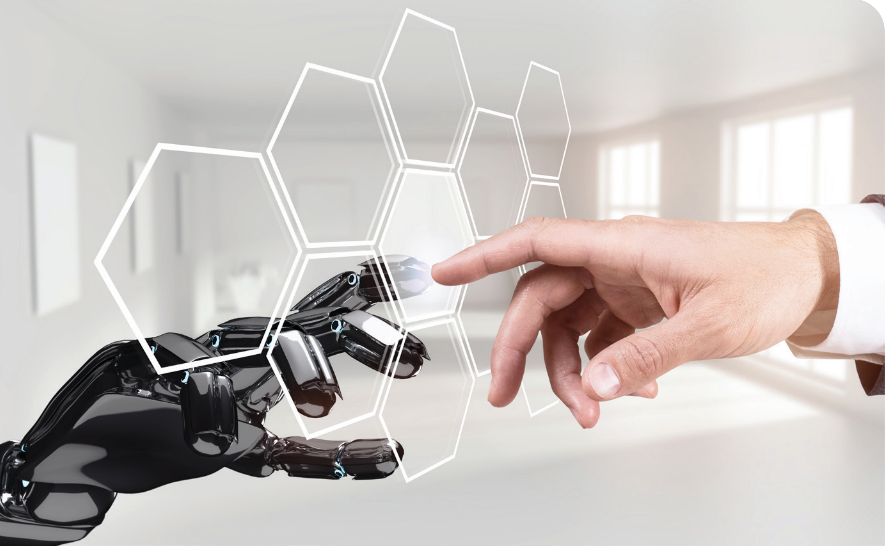
A new cybersecurity frontier

Navigating new technologies and vulnerabilities.

By Jason Timm, CEO & Co-Founder at CloudSmiths

IN AN ERA of unparalleled tech development, enterprises are rushing to stay current and take advantage of the new opportunities that advances in Automation and Artificial Intelligence are providing. But racing to capitalise on these technologies too quickly brings risks.

Benefiting from these technologies requires careful planning and robust implementation of cloud and data integrations. If rushed or not done correctly, it can lead to severe cybersecurity and data governance risks. Unsecured data and poorly managed integrations can expose sensitive information, making systems vulnerable to breaches and cyberattacks.



Navigating these complexities calls for a shift in approach and that's where the new role of Channel partners becomes essential. They have evolved beyond their traditional role as simple tech service providers and become trusted advisors. The term "solution" now denotes more than just technology. It represents a comprehensive approach that considers all facets of a business's needs.

Success in harnessing technology today hinges on a Channel partner's ability to tailor their services to each customer's specific context, industry and challenges. The position of Channel partners goes beyond just delivering a product; it includes advice around the proper implementation, change management to ensure adoption and a host of other considerations.

Artificial Intelligence: friend or foe?

AI has the potential to revolutionise cybersecurity by automating threat detection, incident response and vulnerability assessments. AI-driven security tools can analyse vast amounts of data and identify patterns indicative of cyber threats, allowing organisations to respond swiftly and proactively to potential attacks.

This may sound enticing, but as is often the case with technological advancements, there is a flip side to consider. No, we're not going to delve into the usual concerns of AI taking over the world or developing consciousness; those topics belong to a different discussion. Instead, it is essential to highlight that new emerging technologies, including AI, bring their own security challenges by introducing vulnerabilities into businesses with no prior blueprint on how to address them.

The effectiveness of AI solutions is highly dependent on the quality of the data being fed into them. Poor or manipulated data can lead to compromised decision-making and biased AI outputs. At the same time, the mere act of pasting internal documents, contracts or information into third-party LLMs or GenAI tools almost certainly constitutes a breach of contract.

This emphasises the need for businesses to invest in secure, privately managed AI environments that are resistant to bias, intrusion, or attack.

Challenges around AI also include heightened risks of data breaches and privacy concerns due to handling vast amounts of sensitive data. Alongside these risks, introducing new technologies inevitably leads to a skill gap. Businesses are now exploring how they can best harness the benefits of AI while

MANAGED SERVICES SUMMIT LONDON

13 SEPTEMBER 2023

155 BISHOPSGATE
LONDON, UK

The 13th Managed Services Summit London is the premier managed services event for the UK IT channel. 2023 will feature presentations by leading independent industry speakers, a range of sessions exploring technical, sales and business issues by specialists in the sector, and extensive networking time to meet with potential business partners. This is an executive-level event, exploring the latest trends and developments, evolving customer requirements and how to create value through managed services – both for your own organisation and your customers.

THEMES, TOPICS AND TRENDS

The Managed Services Summit will address the key trends and issues that impact the managed services sector including:

- How to build differentiation within an increasingly competitive market
- Maximise value and increase efficiencies for MSPs and their customers
- Increasing knowledge of new technologies, processes, and best practice
- Analysing trends in buyer behaviour and successful sales strategies
- Changes and trends in regulatory compliance
- Successfully adoption of Zero trust architecture (ZTA)
- Emerging advances in AI, automation and XaaS
- The state of cloud adoption, and hybrid and edge computing
- Hybrid and remote working best practice
- Addressing the growing cyber security skills gap
- Participation with local business community leadership organisations

TO DISCUSS SPONSORSHIP OPPORTUNITIES CONTACT:

Sukhi Bhadal
sukhi.bhadal@angelbc.com
+44 (0)2476 718970

Peter Davies
peter.davies@angelbc.com
+44 (0)2476 718970

Adil Shah
Aadil.Shah@iteuropa.com
+44 (0)7516 501193

Stephen Osborne
Stephen.Osborne@iteuropa.com
+44 (0)7516 502689

https://managedservicessummit.com

maintaining a cautious approach to avoid burdening IT teams with additional security headaches.

This new landscape has placed Channel partners in a unique position to offer the education and training needed to help businesses navigate the brave new world of AI. Afterall, knowledge can often be the best solution.

Clean your room!

As businesses increasingly rely on data-driven insights and AI technologies to enhance their operations, robust security measures and controlled environments are paramount. One solution gaining traction in this complex landscape is the concept of data clean rooms.

Data clean rooms have emerged as a secure and privacy-compliant environment for fostering collaborative data analysis between multiple companies or divisions. Essentially, they provide a space where sensitive data can be analysed and shared without the risk of unauthorised access or breaches.

> This new landscape has placed Channel partners in a unique position to offer the education and training needed to help businesses navigate the brave new world of AI. Afterall, knowledge can often be the best solution

In short, a data clean room functions like a protective filter: it provides aggregated and anonymised user information to protect user privacy while still allowing advertisers, for example, to access non-personally identifiable information (non-PII) to target a specific demographic and measure their audience. This way, businesses can harness valuable insights without compromising individual privacy or running afoul of regulations.

In the era of heightened data privacy concerns and complex regulatory frameworks, the significance of data clean rooms for global businesses cannot be overstated. They serve as a testament to the evolving strategies that are required to protect valuable data assets in today's interconnected world.

Compliance with privacy laws such as GDPR and CCPA is more than a legal obligation; it's a core aspect of responsible global business operations. Data clean rooms align data usage with these regulations by safeguarding individuals' Personally Identifiable Information (PII) anonymity. By anonymising PII within the clean room, businesses can collaborate on data analytics without compromising privacy or exposing sensitive information.

In the realm of cyber and data security, data clean rooms act as a fortified shield, safeguarding sensitive information and mitigating risks associated with data sharing. This dual approach not only strengthens businesses against breaches but ensures strict adherence to data protection regulations. Think of it as killing two birds with one stone, enhancing both security and compliance.

The Human Factor

Amidst the hype surrounding emerging technologies, it is all too easy to overlook our most significant security weak point: human error. Shockingly, employee mistakes account for over 80% of data breach incidents. Given the scale of this issue, there is an undeniable and pressing need for heightened user awareness, comprehensive training programs for employees and proactive monitoring.

Fortunately, recent technological advancements are allowing businesses to distance humans from interactions where they might make mistakes. By incorporating machine learning and natural language processing into cybersecurity systems, organisations can detect cyber anomalies, fraud and intrusions with a level of sensitivity that often eludes human observers.

This reliance on automated tools is not without its challenges. The role of human oversight remains indispensable. Proactive monitoring by Channel partners can answer the challenge of human error in cybersecurity. With sophisticated surveillance and alert systems, businesses can respond immediately to potential threats, compensating for the lack of in-house expertise and adding a vital layer of defence against cyber threats.

This approach to mitigating human error continues beyond automation and monitoring. Highlighting the severity of the situation, the Department for Science, Innovation and Technology recently published a report revealing that approximately half of UK businesses lack the necessary personnel to carry out basic cybersecurity tasks.

To bridge the IT skills gap, Channel partners are investing in upskilling their clients' teams. By developing tailored training programs and automating routine cybersecurity tasks, Channel partners enable businesses to minimise the likelihood of human error in day-to-day operations. This collaborative approach allows companies to concentrate on strategic priorities while maintaining a resilient security posture, knowing they have the essential IT skills to manage complex technologies securely.

Why trust and transparency hold the key to channel success

The IT channel moves at such a pace that it can be easy to forget the foundations on which effective partnerships are built. Great technology and support are a must, of course. In helping to enable positive sales engagements, they are a key criteria for vendors and partners alike. But arguably even more important are the bonds of trust and transparency that both sides must forge.

By Camilla Currin, Senior Partner Manager at Trend Micro

TRUST in particular takes a long time to build, but is easy to lose. Maintaining it over time can be challenging, but the results speak for themselves: long-term relationships, significant repeat business and referrals, and innovative new initiatives and products to build excitement and generate new sales.

How to get there

What creates strength in channel engagement? Is it just about the lowest price? Or who responds the quickest? Or who puts on the best social activities and the biggest events? They might have some impact on partners and vendors, but are certainly not the key to building lasting relationships. That falls to trust and transparency.

The two go hand in hand. Channel businesses can't hope to build trust if they are not transparent. And transparency is meaningless without trust.
To create these bonds, it's critically important to be true to your word, time and again. It's not just a job for the channel manager, but the entire team. Only with everyone on board and pulling in the same direction will the business as a whole be seen in the same positive light. Another vital part of building trust and transparency is by taking responsibility if and when something goes wrong. There will always be hiccups in managing dynamic and complex business relationships. The key is to take ownership when something happens and ensure it's brought to a swift resolution. In fact, it's during the difficult times that the strongest partnerships are often formed. It's when you learn how important that mutual understanding is to drive the quickest and most equitable outcomes.

Trusting your vendor

These bonds of trust will carry partners through some potentially tricky times—such as during contract renewals, when partner managers are most nervous that vendor relationships may fall apart. By working closely with their vendor counterparts throughout the lifecycle of a contract, savvy partner sellers can not only protect the renewal but even gain the upsell.

In the cybersecurity channel, trust is, of course, critical not only for the vendor-partner relationship but also between vendor/partner and end customer. IT and security buyers are increasingly putting their faith in fewer vendors to deliver their threat prevention, detection and response capabilities across the entire attack surface. But although this makes absolute sense from an operational and cost-control perspective, consolidating in this way puts more pressure on the relationship. Both customer and channel partner need to be sure that their chosen vendor can deliver expertise across a broad sweep of capabilities.

That's where it makes sense to look at players who can bring decades of industry expertise to bear, with global threat intelligence and a true platform-play built from the ground up.

Navigating the cybersecurity landscape: A guide for channel partners in 2023

The cybersecurity landscape is undergoing a notable shift as we enter the second half of 2023. Developments such as the persistent threat of ransomware, and the introduction of new legislation such as DORA and the NIS2 directive have forced companies to rethink how they approach security. More enterprises accept that preventing all breaches is no longer possible. Instead, the focus now is on resilience, containment, and the ability to operate even in the face of an attack.

By Scott Walker, Senior Director of Channel Sales for Illumio

THE CHANNEL is at the forefront of this transition, guiding organisations through the complexities of this new cybersecurity paradigm. As such, the role of channel partners has never been more critical. They are the linchpins, enabling enterprises to navigate the intricacies of cyber resilience and adapt to the changing tides of technology.

Embracing the shift to cyber resilience

Ransomware and legislative changes have accelerated security transformation. However, this shift is not just a reaction to the threat landscape. We are also seeing enterprises proactively adopting an "assume breach" mindset and moving towards more robust and resilient security postures. It is understood that threats are inevitable in the digital era, but their impact can still be mitigated.

As IT environments become larger, more complex and distributed, organisations face more vulnerabilities and visibility gaps. The channel has a crucial role as an educator to help organisations plug these gaps and develop a security architecture that is futureproof. This requires not just the adoption of new technologies, but a rethink of security strategies and how organisations can build an IT infrastructure that is resilient by design.

Partners can tap into this opportunity by guiding businesses toward more mature and integrated security approaches that reduce the need for numerous point solutions, such as Zero Trust. They should also be developing a bill of materials that can deliver a best-of breed architecture to help customers reduce costs and provide better value. In this era of doing more with less, it's also important the channel enterprises to maximise their existing investments through better use of current tools and technology. The focus is shifting from "how can we help customers bring on more technologies?" to "how can we help them leverage the ones we have and find ways to complement and grow them?"

Maximising investments in the face of economic challenges despite the financial crunch, companies are still increasing investment in security. IDC estimates a 12% global increase in security spending across 2023. However the current economic climate has put a greater focus on return on investment (ROI). This return isn't just about financial benefits; it could be risk reduction, reduced downtime, or improvements in operational efficiency.

In this environment, customers are demanding the biggest bang for their buck. They want to know how to make their existing tech stack work harder. As we move into the second half of the year, we expect to see better-defined, understood, and executed projects as a result. The current economic climate is certainly forcing organisations and channel partners to align projects to business needs. Channel partners must consider their long-term investment in technologies and how they can help customers maximise their existing tools and processes. Those that have already been working as trusted advisors will have a valuable opportunity to strengthen their relationships. Partners that have previously been more focused on volume however may need to reevaluate how they work with their clients.

The current market provides a strong chance to reposition as a strategic long-term partner rather than a tactical advisor. We've already started to see channel partners think more strategically and define a roadmap more effectively.

The future of security: Zero Trust Segmentation

As well as taking a more strategic approach, channel partners should also reevaluate their portfolio to ensure they are offering solutions that can both provide optimal ROI for customers, as well as long-term returns for themselves. One of the most significant areas for growth is microsegmentation or Zero Trust Segmentation (ZTS). Gartner recently predicted that by 2026, 60% of enterprises working toward Zero Trust architecture would use more than one deployment form of microsegmentation, up from less than 5% this year. Zero Trust Segmentation has transitioned from a nice-to-have to a must-have, presenting a huge revenue and growth opportunity for channel partners.

Many organisations have already embarked on their Zero Trust journey and are wrapping up Zero Trust Network Access (ZTNA) deployments. Zero Trust Segmentation is the next logical step for these projects and serves as a critical pillar in any Zero Trust architecture. Channel partners have a unique opportunity to guide their customers through this transition, helping them understand the benefits of Zero Trust Segmentation and how it can enhance existing security stacks.

> Many organisations have already embarked on their Zero Trust journey and are wrapping up Zero Trust Network Access (ZTNA) deployments. Zero Trust Segmentation is the next logical step for these projects and serves as a critical pillar in any Zero Trust architecture

Zero Trust Segmentation is also well suited for the drive towards resilience. Dividing the network into airtight sections significantly reduces the impact of a breach, especially fast-moving threats like ransomware. A Forrester Total Economic Impact™ study of Illumio's Zero Trust Segmentation platform, commissioned by Illumio found that Illumio ZTS can decrease overall risk exposure to an equivalent value of $18m and reduce the cost of downtime by $3.8m. Other benefits include improved security operational efficiency, better regulatory and insurance compliance, and improved accuracy and granularity of configuration management database (CMDB).

Navigating the future of cybersecurity together

The shift towards cyber resilience, the need for streamlined security architectures, and the focus on maximising existing investments are all trends set to continue. This means that the future is full of meaningful changes and the role of the channel has never been more critical.

Channel partners stand at the forefront of these changes, guiding their customers through the complexities of the digital era and empowering them to face these challenges head-on. The opportunity lies in helping organisations secure any gaps and developing a security architecture that fits the purpose for years to come. While the cyber challenges faced by enterprises are complex and ever-changing, with the right guidance and support from their channel partners, organisations can navigate these challenges successfully and build a more secure future.

How to help customers rationalise security portfolios

The world of IT security is becoming ever more complex and riskier.

By Francis O'Haire, Group Technology Director, DataSolutions

IN CONJUNCTION, businesses are seeing their own IT environments become more complicated and distributed. Your customers will be grappling with the likes of multi-cloud environments, remote and hybrid working practices to name but just a few. They need resilient cybersecurity strategies that allow them to run their businesses smoothly, whilst also protecting against any potential security threats.

And let's not forget about the current economic backdrop. With a tightening of the purse strings there is an ideal opportunity for you to guide your customer through a consolidation process. With everyone painfully aware of the cost-of-living dilemma, how many security products does an organisation need, or use? And with the channel becoming ever more useful as a source of help for customers, this is a great time to offer the expertise and guidance necessary to help customers stay secure in a cost-effective way.

Keeping pace

To keep pace with this evolving threat landscape, most organisations have had to bolt on new cyber security technologies as they've become available over the years. There are several ways to address the resulting complexity, but the best approach very much depends on the specific needs and capabilities of each business. In an ideal world or for organisations that are starting out from scratch, a unified platform from a single vendor is the best approach. Visibility is key here - dealing with one vendor who offers a standalone solution and yet another for a different solution, is a sure way to lose sight of the overall picture when it comes to securing any IT estate.

Consider an MSSP

For smaller businesses that do not have the in-house skills, engaging with a Managed Security Services Partner is the best option. Customers can benefit from highly sophisticated cyber security protections, developed, and managed by the MSSP, without needing to have the skills or deal with the complexity themselves. Many SMBs choose to work with a MSSP to mitigate the pressures that they face in all aspects of information security - malware, data theft, skills shortages, limited resources, evolving cyber threats etc. It pays to remember the falsehood that cyber security isn't as important for SMBs as it is for larger organisations. Cyberthieves are particularly keen to target smaller businesses because they are normally poorly defended from a cybersecurity point of view and offer easy pickings.

Security data

For larger organisations, or indeed MSSPs that have built up their own cyber security capabilities using many point solutions and that are not able to abandon them in favour of a unified platform, there is the option of lowering the complexity and cost of managing the entire stack while also increasing its effectiveness using SOAR (Security Orchestration, Automation and Response). SOAR technologies, from vendors like D3, allow larger organisations to collect and aggregate huge quantities of security data and alerts from myriad sources. SOAR allows point solutions from different vendors to be integrated while correlating and automatically making sense from, and prioritising, all the event data coming from those solutions.

SOAR can also help organisations with the very real resource constraints that exist in the cybersecurity market. Businesses of all shapes and sizes are having to deal with a cybersecurity skills gap and SOAR can help to address the talent gap through automation. The technology allows security teams to prioritise the most immediate threats and gives them enough time to deal with them. By automating repetitive tasks, you free up (human) resources allowing you to target areas that require people input.

Now is an ideal time to be helping customers to rationalise security portfolios. With a cost-of-living crisis and challenging economic conditions, your guidance and expertise can help businesses, both small and large, to continue to operate safely and securely in the face of an evolving threat landscape.

Huntsman®

MSSP SIEM

A mission critical cyber security analytics application that deploys from a single SOC platform managed by your team.

TRUE MULTI-TENANCY

INTEGRATED MITRE ATT&CK® SUPPORT

FULLY FLEXIBLE, INCLUDING DATA SOURCE SUPPORT

SCALABLE AS YOUR BUSINESS GROWS

BOOK A DEMO

huntsmansecurity.com

Empowering the Channel for Unified Cyber Defense

Recognising and rewarding channel efforts in maintaining a secure ecosystem, along with continuous training opportunities reinforces their importance and fosters a strong cybersecurity ecosystem.

By Spencer Starkey, VP EMEA, SonicWall

THE STATE of cybersecurity in 2023 is full of escalating threats. Ransomware attacks and data breaches, which frequently target individuals, businesses, and governments, are very prevalent forms of cyberattacks.Supply chain attacks and remote work vulnerabilities gained prominence due to the COVID-19 pandemic, as well as Internet of Things (IoT)malware attacks, attacks which target smart devices. Businesses must be prepared and protect themselves against all attack types.

Investing in the right cybersecurity tools is essential, especially in today's ever-changing threat landscape. Opting for the very best options ensures comprehensive protection.

Sales channels in security are pivotal for businesses due to their ability to extend market reach, leverage specialised expertise, manage distribution logistics, and enhance cost efficiency. Collaborating with established channels offers access to better market insights, resources, and brand visibility, while also sharing risks and diversifying revenue streams.

Having this kind of partnership-driven approach allows businesses to adapt to changing market conditions, build customer relationships, and optimise growth strategies. By harnessing the strengths of various sales channels, businesses can effectively connect with target

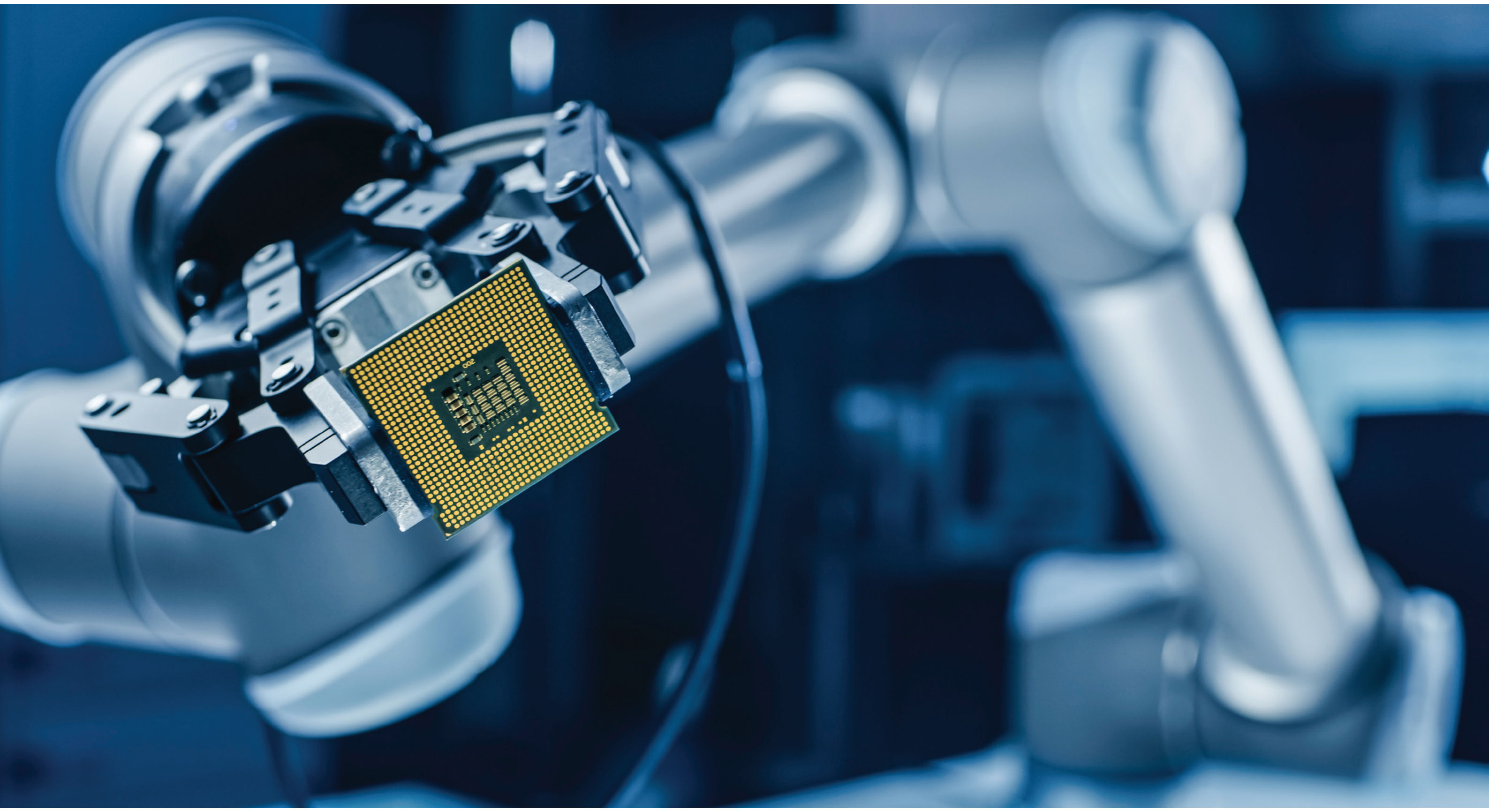
audiences, streamline operations, and capitalise on opportunities for expansion. Cybersecurity must be a priority for all in the channel due to its critical role in safeguarding customer data. Ensuring robust cybersecurity measures helps maintain the reputation of both the channel and the brands it represents, while also complying with legal and regulatory requirements. By protecting against cyber threats, sales channels can avert potential financial repercussions, sustain business continuity, and gain a competitive advantage. Also, strong cybersecurity practices positively impact relationships within the supply chain and underline the channel's commitment to security in an increasingly digital business landscape.

For us at SonicWall, customers are extremely important. "Listen more and talk less" is a key mantra for vendors seeking a strong and successful relationship with channel partners. Vendors can gain a lot from listening to where channel partners are going with their businesses, their requirements and their pain points. A widening attack surface, supply chain disruptions and a flurry of never-before-seen malware variants are proving very difficult to manage. Having a strong understanding with partners is key to making sure it is able to provide better technology and support.

There are no signs that security threats are reducing, with everyone a target. A recent report from SonicWall found that within the UK alone, malware attacks on IoT are up 53%. As well, the rise of cryptojacking, an attack method that isn't so widely known, has risen 479% YoY. Cryptojacking is a virus that, once infected into an unaware device, will endlessly mine for crypto, funding all sorts of illicit activities.Therefore, putting IT security investments on hold will only risk exposing users to more threats long-term. Cybersecurity organisations can do this by supporting partners in driving sales and revenue, training and enablement, and knowledge sharing to build community and flexible pricing and consumption models that match how partners do business.

Cybersecurity organisations also play a crucial role in aiding the security of sales channels beyond products, through having the threat experience and intelligence. They can provide essential cybersecurity solutions such as linked software tools and incident response planning, while guiding the creation of robust security policies. Continuous monitoring and vendor risk management help safeguard against cyber threats and ensure regulatory adherence. Collaborative threat sharing and awareness campaigns further empower sales channels to develop a strong cybersecurity culture and respond effectively to evolving risks, ultimately enhancing their overall cyber resilience.

Creating channel satisfaction through a cybersecurity lens involves nurturing relationships built on trust, transparency, and a shared commitment to cyber resilience. By providing regular updates on security measures, promptly addressing concerns when they arise, and offering guidance on risk mitigation strategies, businesses can ensure that sales channels feel equipped and valued in their role as cybersecurity allies. Recognising and rewarding channel efforts in maintaining a secure ecosystem, along with continuous training opportunities reinforces their importance and fosters a strong cybersecurity ecosystem. This way, businesses can forge a lasting relationship based on shared cybersecurity goals, ultimately promoting channel satisfaction and collective defence against cyber threats. The cyber fight wages on and businesses must be able to trust all elements of their security.



Why aren't MSSPs fully capitalising on their technologies?

It's now down to vendors to attend to the unique needs of MSSPs or risk holding back the market.

By Matthew Rhodes, Regional Director for MSSPs at Logpoint

EVERY MSSP knows that the future to increased revenue lies in automation. And yet, according to a recent survey, many MSSPs say that their ability to create new, value-added service packages remains limited not because of lack of innovation but because of the inflexibility of the market. This is partially down to the inelastic pricing of MSSP services in the eyes of the customer. One of the main reasons companies seek MSSP services is to lower costs, so to justify a price increase, the value must be compelling. In addition, solutions just aren't built with the MSSP business model in mind, which means they then need to self-limit their use of the technology.

MSSPs must invest in emerging technologies that add value to the SOC and integrate with the Security Incident and Event Management (SIEM) system. They cannot afford to stand still which is why there is now a focus on automated threat detection and response in the form of Security Orchestration, Automation and Response (SOAR) and Unified Entity Behaviour Analytics (UEBA).

New revenue streams

Both offer the prospect of new revenue streams. SOAR allows the MSSP to use playbooks mapped to the MITRE ATTA&K framework to detect, respond to and mitigate threats automatically. UEBA, on the other hand, builds baselines for user and group behaviour used to identify unusual patterns and fend off unknown and insider threats. Any anomalous behaviour on the network that falls outside of these boundaries is flagged for analysis in real-time.

Those MSSPs offering SOAR have found customers value the best-practice workflows and playbooks that trigger incident response actions, according to the report. It found that the MSSP was able to deploy the SOAR across the customers own technologies, such as firewalls, Endpoint Detection Response (EDR) and other tools.

What's interesting, however, is that the survey also revealed that MSSPs are only partly utilising these solutions. They're frequently restricting the use of SOAR to data consolidation, enrichment and normalisation (which happens behind the scenes), rather than using it for automated incident response (which would be a chargeable service).

Failing to capitalise on investment

The reason given for this is that the MSSPs claim SOAR is not something that works for them out of the box, without any modifications. SOAR requires planning and needs to be discussed with customers because every customer may have a different setup. In reality, while automation speeds up processes and takes the load off analysts, automating incident detection and response processes in a single company is quite different from automating MSSP processes for hundreds of companies. The best response for a 50-person company may not be the best response for a 5,000-person company. However, not capitalising on the investment in SOAR makes little sense, particularly as those customers that are using it with their own technologies clearly relish the benefits. So, what needs to happen to change this?

Ultimately, the market needs to cater to their needs. MSSPs need a clear path to new service creation and that means they need SOAR vendors who can simplify the process. What they're looking for are flexible licensing options, for instance, and hands-on training to teach MSSP analysts how to design playbooks and implement use cases to speed response and shorten SLAs. As the MSSP begins to work with each customer to get the right rules and playbooks in place, this will increase visibility, which in turn will see customers become more well disposed towards such services and come round to the idea of paying more for the privilege.

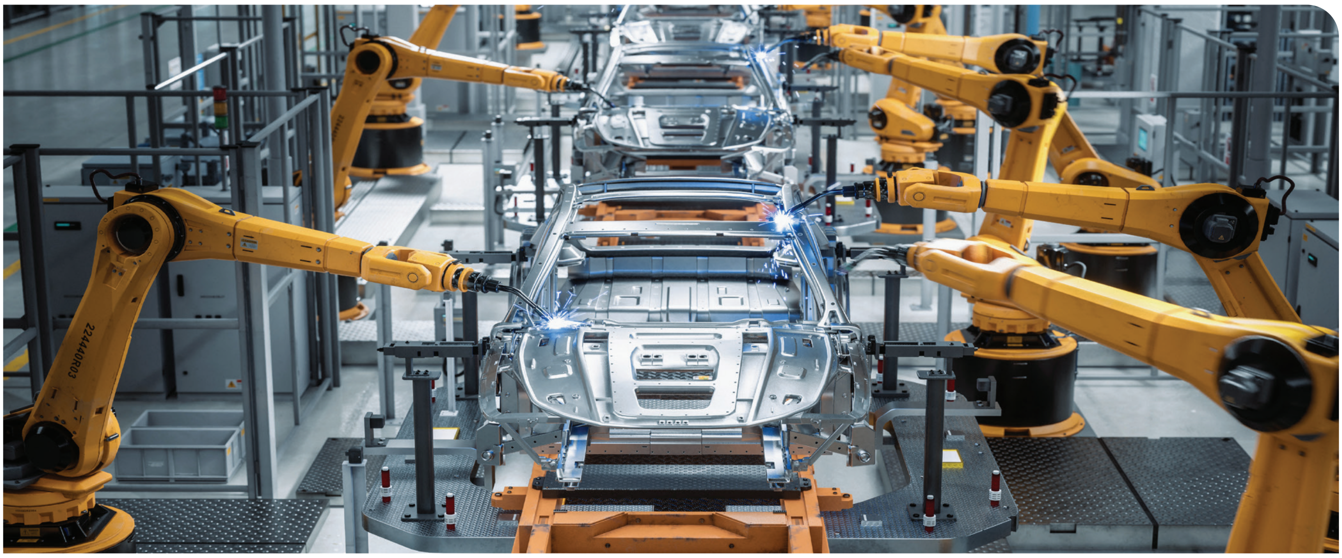
Overcoming the challenges

MSSPs who have deployed UEBA have found this to be more challenging due to licensing structures and the data volumes involved. UEBA analyses masses of data and requires significant infrastructure capacity. So MSSPs will seek to converge these new technologies with existing SIEM platforms, making it easier to deliver a wide array of cybersecurity services under a converged and predictable licensing structure.

In an ideal world, MSSPs want to be able to use a single platform to work on event data from all clients at the same time, rather than have their analysts working in customer silos. According to the real-life experience of MSSPs, the best features are those that allow flexible configurations and easy customisations per client. MSSPs don't want to be limited by an interface that provides a o ne-size-fits-all menu of clickable boxes and buttons.

To get to this point, they must be able to build working relationships with vendors to help configure and support the solution for rollout across their entire customer base. It's a working relationship that can also help benefit the MSSP by allowing them to build up an understanding of the inner workings of the cybersecurity platform and to influence roadmap decisions to assure the continuity of affordable services and efficient operations.

But the danger today is that vendors continue to produce cybersecurity platforms and solutions for 'the enterprise," when MSSPs need platforms and solutions that will allow them to manage hundreds and perhaps thousands of enterprises at the same time, and from a central and unified management tool. Unless something changes, MSSPs will invariably only leverage some of the feature sets in these solutions, and MSSP investment overall is likely to remain low. It's now down to vendors to attend to the unique needs of MSSPs or risk holding back the market.



Navigating new horizons in cybersecurity

Empowering end users through Channel innovation.

By CompTIA

The IT industry is undergoing rapid change. To keep pace with changing and advancing technology, cybersecurity is also undergoing a significant transformation. The Channel plays a pivotal role in matching cutting-edge cybersecurity solutions to its end users' security needs.

However, connecting businesses with relevant, sophisticated cybersecurity solutions requires an understanding of the evolving threat landscape and the concerns plaguing end users. By keeping a watch over the developments in the industry, the Channel can effectively tailor its offerings to ensure robust security measures.

The new frontier: Emerging technologies and demands in cybersecurity

The cybersecurity landscape is evolving fast, driven by the emergence of new technology, and mobile working demands which have especially heightened post-pandemic. These changes could reshape not only the way we interact with technology, but also how we safeguard our devices and infrastructure against new types of cyberthreats.

Some of the prominent technology rising in popularity includes AI and ML, which are being leveraged to analyse massive datasets, identify patterns, and detect anomalies that may indicate cyber threats. Other new considerations include blockchain technology, suitable for securing data integrity, supply chain transactions, and digital identities, as well as 5G security for high speed, mobile data, and protection across complex networks of connected Internet of Things (IoT) devices.

The demands in cybersecurity reflect these evolving uses of tech and their use to create advanced cyber threats. Organisations are increasingly seeking solutions that encompass zero-trust principles, leveraging AI and machine learning for proactive threat detection as cyberattackers attempt to use them for attack vectors. The development of cybersecurity solutions falls to the providers, but even the very best software can be weakened by human error. As such, with increasingly complex threats and solutions, cybersecurity strategy and education also becomes integral to businesses.

Patrick Burgess, co-founder and CEO of Nutbourne and a member of CompTIA, agrees: “We are seeing a huge demand for wider strategy and education. Businesses have become increasingly aware of the need to do something since the pandemic, but they aren't sure what!

"They need trusted partners to guide them in the right direction as fast as possible within the budgets they have. The irony is that getting the basics right doesn't cost a huge amount. But clients don't know what they need to do, and they have other day-to-day priorities within their business.. They want the problem to go away. We need to teach them that it won't - but we can help them reduce the risks."
The Channel can play a vital role in providing education and strategic guidance to its end users through various proactive approaches. Organising workshops and webinars focused on cybersecurity best practices, emerging threats, and strategic planning can empower end users with valuable insights, and help connect customers with ideal solutions.

These sessions can cover topics such as secure remote work, data protection, incident response planning, and regulatory compliance. Moreover, tailored training programs that address the specific needs and challenges of individual organisations can be developed. These programs could include hands-on simulations, role-based training, and practical exercises to enhance participants' understanding of cybersecurity strategies.

By adopting a holistic approach that combines cybersecurity technology technology solutions, including education, practical training, and strategic consultation, the Channel can empower end users to proactively address cybersecurity challenges and develop robust strategies that align with their business objectives and risk tolerance.

Common end-user concerns for Channel resellers

While taking into account emerging technologies and demands is significant for the Channel, it is crucial that it acknowledges the security challenges that end users face, to provide effective and relevant cybersecurity solutions.

The rising frequency of ransomware and malware attacks has left end users vulnerable to data breaches and extortion, and are one of the most dreaded attacks.. Cybercriminals have refined ransomware tactics, locking users out of their own data. Under the threat of data exposure, and without access to critical files, many victims feel pressured to pay exorbitant sums to recover their property. The evolving tactics employed by cybercriminals have underscored the pressing need for proactive measures and digital defences.

To thwart the devastating impact of ransomware attacks, the Channel can offer end users cutting-edge backup and recovery solutions with their cybersecurity solutions. These encompass continuous data backup, secure storage, and rapid restoration mechanisms. By implementing these solutions, organisations can swiftly recover encrypted data and maintain operational continuity, rendering ransom demands ineffectual.

Another key challenge that end users face is regulatory compliance. Navigating complex cybersecurity regulations can be daunting for businesses. Data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), impose stringent requirements on how personal data is collected, processed, and stored. Achieving compliance often involves substantial changes to data handling practices.

To help tackle this, Channel resellers should implement training to guide end users through compliance requirements and offer solutions that ensure data privacy and regulatory adherence.
Finally, supply chain vulnerabilities have also become a significant concern for end users.

Modern organisations operate within complex and interconnected ecosystems where various components, services, and technologies are sourced from third-party vendors. This interconnectedness increases the potential attack surface and provides cybercriminals with multiple entry points to exploit.

Channel resellers can assist by conducting comprehensive risk assessments of third-party vendors to evaluate their cybersecurity practices, identify vulnerabilities, and gauge their overall security posture. Performing regular security audits of vendors' systems, processes, and technologies can also help uncover potential weaknesses and ensure that vendors adhere to best practices.
John Fisher, another CompTIA member and Managing Director of Westway IT, underscores this point, stating, "Cybersecurity has a complexity and fluidity that is hard to always grasp. Issues that you think may not affect you directly can have impact elsewhere in your supply chain. Having sight of the latest threat intelligence helps, as does having community driven solutions and advice on how to better protect your business".

"Trying to tread the path alone is not easy, especially when we need so many layers these days to offer a good level of protection, and trying to educate clients on the real need to improve their security.
Collaborative problem solving to unlock Channel growth

By harnessing emerging technologies, understanding end user concerns, and working collaboratively to educate their customers, the Channel can serve as a guiding light, providing the necessary solutions and support to fortify digital defences. As the digital realm continues to expand, the partnership between the Channel and end users will undoubtedly play a pivotal role in shaping a more secure and resilient digital future.

Channel Partnerships – Paving the way for fundamental security resilience

With so many cybersecurity solutions available on the market, customers can be left feeling underwater. Uncertainty around how tools can mesh into current IT and OT infrastructure, coupled with lack of resourcing and economic constraints can present a challenge in choosing the right technology to bolster their security.

By Ed Baker, VP Global Channel Sales, Trellix

THIS IS WHERE channel partners come in. Offering consultative, strategic advice and bespoke solutions, partners with security expertise can equip businesses with valuable resources and knowledge around the dynamism of the cybersecurity ecosystem. Whether that's by enabling CISOs to make fully informed decisions around choosing their cybersecurity tools, providing outsourced security, or streamlining existing security architecture; there is an opportunity for channel partners to help protect end-customers from threats.

Here we explore how partners are best placed to enhance customers' resilience and provide them with real value, as they navigate the cyber threat landscape.

Business decisions in uncertain times

It's safe to say that the global economy has been unpredictable at best. This uncertainty has continued to filter through to the cybersecurity and wider technology markets, as macroeconomic factors like inflation and high interest rates have impacted market confidence.

Customers are growing more cautious about investing in new technologies, as long-term return on investment isn't always clear.

As budgets tighten, the ability to resource and support robust security infrastructure also weakens. Many mid-sized customers are now finding themselves struggling to establish or maintain in-house security teams with the capabilities to mitigate threats. Without the adequate skillsets or technology required to bolster security, they are subsequently looking to external alternatives.

By outsourcing certain security functions to an MSP or MSSP, organisations can better reduce the risks posed to them. Providing the resources, expertise, and technology to plug the gap, MSPs and MSSPs can help customers manage their security ecosystem.

Services within the channel can also help support end users when it comes to choosing the right solutions. Distributors and system integrators can offer bespoke, strategic advice and training throughout the purchasing process which can prove invaluable for customers. While independent procurement can muddy the water, the channel offers clarity as to how exactly each solution can be maximised. This offers more flexibility to how cybersecurity solutions can be purchased, and transparency over return on investment.

Ultimately, by consulting channel partners around purchasing decisions and integrating new security solutions, CISOs can be confident in a more secure organisational environment. Whether supporting in-house operations or resourcing external security offerings, in considering the bigger picture, channel partners are well placed to curate a more aligned security mindset.

The importance of removing siloes in security

Organisations are becoming more exposed to threats, and so CISOs and other decision makers are increasingly looking to more sophisticated security solutions to protect their businesses. Research from Trellix found that two-thirds (64%) of UK CISOs had over 20 disparate solutions in place – fed by the often-misguided thought process that layering multiple security tools on top of each other is a more effective form of security. In reality, we can see that having a more focused, streamlined approach eases the monitoring management of an organisation's security environment.

Cyber-attack surfaces are dynamic and flexible, with threat actors constantly changing the game, integrating new tools into their cybercrime initiatives. Here is where channel partners, value added resellers and systems integrators play an active role in consolidating and condensing security solutions. In turning to MSPs and MSSPs, businesses can remove silos and increase visibility by 'connecting the dots' between disparate solutions.

This enables customers to navigate the complex security environment and support their IT and OT infrastructure by reinforcing their internal security. This value proposition fully measures return on investment – especially when businesses fall into the trap of investing in too many siloed solutions. Diversity in offering is helpful, however, ensuring products from multiple vendors mesh and complement one another to plug an attack surface. Channel partners are the bridge in making cybersecurity technology more accessible to customers, driving sales and bolstering market confidence.

How the channel will evolve

It's difficult to fully predict how the cybersecurity technology market will evolve. Solutions – much like the threat landscape and the wider economy – are continually changing. However, whether it worsens or improves, the channel landscape will continue to adapt and remain resilient.

Channel partners will play a core role here. Partners should continue to unlock value for end-customers and ensure security objectives are met. By aligning business goals and the hunger to grow through dynamic innovation and a positive security culture, we will see relevant, valuable partnerships form. This will provide customers with both the financial and cyber security to withstand changes in the market and remain resilient to threats, both now and in the future.

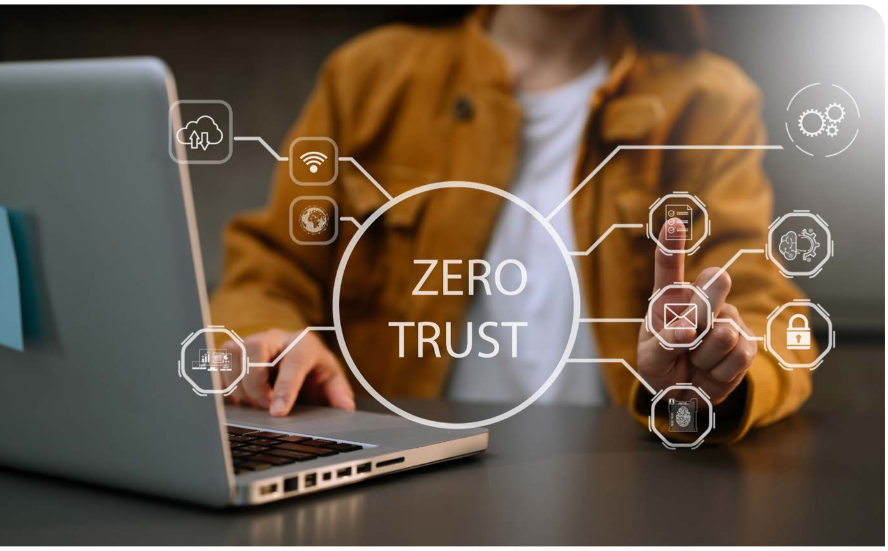
The quest for an zero trust endpoint security solution

Apex Computing Services in Manchester, talks about the lack of cybersecurity awareness for many organisations, the issue of mistaken downloads leading to continuous security breaches, and how Threatlocker has stepped in to provide better protection for all.

By Nathaniel Gill, Head of Cyber Security at Apex Computing Services

SDC: *Tell us a bit more about Apex Computing Services and your role?*

NG: Apex Computing Services is a well-established computer services business that is 20 years old this year. With offices in Manchester city centre and Salford Quays, Apex offers the full spectrum of IT services including installation and support, repair and maintenance, email and internet and software development. It works in many markets across the North West - hospitality, legal, security and professional services. I work as Head of Cyber Security at Apex tackling many issues including those created by downloading unverified software.
Why did you start to look for a Zero Trust endpoint security solution?
We were facing daily challenges associated with customers downloading unverified software which compromised the security of their devices. A general lack of cyber security awareness was resulting in continuous breaches - downloading free versions of software was a nightmare - and we were seeing quite significant increases in workload as we had to constantly deal with sorting out the threat.
It is amazing the lack of due diligence schools and others show before installing new applications on the Internet. It became so hard to properly secure a customer's IT infrastructure without any proper training or understanding at their end.



So we started to look at Zero Trust as a solution. We wanted to carry on providing the best service that we could to our customers without being overly expensive and losing out to cheaper options in the market. We just wanted to do a better job of protecting our customers' environments.

SDC: *What was the benefit of Zero Trust?*

NG: It was easily deployed from a centrally-managed platform and immediately gave us better visibility on all user endpoints. The Zero Trust controls stopped 'fileless' malware and limited damage from application exploits straight away, and I am delighted to say we have had no reported breaches since we started using Threatlocker to partner with us in this space. This has resulted in much less fire-fighting across the board.

How do you deliver customer peace of mind?
It was essential for us to create a bundle of services that could enhance our end-user cyber security stack. So, when we were looking for an application whitelisting solution, we went for Threatlocker. That was just over 18 months ago now. The main reason we wanted to partner with ThreatLocker was it allowed us to screen any software that was being run or had been installed on our end customer networks and devices. It was also then possible to create compliance lists for cyber essentials and

ISO certifications because you can pull the lists off the approved software. It gives everyone maximum peace of mind.

SDC: *How do you curtail the damage caused by 'unaware' end users?*

NG: We have found that implementing zero trust controls to 'deny by default' is absolutely the best way to prevent untrusted software from running regardless of customer actions. Being an MSP, I look at how easy it is to deploy and manage a centrally-managed platform with a lot of clients. You can go from one to the other really easily and the support from the Threatlocker team is second to none.

SDC: *How was the onboarding process at Threatlocker for you?*

NG: It was seamless. The Cyber Hero team has provided support from the trial period until now. No issue was too small. So even if we had a tiny problem that was affecting what we were seeing, the Threatlocker team would jump straight on it, help us out, and get results for us as quickly as possible. It was important for us to partner with a company that shared our values and beliefs. When we looked at ThreatLocker's mission, we felt it was very much in line with ours, so all the focus is on ensuring our customers are the safest and happiest they can be.

How has Threatlocker impacted your business? By implementing Zero Trust, our business has benefited exponentially.

The primary metric that I look at is how often our customers are being breached. Since installing ThreatLocker on our customers - 85 at the last count - we've not had a single customer report a breach or virus, which is astonishing.

They have also significantly reduced our global ticket volume, which was predominantly coming from users making mistakes and then being helpless as the mistakes created issues for them. The product is great, and it helps protect our customers without being overly expensive and our customers no longer need to worry about their mistakes racking up huge fines.

We have also taken on the Endpoint Network Access Control (NAC) solution from Threatlocker in recent months. This has been especially beneficial for smaller customers who do not have firewalls in place, and better protects remote workers, helping to cut down malicious traffic.

We have now created a cyber security bundle to protect customers across the board with Threatlocker at its heart. The team is super competent, the product performs and we have had no breaches. You cannot argue with that.

Dispelling four common misconceptions about hard disk drives

Hard disk drives (HDDs) have now disappeared from most computer terminals, but it would still be wrong to regard this classic form of storage as obsolete. After all, many prejudices that have developed over recent years do not hold up on closer consideration, dispelling the most widespread misconceptions.

By Toshiba

HDDs do not deliver state-of-the-art performance: An Enterprise hard disk drive with 250 megabytes per second and 400 IOPS certainly cannot keep up with a single Enterprise SSD (solid state drive), which transfers around 2,500 megabytes per second and achieves 100,000 IOPS. However, unlike in computers, storage systems used by companies, cloud providers and hyperscalers do not contain just one data storage medium in any one case - storage arrays are usually equipped with several dozen drives. In such a network, hard disk drives manage over 5 gigabytes per second and more than 10,000 IOPS, sufficient for many modern applications. Since their unit costs are significantly lower than those of SSDs, it is also more economical to equip the systems with many HDDs rather than a few SSDs.

HDDs have a shorter service life: The hard drive mechanical elements, with their moving parts, are often said to cause high wear on HDDs. However, they do not fail more quickly or more often than SSDs – the mean time to failure (MTTF) of most HDD and SSD models in the Enterprise class is 2.5 million hours, which equates to an annualised failure rate (AFR) of 0.35 per cent. In a data processing centre with 2,000 drives, this means that, in statistical terms, companies need to replace seven hard drives per year. To avoid a higher figure, they should make sure that they observe the ambient conditions specified by the manufacturers, such as temperature and vibrations, and use the hard drives in accordance with their intended purpose. Desktop HDDs are not designed for 24/7 operation, and with the high workloads in a server or storage system, they wear out quickly. Generally, they cope with a workload (rated workload) of 55 terabytes per year, while NAS HDDs can cope with 180 and Enterprise HDDs as much as 550 terabytes per year.

HDDs consume a lot of electricity: The hard drive’s mechanics are also often rated negatively in terms of power consumption, but modern drives with helium filling are pretty frugal. Since most of the energy is used to rotate the spindles, their power consumption is about 7 to 8 watts, regardless of capacity and workload. SSDs which provide a similar amount of storage capacity as hard drives require just as much, if not more, power for the same data throughput. However, their power consumption depends directly on the capacity, whereas hard drives always have a specific base power consumption for spindle rotation. SSDs, therefore, score well at capacities below one terabyte, which is the case in most portable and battery-powered devices.

HDDs are yesterday’s technology: In terms of basic technology, hard drives may not have changed since their early days, but the components, materials and recording methods are constantly evolving. As a result, the storage capacities of the drives have been increasing by about two terabytes per year for some time now, with the costs remaining unchanged. In 2021 the first models using the new MAMR (Microwave Assisted Magnetic Recording) recording method came onto the market. Here, microwaves at the write head control and concentrate the magnetic flux so that less energy is needed to magnetise the bits. Consequently, the write heads can be smaller and write data more densely. According to experts, the further development of MAMR will increase the capacities of hard drives to up to 50 terabytes in the next few years.