Building resilience in the age of AI
A guide for channel partners

ENVIRONMENTAL VALUE – THE SI OPPORTUNITY

Countries are coming together to address the financial implications of climate change

THE PATH TO DIGITAL MATURITY

Embracing digital transformation to reshape your growth strategy

AUGMENTING YOURSELF WITH AIREDEFINED

Customer service have risen, with emphasis on anytime, anywhere, any channel responses
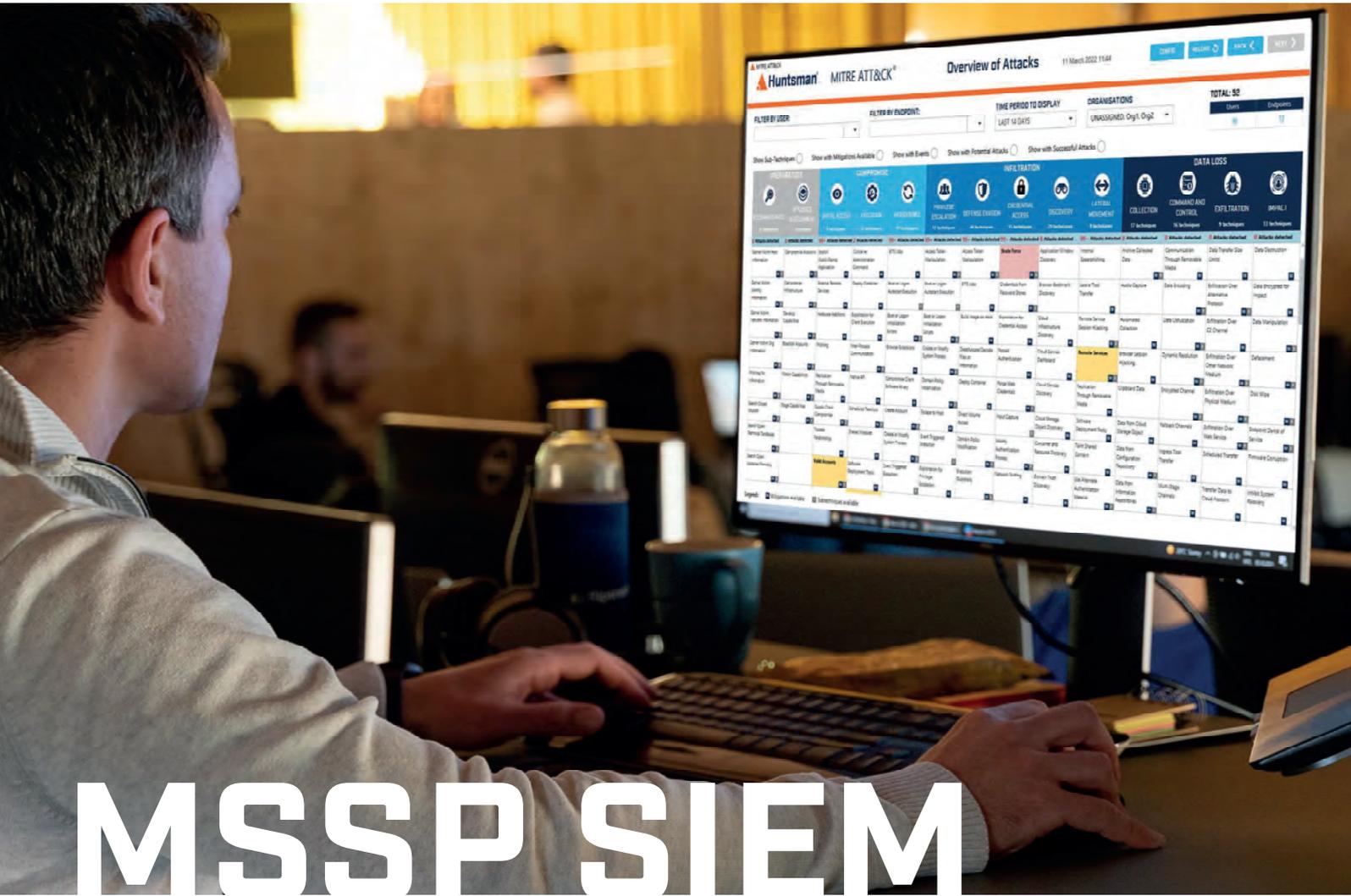
VIEWPOINT

By Phil Alsop, Editor

AI – be careful what you wish for

HOT ON THE HEELS of the increasing requirement for MSPs to turn themselves into MSSPs to help their customers deal with the very real problems of cybersecurity, we now have the distinct possibility that MSPs will soon be required to evolve into MAISPs for the same reason.

After all, if the ongoing challenge of keeping IT infrastructure safe and secure is beyond the expertise of many an enterprise, we can be fairly certain that the complexities of AI will add a whole new layer of incomprehension for end users. Yes, I am sure most if not all have played around with 'basic' (but really very complex!) AI applications which allow articles and presentations to be written based on a few key words and prompts, but the type of AI and associated Machine Learning capabilities already heading to organisations of all shapes and sizes requires expertise somewhat beyond the ability to type!

And, of course, AI is not totally separated from cybersecurity. Yes, the technology can be harnessed to improve IT defences but, alas, it can also be enlisted by the bad actors to 'improve' their criminal activities. No one can say with certainty how the AI landscape will develop. At one end of the argument are those who predict that AI will decimate the jobs market – replacing millions if not billions of workers as we head towards a dystopian future that might just rival climate change as a global societal disruptor. At the other, we have the optimists who believe that AI will work largely in tandem with humans, and also create a whole new set of jobs as yet not fully understood. I suspect the truth lies somewhere in between.

Of one thing I am sure, the talk of AI and ethics, or ethical AI, is a non-starter. Big tech already drives a coach and horses through the best attempts to regulate its power and dominance. And the pursuit of profit already overrides any serious consideration of what is 'right'.

No matter how often quoted, the idea that any infringement of a powerful organisation's intellectual property is spotted and clamped down on within seconds by the big tech companies, while at the same time they claim to be unable to intervene when it comes to matters of 'free speech' (as regulating such things brings no profit), becomes no less powerful a symbol of the horrible place we have reached.

AI will just make this bad situation far, far worse. Apologies if this sounds bleak, but if history teaches us one thing (and sadly it does not appear to be teaching many politicians many things right now), it is that, once the genie is out of the bottle, there is no going back.

In conclusion, by all means enjoy the fantastic things which AI will enable, and the opportunity it provides the Channel to help end users embrace a brave new world, but don't be surprised, let alone angry, when AI causes levels of work-related and social chaos that makes the current cybersecurity landscape look like a summer's day picnic.

18

NEWS

10

Companies' reliance on IT Managed Services increases in 2023

IT channel partners selling managed services are poised for robust growth in 2023, with a new forecast predicting global expansion of 12.7 percent, up from US$419 billion in 2022.

FINDINGS from a global study commissioned by Cisco and conducted by Canalys, reveal that IT channel partners focusing on managed services are expected to see significant growth in 2023. Despite global economic uncertainty, the projected outlook for managed services indicates a worldwide growth of 12.7 percent, reaching a total value of US$472 billion. This growth surpasses the estimated 3.5 percent growth in overall IT spending.

Key Drivers: Cybersecurity, Expertise, Demand for Flexible Consumption Models

A key driver of this demand is the pressing need for cybersecurity, as organizations across the globe contend with a rapidly evolving threat landscape. This challenging landscape, in addition to a global shortage of cybersecurity and IT talent, has prompted many organizations to turn to partners in managed services for their technology expertise and support. Findings from the study indicate that 56 percent of channel partners expect revenues from cybersecurity managed services to grow this year.

"Customers are integrating more technology into their operations and they expect their IT partners to provide agility, value and flexible consumption models to efficiently manage their growing and complex technology needs," said Alexandra Zagury, Vice President of Partner Managed Services and as-a-Service Sales at Cisco. "The evolving ecosystem of IT partners selling managed services is adapting to meet customer needs and challenges by finding ways to modularize and package what once were customized solutions. We anticipate more innovation and specialization from channel partners through managed services that offer distinct business outcomes and exceptional experiences."

Global Growth

Buoyed by global growth, confidence among channel partners selling managed services has surged significantly. The study reveals that in June 2023, 35 percent of channel partners said they expect growth of at least 20 percent in their managed services business this year. This represents a significant increase compared to the 27 percent reported in 2022 and points to a rapid update of managed services by organizations of all sizes.

"Managed services are the force driving the global IT industry's adaptability and growth. Our research underscores the substantial potential for companies selling managed services, opening up diverse avenues for them to thrive in a post-pandemic era," said Robin Ody, Senior Analyst at Canalys.

The study also identified cloud infrastructure management as another key growth opportunity. As organizations digitize operations and move to the cloud, they face challenges with complex cloud infrastructure spanning private and public clouds, along with distributed applications and services. This has increased the need for cloud infrastructure management and expertise, with 55 percent of channel partners saying they expect revenues in this segment to grow in the current year.

Revenue growth for managed service providers is also likely to accelerate with emerging technologies like AI and the growing emphasis on sustainability measures driven by IT investments. According to the study, nearly six in 10 partners (59 percent) believe AI presents a business opportunity, with 39 percent stating it will be "significant" or "tremendous." Similarly, 57 percent believe customers would be willing to pay a premium for sustainability products and solutions.

"At their core, managed services are about businesses getting the most from technology investments, and as new technologies emerge, managed services are vital to an organization's digital business strategy. By specializing in specific verticals, technologies, or even geographic areas, partners in managed services are helping customers to solve their IT challenges, remove complexity and deliver outcomes that drive a business forward," said Ody.

The study showed that revenues for partners delivering managed services are poised for global growth between 2023 and 2025, with double-digit Compound Annual Growth Rate (CAGR) figures anticipated across all regions. In Asia-Pacific, the sector is expected to grow to 14 percent from US$95 billion. In Europe, the Middle East and Africa, where managed services revenue is currently US$122 billion, growth is forecast up to 12 percent. Latin America is expected to grow 11-12 percent from US$11.5 billion, while North America will see growth of between 10-12 percent from US$190.6 billion.

Survey focuses on cybersecurity disasters

Research finds 40% of organisations have experienced a cybersecurity incident, yet 48% did not disclose those incidents to the appropriate authorities.

KEEPER SECURITY has released findings of its Cybersecurity Disasters Survey: Incident Reporting & Disclosure. The findings reveal widespread shortcomings in reporting cybersecurity attacks and breaches, both to internal leadership and external authorities. Cybersecurity incident reporting falls short

Keeper's survey shows a lack of policies for cyber incident reporting, despite the growing risk of cyberthreats. Nearly three-in-four respondents (74%) said they were concerned about a cybersecurity disaster impacting their organisation, and 40% of respondents said their organisation has experienced some type of cyber disaster. Despite these concerns, reporting breaches to a company's leadership team and to proper authorities is often avoided. External reporting: 48% of respondents were aware of a cybersecurity attack that their organisation did not report to the appropriate external authorities. Internal reporting: 41% of cyberattacks were not disclosed to internal leadership.

Incident reporting is low; guilt is high
Of those who admit they've failed to report an attack or breach to leadership, 75% said they felt "guilty" for not doing so. Fear, forgetfulness, misunderstanding and poor corporate cyber-culture all contribute to widespread underreporting of security breaches. The top three reasons why an attack or breach was not reported to leadership:

- Fear of repercussion (43%)
- Thinking reporting was unnecessary (36%)
- Forgetting to report the incident (32%)
- Organisational cultures do not prioritise cybersecurity

Despite the potential for long-term financial and reputational consequences, poor disclosure and transparency practices prevailed. Failure to report was largely based on the fear of short-term harm to the organisation's reputation (43%) and potential for financial impacts (40%). Respondents also cited a strong need for senior leadership to demonstrate a vested interest in the organisation's cyber posture, and stand beside their IT and security teams, providing the resources and support they need to report and respond to attacks.

A combined 48% of respondents did not think leadership would care about a cyberattack (25%) nor would respond (23%).

> In the current high-risk security climate it's critical for enterprises to encourage transparency and honesty in cyber disaster reporting, and to adopt best practices, policies and procedures to safeguard against ongoing threats.

Nearly one-fourth of all respondents (22%) said their organisations had "no system in place" to report breaches to leadership.

"The numbers point to a need for organisations to make significant cultural changes around cybersecurity, which is a shared responsibility," said Darren Guccione, CEO and co-founder of Keeper Security.

"Accountability starts at the top, and leadership must create a corporate culture that prioritises cybersecurity incident reporting, otherwise they will open themselves up to legal liabilities and costly financial penalties, and place employees, customers, stakeholders and partners at risk."

Best practices
In the current high-risk security climate it's critical for enterprises to encourage transparency and honesty in cyber disaster reporting, and to adopt best practices, policies and procedures to safeguard against ongoing threats.

Some of the most effective ways to prevent cyber disasters, including password and privileged access management, are the simplest, yet most critical to protecting organisations.

Changing work practices challenge network infrastructure

87% of organizations allocated budgets to update network tools for remote and hybrid users, but only 32% have been successful in doing so.

NEW RESEARCH by Enterprise Management Associates (EMA) and Auvik, an award-winning provider of cloud-based network management software, revealed that the ongoing shift to hybrid and remote work environments has resulted in key changes to the roles and priorities of network administrators in order to address new connectivity challenges and prioritize and preserve a secure, productive end-user experience.

The report examined the remote and hybrid work paradigm through the lens of network operations teams – 73% of which reported an increase in workloads, either slightly or significantly, following the shift from traditional to hybrid work environments.

Results from the report demonstrated that the top challenges associated with the remote work experience are poor home Wi-Fi setups, distance from applications, and poor ISP quality. To combat these obstacles, 72% of surveyed organizations have deployed network hardware to the homes of remote workers, including network security devices (62.7%) and Wi-Fi access points (54.1%). Additionally, 90% of organizations with hybrid workers shared that they had to upgrade Wi-Fi networks to address increased office mobility requirements.

"These results reinforce that although people are beginning to return to the office, hybrid work is here to stay and is resulting in significant changes for network administrators," said Alex Hoff, co-founder and Chief Strategy Officer for Auvik. "Although IT teams no longer own all the assets utilized daily by employees, they are still responsible for these operations. And despite not being able to directly exert control over employees' home

networks, they can have visibility over these environments with network monitoring tools. Implementing network visibility software helps IT professionals overcome these new obstacles by providing the ability to maintain visibility and control amid changing work circumstances. The data provided in this report reinforces Auvik's place in the market and demonstrates that our recent acquisitions, integrations, and expanded product offerings that were designed to help IT teams adapt to these new norms are well-suited for the challenges that are being identified within the industry."

Additional findings from the report include:

- Nearly 49% of network operations teams started working with a new tool vendor to help them manage the network experience of remote workers.
- 76% of organizations need to unify how they manage network access policies across on-premises networks and remote users.
- Remote desktop access tools (deployed by 81% of companies) remain the go-to solution for troubleshooting remote users'

problems, but endpoint monitoring tools are increasingly popular (79%).
- Although 87% have allocated funds in their budget to update network operation tools for remote and hybrid user support, only 32% of organizations shared that they have been successful in doing so.
- The top issues employees most often report when they are working from home are VPN access issues, followed by performance issues with SaaS applications.

"96% of IT organizations said they are supporting hybrid workers, and 30% of all employees who work remotely are hybrid workers," said Shamus McGillicuddy, VP of Research, EMA. "With employees working both at home and in the office, it is important to have the assets and software necessary to support them in both locations. This means enterprises must invest in more secure remote access solutions that offer integrated network security automation, centralized management, and network optimization or network enhancement, as well as network observability tools that are able to monitor performance across disparate locations."

Funding shortfall puts innovation plans in jeopardy

33% of businesses have insufficient financial resources to innovate.

THE FIFTH annual International Innovation Barometer reveals that a declining global economy has stalled innovation potential.

The report by innovation consultancy, Ayming, reveals that the global boom in innovation – reflected in the 38% of firms that now rank it a top priority for the business – is under threat from a lack of adequate financial resources, cited by a third of respondents.

Governments around the world are putting innovation at the heart of policy agendas and anchoring their plans for prosperity to ambitions of becoming an 'innovation-led economy'. But for innovation to become an integral part of the mechanism of any economy, funding must be accessible, and the report shows that current funding streams are not currently providing businesses with the necessary means to innovate.

Inflation has driven up costs and critically damaged fragile profit margins, forcing businesses to seek funding from outside sources. The number of businesses using equity and debt funding nearly doubled from 23% in 2022 to 41% in 2023, making it the most popular source of funding this year, while the proportion of those self-funding innovation dropped by a fifth.

However, rising interest rates have made debt funding a much harder route to take for start-ups and smaller businesses, resulting in a parallel rise in the number of businesses using crowdfunding tactics, which respectively rose from 7% to 26%. Njy Rios, Director of R&D Incentives at Ayming UK comments, "The bottom line is that the current economic climate has created a tension between business' short and long-term plans that is having a negative impact on innovation output. Policymakers must find a way to align the two or risk jeopardising future innovation."

The Barometer also examines the widening intersection between innovation, technology and sustainability. The data reveals that despite ideological support, financial barriers are again impeding essential progress with 41% of businesses citing the high upfront cost and investment required as the obstacle preventing them from undertaking sustainable innovation.

The US government's Inflation Reduction Act was signed into law in August 2022 with the intention of making sustainability a priority for US businesses, but just 22% currently see it as such and it's too soon to tell if the EU's Green Deal Industrial Plan, presented in February 2023, will be effective in scaling up the continent's manufacturing capacity.

The report's findings reveal that businesses are acutely aware of the economic opportunities offered up by the net-zero transition with an emphatic 78% allocating up to 20% of their annual budget to sustainability initiatives. But a set of short-term economic priorities are undermining these intentions and slowing businesses down.

Rios continues, "While governments pay lip service to the need for green tech to save the world, the would-be drivers of this sustainable innovation require urgent access to funding. So as the world continues to advance towards climate crisis, governments need to address the funding gap with far greater resolve if policy is to be translated into practice. Until businesses are deriving economic value from prioritising sustainability, short-term economic pressures will always be a roadblock."

In June 2023, Ayming surveyed 853 R&D and innovation directors, Chief Financial Officers and Chief Executive Officers. Respondents were sourced from the following
17 countries: Belgium, Canada, China, Czech Republic, France, Germany, Ireland, Italy, Hungary, The Netherlands, Poland, Portugal, Singapore, Slovakia, Spain, United Kingdom, United States. Respondents were split evenly between seven sectors: automotive, construction, finance, manufacturing, finance, pharma and technology, and reflect an equal representation of large and small businesses.

New research shows critical role of cloud strategy in driving business innovation

Cloud is rapidly becoming the optimal business platform for innovation at scale; technologies like generative AI (GenAI) and cloud go hand-in-hand.

HCLTECH has launched a new report providing compelling insights into how organizations can overcome key obstacles like security concerns, talent gaps and company culture to maximize the business impact of their cloud investments. Titled "Cloud Evolution: Make Innovation a Habit," the report is based on a survey of 500 senior business and technology leaders across industries.

The report revealed that while 73% of executives believe their companies are only beginning to leverage the potential of cloud, over 90% recognize cloud's vital role in enabling rapid response to critical business events, strategic pivots and adopting leading-edge technologies like AI.

Cloud continues to enable businesses to pivot when faced with new and unforeseen challenges. As high as 87% of the respondents in the survey said that they would not have been able to make significant pivots last year without cloud. Businesses are relying on cloud to meet sustainability goals (91%), to work through pandemic-related staffing and supply chain issues (87%) and mitigate the impact of rising inflation (77%), showed the survey.

"Cloud is rapidly becoming the optimal business platform for innovation at scale," said Kalyan Kumar, Global Chief Technology Officer & Head – Ecosystems, HCLTech. "However, many companies have yet to fully tap into its potential. This report offers a blueprint for developing the right cloud strategy to drive competitive advantage."

The respondents agreed that innovative technologies like generative AI (GenAI) and cloud go hand-in-hand. Of the respondents, 58% noted that businesses have increased or are planning to increase investments in GenAI and 85% believe it is only possible with the right cloud strategy. Both IT leaders (86%) and business leaders (81%) agree that they closely collaborate with one another to discuss cloud strategy to unlock their potential to innovate.

However, 73% of the survey participants said that their business is only just beginning to unlock the potential of cloud. Nearly a third of the senior executives (32%) said that a lack of alignment and collaboration between business and technology departments is an obstacle to achieving their business goals.

"Forward-thinking leaders recognize that cloud is no longer just an infrastructure play but rather a transformational business platform," said Siki Giunta, Executive Vice President, CloudSMART and Industry Consulting, HCLTech. "By following the recommendations in this report, organizations can truly unleash cloud's potential to accelerate growth and resilience."

To make innovation through cloud a norm, the report advises companies to leverage cloud's agility, shape their organization's culture around cloud, break down departmental barriers, increase cloud literacy and tightly align cloud strategy with AI and other emerging technology adoption plans.

Cloud continues to enable businesses to pivot when faced with new and unforeseen challenges. As high as 87% of the respondents in the survey said that they would not have been able to make significant pivots last year without cloud

AI budgets increased by more than three quarters

IT leaders report a significant impact to customer value, employees' well-being, and enterprises' return on AI investments.

THE ECONOMY may have had a downward impact on enterprise investments, but these increased exponentially when implementing AI, according to 76% of UK IT executives taking part in the latest State of Intelligent Automation Report: Impact of the Economy on AI Priorities, commissioned by ABBYY.

Respondents from the UK ranked consistently higher than their French and German counterparts when it came to attributing an increase in higher value work (68%), happiness (65%), and employee innovation (61%) – noting that intelligent automation freed them from many routine and mundane tasks to focus more on customer and revenue-driven initiatives.

Nearly half (47%) of UK respondents reported an increase in staff retention levels since introducing intelligent automation, which is significant in the era of "silent quitting."

They also stated that improvements in employee efficiency (53%) and productivity (50%) were among the top benefits to the organisation, as well as the benefit to employees, with nearly four in ten (38%) stating there was better work-life balance. Globally, the

US led in the reduction of work stress (41%), followed by the UK (38%).

"IT executives in the UK – and globally - are gaining powerful value from their AI investments," stated Neil Murphy, Chief Sales Officer, at ABBYY. "Notably, half of UK leaders surveyed stated higher quality products and projects, and even more cited faster delivery of their products to customers (55%). More than a third (37%) reported improved customer service outcomes. It's no surprise they achieved twice the ROI by leveraging AI in their intelligent automation initiatives to accelerate the improvement of complex processes and putting data to work."

Greater ROI, greater investment Almost half (44%) of enterprise executives saw a 2x return on their AI investments in 2023. Additionally, 76% said their AI budgets increased this year and 43% plan to invest more, despite reductions in costs in other parts of the organisation.

The survey also revealed that, across the globe, mid to large enterprises are placing the greatest investments in AI to enable intelligent automation. Increased investments of up to 35% by emerging enterprises indicates

growing recognition that AI is leveling the playing field and required for a competitive advantage.

As AI adoption becomes more widespread with the use of large language models such as generative AI, 90% of UK IT executives responded that they have AI strategies in place. More than a third (36%) have compressed their roadmaps into three-to-five-year plans, noting revenue-impacting processes as top priorities including operations, marketing, product development, sales (as it relates to customer experience), and logistics services.

Lack of cloud management wastes IT resources

Aptum has recently released part two of its annual Cloud Impact Study 2023 - Maximizing Value: Controlling costs and optimizing cloud spend. According to the study, 71% of IT professionals surveyed stated that cloud-related costs make up 30% or more of their total IT spend.

THE STUDY involved 400 senior IT professionals from organizations with 250+ employees across the U.S., Canada, and UK. It explores the trends in cloud cost management and how these trends have evolved over time.

In today's challenging economic climate, organizations are becoming increasingly aware of the financial implications of their business operations. While the cloud has brought benefits such as flexibility, scalability, agility, and cost efficiency to organizations in recent years, there are still unforeseen costs. More than half (52%) of IT professionals admitted their organizations have wasted significant IT spend due to inefficiencies with cloud platforms and services.

In fact, 73% of IT respondents reported that their cloud investment has resulted in higher-than-expected IT costs within the last 12 months, marking a 28% increase compared to 2021 figures. Additionally, the majority (92%) of IT professionals stated that they are likely to conduct a full ROI (return-on-investment) analysis of cloud spending, a rise from 89% in 2022. But what is causing these increased costs?

The survey identified several factors, including poor planning, a lack of internal expertise, the acceleration of cloud adoption, and a lack of familiarity with complex cloud solutions. These challenges are considerably magnified when organizations implement a hybrid, multi-cloud strategy that incorporates both on-premises and public cloud services for different data services and workloads.

Currently, 62% of respondents agree that a lack of internal expertise has prevented them from expediting cloud implementations. However, to mitigate these escalating costs, developing skills and knowledge in cloud strategy is crucial.

"Many organizations believe they are excelling in the cloud, but in reality, like flying in a cloud, they have to rely on instrumentation, which is usually inadequate to begin with, and piloting experience which takes time to develop," said Ian Rae, CEO & President at Aptum. "It isn't the cloud that is costly but the lack of observability and governance which hinder management and lead to cost overruns. This shortfall significantly hampers the ability to unlock the cloud's potential for enhancing operational efficiency while controlling costs."

The results demonstrate that organizations struggle to fully realize the value of their cloud spending as they expand their adoption of cloud services. The lack of a comprehensive, multi-cloud strategy poses a challenge for many IT leaders, preventing them from fully harnessing the transformative capabilities of the cloud.

But continued cost savings rely on a clear cloud investment strategy that focuses on visibility and control of costs – especially for those accelerating cloud investment and moving into more complex, multi- and hybrid cloud environments. FinOps principles are key to ensuring organizations are operating efficiently in the cloud:

1.Cost Visibility and Accountability: FinOps helps gain visibility into cloud expenditures, allowing teams to be more conscious of their spending.

2.Optimized Resource Usage: FinOps practices help identify underutilized or unused resources, leading to termination or downsizing.

3.Enhanced Decision-Making and Forecasting: With clear insights, informed decisions can be made based on usage analysis, reducing the likelihood of unexpected overruns.

4.Cultural Change: A FinOps culture encourages cost to be an organizational mindset and a standard part of operational discussions.

5.Continuous Improvement: The iterative nature of FinOps ensures continuous improvement to cloud financial management practices, leading to ongoing savings.

DON'T
GET YOUR
SaaS
KICKED!

TAKE CONTROL NOW AND PROTECT YOUR SaaS DATA

Global SaaS vendors like Microsoft, Google and Salesforce don't assume any responsibility for your data hosted in their applications. So, it's up to you to take control and fully protect your SaaS data from cyber threats or accidental loss. Arcserve SaaS Backup offers complete protection for your SaaS data, eliminating business interruptions due to unrecoverable data loss.

Arcserve SaaS Backup

Complete protection for all your SaaS data.

arcserve.com

arcserve®

Protect what's priceless.

Building resilience in the age of AI:
A guide for channel partners

The promise of Artificial Intelligence (AI) as a groundbreaking innovation is undeniable. From healthcare to retail, the transformative power of AI has captivated industries, and the cybersecurity sector is no different. However, for all its good, AI is a tool that can be utilised as a weapon too. As the technology gets stronger, we are increasingly seeing cybercriminals leverage more AI-driven cyber threat techniques.

BY SCOTT WALKER, SENIOR DIRECTOR, CHANNEL SALES EMEA, ILLUMIO

THE CURRENT WAVE of generative AI has seemingly lowered the entrance barrier to threat actors. Unskilled cybercriminals, labelled as 'script kiddies', can use AI to access new attack options, such as using prompt injection to create malware. While mainstream tools like ChatGPT employ measures to block harmful requests, more malicious versions and alternatives like WormGPT and FraudGPT have emerged.

As AI threats escalate, organisations are increasingly seeking expert guidance to bolster their cyber defences. This shift presents a unique opportunity for channel partners to move away from being seen as tactical solution providers, to trusted advisors, advising businesses on adopting resilient security architectures like Zero Trust. This evolution not only meets immediate security needs but also positions channel partners as long-term strategic allies in the fight against future AI-driven threats. The challenges of AI-drive defences One of the key security challenges around AI-driven threats is that traditional network-centric security solutions are no longer fit for purpose against modern threats. We've seen this in our own incident responses, where advanced threats download an attack or a piece of malware, along with all the components needed to execute it. Conventional firewalls and network security measures simply cannot keep pace with such dynamic threats.

To combat the threats posed by AI, many vendors are pushing a "fight fire with fire" approach, encouraging organisations to implement the latest AI-based defensive solutions. But whilst AI should have a significant place in an organisation's security stack, relying entirely on using the technology for defence is a major mistake.

Cyber adversaries today can poison and trick defensive AI tools into overlooking malicious activities by feeding them false data. If an organisation's defensive measures are entirely based on such tools, it could be highly vulnerable to techniques like this.

Deploying defences indiscriminately against evolving AI threats is akin to prescribing antibiotics for every illness—a practice that eventually leads to antibiotic-resistant pathogens. The overuse of antibiotics has taught us valuable lessons about resistance – showing restraint round AI may be the best way to counter its misuse.

Rather, the channel should be advising organisations that the best defence against AI-attacks is in fact doing the fundamentals even better. This means shifting the focus from network-centric security to

asset-based security to provide a more granular level of protection. By focusing on securing assets, businesses can contain threats to specific servers or workloads, allowing the rest of the organisation to continue functioning even in face of an attack. Within this approach, different AI systems can be trained to adapt and respond dynamically to different asset labels.

This is a step beyond what traditional network security can offer, bringing agility and true resilience to organisational defences.

A balanced approach: Combining AI with core security principles

The channel has a responsibility to steer its customers away from a tunnel-vision approach that solely prioritises AI-based solutions. Partners should be advising businesses to adopt a balanced approach that marries AI to fundamental security principles. To facilitate this, there are several aspects that the channel must consider:

Reducing the attack and learning surface
One of the best ways to build resilience against cyber threats is to reduce the attack surface. The fewer the points of entry, the lower the risk. However, the advent of AI means businesses also need to consider the 'learning surface' as well as the attack surface.

Constraining the 'learning surface' is not merely about blocking resource access for invasive malware; it's also about intelligent resource allocation. The channel should support and guide its customers in auditing which assets need to be completely shielded from the AI lens, thereby further reducing the available surface for offensive AI to learn and adapt. This goes hand in hand with Zero Trust's tenet of 'least privilege access,' which emphasises allowing only the necessary permissions for each asset based on its role in the organisation.

Embracing Zero Trust
The best way of achieving a reduced attack and learning surface is by implementing microsegmentation solutions aligned with a Zero Trust framework - or better yet, Zero Trust Segmentation. Such solutions provide a level of granular control that isn't just about stopping an attack, but rather about understanding the 'why' and the 'how' of an attack pathway. By giving customers the tools to track how an intruder navigates, channel partners can help businesses stop an attack in its tracks and gain invaluable insights into attack methodologies. These insights are critical for pre-emptive actions in the future.

Zero Trust Segmentation's agile approach also enables businesses to flip the security paradigm. It replaces static security directives with dynamic guidelines that can adapt in real-time to an evolving threat landscape. This level of adaptability is crucial when combating AI threats that continuously learn and adapt.

Integrating regulatory directives
We are also starting to see an evolving regulatory landscape around AI that the channel must be aware of. To-date most of the discussions are about protecting AI from attacks, not protecting organisations from AI. Partners have an opportunity to bridge this gap and help organisations boost resilience by offering solutions that are seamlessly integrated with regulatory directives and frameworks, such as the NCSC's Cyber Assessment Framework (CAF). The CAF already outlines the critical elements of network segmentation and system communication, but it needs the agility that ZTS brings. By combining the foundational guidelines of the CAF with the dynamic capabilities of ZTS, the channel can offer customers a robust, sustainable, and future-proof security strategy. Don't forget education.

Finally, let's not forget the importance of educating our customers about these layered security strategies. It's one thing to implement them, but it's another to ensure they're being utilised to their maximum potential. Regular training sessions, webinars, and workshops can go a long way in ensuring that the workforce is equipped to manage and respond to AI-induced threats effectively. In the age of AI, the channel's responsibility is significantly increasing. It's not just about equipping the customers with the right defensive tools, but rather it's about educating them, supporting them to develop a robust policy, and helping them consistently throughout their cyber resilience journey.

Given the buzz around AI, it is understandable that businesses will increasingly ask for AI-driven defensive solutions. So, the channel must increase awareness among its customer base that defensive AI is not a silver bullet. Rather, a balanced approach incorporating Zero Trust Segmentation and asset-based security can offer a more robust security infrastructure and make businesses more resilient.

How MSSPs can leverage generative AI to boost their service offerings

For many organisations, electing to use a Managed Security Services Provider (MSSPs) isn't just about keeping costs in check by outsourcing the cybersecurity function. It provides additional benefits such as reducing complexity, assurance with regards to ongoing management and compliance, and the ability to benefit from technology that the team may not have the resources to invest in.

BY EDY ALMER, DIRECTOR PRODUCT MANAGEMENT FOR THREAT DETECTION AND INCIDENT RESPONSE AT LOGPOINT

GENERATIVE ARTIFICIAL INTELLIGENCE (AI) is now one of those technologies. Large Language Models (LLMs) such as Open AI's ChatGPT, Google's Bard and Microsoft's Bing promise to revolutionise how we work. Trained on copious amounts of data, these models utilise Natural Language Processing (NLP), enabling them to rapidly respond to requests in a human like fashion at lightning speed.

How Gen AI can generate value

MSSPs can therefore harness AI to their advantage in a number of ways. They can use it to help fill the skills gap because the automation of certain routine processes will alleviate the pressure on its security analysts. The way generative AI functions using NLP paves the way for the possible democratisation of cybersecurity, which means those with lower skill sets could carry out roles that were previously the preserve of the security analyst. The MSSP could then use that spare capacity to dedicate more time to customer interactions or to scale their operations. But perhaps most excitingly, they can integrate generative AI with their current service offerings to enhance the product portfolio.

Doing this inhouse is, however, complex. The MSSP will need to look at building integrations between systems and the LLM which would require a data science team. It would need to train up its analysts on how to prompt systems effectively and would need fail safe policies to govern use as AI has been known to exhibit bias. For these reasons, it makes much more sense to look to vendors who have begun to integrate AI with their solutions. But where can AI really add value?

Time critical incident response is a prime candidate for AI integration. Technology such as Security Orchestration and Response (SOAR) that collects alert data from multiple systems is already using standard AI to prioritise threats, make recommendations and automate response using pre-configured playbooks, so why not add the 'Ask Me Anything' attributes of generative AI? Incorporating the responses into playbooks and use cases could provide real benefits in numerous use cases.

To start with, security solutions need to wade through copious amounts of data and in the event

of a breach, the Security Operations Centre (SOC) team will need to digest that and supplement it with information from internet sources. Generative AI can significantly reduce this by consolidating data from multiple sources, internally and externally, to produce a two-to-three-page report from more than ten times that in hours rather than days.

Of course, such information will still require human verification, especially given that attack summary reporting is a legal requirement across much of Europe. But it is much less laborious for an analyst to review and approve the draft report before it is distributed rather than from scratch and as LLMs can only go by the existing information they are fed they are unlikely to produce inaccuracies within a closed context.

Shrinking MTTR

For the MSSP, a key priority is the Mean Time to Respond (MTTR) and their ability to effectively reassure their customers who want to know the implications of a breach and what they need to do as quickly as possible. Gathering together the evidence and reporting to customers inevitably leads to a longer MTTR. But, with SOAR and generative AI automating both, the MSSP can spend the time that was devoted to those tasks on analysis while at the same time driving down MTTR, making it a win-win. The ability of generative AI to distil down information into an easily digestible format

also lends itself to summarising reports. Generative AI can tackle lengthy compliance reports to produce succinct executive summaries that detail the main findings and remediation recommendations. These are then much more intelligible for the board and senior management, helping to aid decision making.

Furthermore, generative AI in combination with SOAR can also be used to develop awareness training. The AI can automatically generate phishing emails that are crafted to be much more realistic by including information obtained from online sources such as LinkedIn. The SOAR playbook extracts data from LinkedIn, enriches it with email addresses and connections from past logs, and sends the phishing email to select recipients, before then measuring how many click throughs are made and how many alerts the phishing response team receive.

It's still early days for generative AI with the technology in its infancy. Right now, MSSPs are experimenting with how they can use such integrations to extend the capabilities of automated solutions and nearly a quarter of C-suite executives are already using it, according to McKinsey survey, which found early adopters are already outpacing their competitors. So, for MSSPs that seize the initiative, the technology has the potential to drive down the time to respond, bring them closer to their customers, free up resource and see them grab market share.

Augmenting yourself with AI:
Customer service redefined

Over the past few years, expectations of customer service have risen, along with an increased emphasis on anytime, anywhere, any channel responses.

BY SIMON JOHNSON, VP SALES, GENERAL MANAGER UKI, FRESHWORKS

EMPATHY, personalisation, speed and convenience are now defining the modern customer service experience, and businesses have no choice but to adapt or fall behind. According to Gartner, when businesses go beyond mediocre customer service and give value-driven customer service interactions, customers are 86% more likely to repurchase, 82% more likely to be retained, and 97% more likely to spread positive word-of-mouth about your business. Fortunately, developments in AI have made it easy for businesses to adapt and improve their customer service approaches to meet new expectations.

Using conversational AI for example, many businesses are adopting AI-powered chatbots to deliver a hyper-personalised and seamless approach to automate customer support. This article will explore the transformative impact AI can have when paired with customer service agents, the importance of preparing the workforce for the implementation of AI, and the key factors to consider when choosing an AI customer service solution.

The benefits of AI

Whether you're for the AI revolution or a critic, it can't be denied that AI has demonstrated its potential to enhance productivity for professionals. In fact, a recent study by Freshworks found that 95% of IT pros see the benefits to employees using generative AI to help complete work. The productivity potential present translates into real business success: think higher customer experience, satisfaction, retention rates, and boosts in revenue.

Within customer service, there is a clear space for the application of AI technologies. Chatbots have already laid the foundation, providing customers with instantaneous assistance. Over time, the limitations for what chatbots have been capable of

have reduced further and further, with generative AI creating the possibility of a more human-like interaction than could be achieved before. This has opened an opportunity for businesses to maximise efficiency for their customer service agents, by retaining them for requests that require a more direct human touch. Through leveraging natural language processing, chatbots and virtual assistants can handle routine customer inquiries, streamlining repetitive processes while also reducing response times.

Sometimes, however, customers aren't fulfilled by the solutions provided by AI assistance, and this is where the potential for generative AI to shine really comes into play. The human element in customer service is irreplaceable at a certain point, so AI solutions should be equipped to best support agents in a variety of contexts.

Developments in AI agent experience solutions have been shown to provide instant summaries of customer inquiries, connect teams across ticket generation, and augment responses with language suggestions. These vital tools highlight how human agents can be augmented with AI to turn them into super-agents, capable of answering customer inquiries faster and better than non-AI-supported teams.

Getting left in the dust
It's looking increasingly likely that businesses must embrace AI to remain competitive and avoid getting left behind with inefficient work practices. AI-powered customer service solutions enable organisations to meet evolving customer expectations, delivering personalised experiences that customers will come to demand more as time goes on. There's a reason remembering a customer's name encourages loyalty – personalised experiences tailored to you are far more desirable than those that aren't.

Businesses embracing AI find themselves able to anticipate customer needs, offer proactive support, and identify opportunities for excellent customer service that human agents might not always recognise. Organisations that fail to utilise an AI solution risk a competitive edge in a market that is constantly changing.

Preparing the workforce
As organisations increasingly recognise the benefits of using AI, they must ensure they are taking the necessary steps to prepare their workforce for AI implementation before deploying it. IT leaders play a crucial role in training their teams to adapt by fostering a culture of continuous, enthusiastic learning and reskilling, equipping employees with the necessary AI literacy and proficiency. Without this necessary reskilling, businesses risk losing the efficiency gains via speed bumps in implementation. Through active training, agents will see the value in utilising AI as their response times go down, and

day to day workflow clears up menial, repetitive tasks. In the same way that business leaders are responsible for providing the opportunity for customer service agents to reskill, agents must also keep an open mind as to the possibilities of support that AI can provide to themselves and the customer. By maintaining open communication on the role of AI within an organisation, employees and business leaders can ensure a collective movement to refine customer service processes with a true commitment to efficiency and productivity.

Practically, this means training workshops, demos across organisations, and actively encouraging opportunities for employees of all levels to experiment with AI technologies made available to them. Appropriate training on the use of AI can be as critical to implementation as the technology itself, and only through investing in the process of meaningful integration can businesses expect to see the benefits shine through.

Taking the first step
Selecting the right AI solution for your business is critical to achieving the benefits available through implementation. Ensuring your solution has been trained on relevant data sets that facilitate a customer experience suited to you can make the implementation process a lot smoother, and should always be a factor considered when shopping for the perfect AI.

Scalability and flexibility are also crucial to your business' success in the long run. Solutions that aren't capable of both of these won't accommodate changing business needs and can end up hampering future growth further down the line. Additionally, robust security measures to protect customer data and compliance with privacy regulations are paramount. Generative AI solutions shouldn't make it past the initial stage if they aren't able to guarantee your data is handled with the appropriate level of protection and compliance according to your regulations. A business that risks its data, risks its livelihood, and this is arguably the most important factor to consider.

The future of customer service
All in all, AI presents an opportunity for businesses to stimulate growth and produce efficiency across their customer service model. Implementation of AI can't be rushed along, organisations must ensure they've done their due diligence when it comes to choosing the correct solution and have adequately prepared their teams for AI augmentation. By doing so, businesses can unlock the potential to transform their customer service into a productive and efficient workforce that deliver exceptional service, every time.

All is not what it SIEMS!

Observations from working with Managed Security Services Providers (MSSPs).

BY PIERS WILSON, HEAD OF PRODUCT MANAGEMENT, HUNTSMAN SECURITY

STAYING RELEVANT with best practice and navigating the constantly evolving threat environment weighs heavily on MSSP operators and security teams more generally. The burden of demonstrating value to clients and protecting their environments is often not recognised as important, as long as risks continue to be averted.

Attracting and retaining resources as part of a high-performance team, without the technology necessary to support their endeavours, can sometimes mean high levels of effort and organisational stress; particularly when much of this time could probably be better spent focussing on meeting the challenges of delivering effective cyber security services. In speaking with the MSSPs we work with, these challenges are

common. In response to addressing the market need, some offer bespoke services tailored to the specific requirements of the customer and others offer defined services often in increments of sophistication and cost.

Whatever their speciality, we hear service providers are striving to maintain a level of inbuilt flexibility in their operating model to meet the changing requirements of their customers, which is why Security Information & Event Management (SIEM) solutions are generally the foundation of security monitoring, and the provision of SOC and other MSSP services. SIEM is a mature technology sector, with most vendors offering similar functionality. Most, however, were designed to be deployed in a single enterprise and so are inherently not a

good fit for a multi-customer managed security services business model – but there are newer next generation options that MSSPs are adopting. When choosing a SIEM solution to support managed security services, we found that there are four considerations that have a significant impact on the cost effectiveness and profitability of an MSSP's business offerings.

- **Time to revenue –** factors that influence the speed and overhead of onboarding new customers.
- **Demonstrating value to customers –** and improving customer retention.
- **Scalability –** primarily, the choice between Software and Appliances.
- **Integration with future technologies –** and the use of emerging security monitoring tools.

Time to revenue

One of the biggest considerations is the ease and ability to support multiple customers on a single platform, so-called multi-tenancy. Managed service providers will inevitably need to support multiple customers and be adding new ones regularly. If they need a new instance of a technology each time they win a new customer, it can undermine the cost-effectiveness of the outsource model – leading to multiple platforms for their SOC analysts to administer and, ultimately, excessive "per customer" costs.

Analysts need a one-to-many console - so additional application windows or dashboards are not required for each customer. For new customers, onboarding onto a working system with existing configurations, also saves providers implementation and onboarding time. Multi-tenancy makes this operationally possible and massively streamlines the effort of bringing a new customer into service. While a number of technologies offer this capability, most achieve it through an access control by group mechanism (one group for each customer) rather than true multi-tenancy.

Another opportunity to accelerate new customer on-boarding is with platform flexibility. So that adding new data sources/types, whether standard or bespoke, can be done easily. For an MSSP with multiple customers, there could be dozens of system types, firewalls, business applications and cloud providers, so the ability for the SIEM to be flexible enough to cope with this diversity is a priority. Some technology solutions, less well suited to the MSSP market, rely on expensive professional services each time a new type of technology needs to be accommodated.

Demonstrating value to customers

Improving customer attraction and retention means being able to demonstrate value that is both visible

and real. A service that operates in the background may suffer if there is little to show customers for their investment. Conversely, a constant stream of alerts that need technical interpretation, or involve further action, is likely to be seen to generate effort, rather value.

Getting the right balance between reports showing what the service has achieved and managing the throughput of alerts with supporting detail, is critical. Ideally, customers should be notified of incidents with findings and recommendations so they can respond appropriately. They need to see the service benefits, regular reports on volumes of events analysed, alerts triggered etc. and service performance levels based on operational KPIs.

Customised reports with commentary on investigations and alerts are highly valued by customers. They are paying for the expertise of the MSSP, so prioritised recommendations, rather than general information dumps, are a significant differentiator for many MSSPs.

Scalability

All IT systems need to scale. In the MSSP space, each new customer means additional systems to on-board and manage; and the SIEM needs to support this by design. Ideally the SIEM should scale horizontally - adding more storage, processing capacity, archive space and customers. And so minimising the constraints typically imposed by capacity expansion. Scalability is particularly acute when considering whether to buy an appliance-based SIEM or software solution. Initially the ease of having a single appliance to

support seems obvious, but the constraints can quickly become clear. No one wants to have to rip out a SIEM solution they bought two years ago and replace it with a larger one; or bear the initial cost of a larger box from the outset, in the hope of future growth. SIEM software solutions are infinitely better suited to progressive expansion than the alternative.

Integration with future technologies

The reality is that SIEM technologies continue to be the focal point for the provision of managed security services. Even when other technologies are being used, there is invariably an overarching SIEM in use to consolidate the log and security event data from across the enterprise.

This is important because of the vital role that SIEM plays, even as the demand for auxiliary services (like E/XDR and NDR) grows over time. Additional technology solutions, that add particular value will always need to be integrated into an overall SOC solution – and SIEM enables this expansion without adding numerous application consoles for operators. Automation and SOAR are also drivers, especially where workflows span multiple solutions. Then, there is growing interest in MITRE ATT&CK®.

This classifies the tactics and techniques attackers use, to enable the MSSP and its customer to understand the nature of particular incident, and the stage of the related attack. It also provides a set of mitigations that the MSSP and customer can work together to put in place. This sort of value-added capability, of course, can present further sales or consultancy opportunities for the provider. Security is technical in nature; and MITRE allows the MSSP to work with and advise their customers on new and emerging threats or potential solutions, as they arise.

Again, implementations of MITRE ATT&CK® vary. Endpoint solutions, for example, are focussed on user behaviours and workstation signals. SIEMs, however, are well suited to providing information about what's happening across the rest of the infrastructure; then aggregating that information for better visibility of your overall cyber security position.

Summary

From our work with MSSPs, we understand that the security technology market is highly diverse, with many suppliers offering varying capabilities at various price points. The desire by customers for MSSPs to demonstrate value through service, and not just routinely issue a report of an incident, is clear. Actually investigating, and providing an annotated interpretation and recommended resolution is emerging as a new requirement for many customers; and a revenue opportunity for MSSPs.

For enterprises, the technology choices are complicated enough; but for managed security service providers, the additional considerations of time to revenue, perceived and actual value, scalability and future-proofing your technical platform are added complexities.

The best traditional enterprise solutions may not work as well in a multi-customer environment – it was not their use case. They may not allow the accommodation of multiple customers or the economies of scale necessary to match the rapid business growth the provider expects; or they may lack the flexibility to cope with the range of technologies that will be encountered into the future. The good news is that there are now contemporary options that solve some of the traditional obstacles MSSPs face in better meeting the needs of end customers.

If you and your team are looking for a true multi-tenancy SIEM that is built for MSSPs, consider Huntsman Security's SIEM solution: https://huntsmansecurity.com/products/mssp-siem/ or request a demonstration by emailing: ukinfo@huntsmansecurity.com

MANAGED SERVICES
SUMMIT
NORTH

21 NOVEMBER 2023

MANCHESTER CENTRAL, PETERSFIELD, MANCHESTER
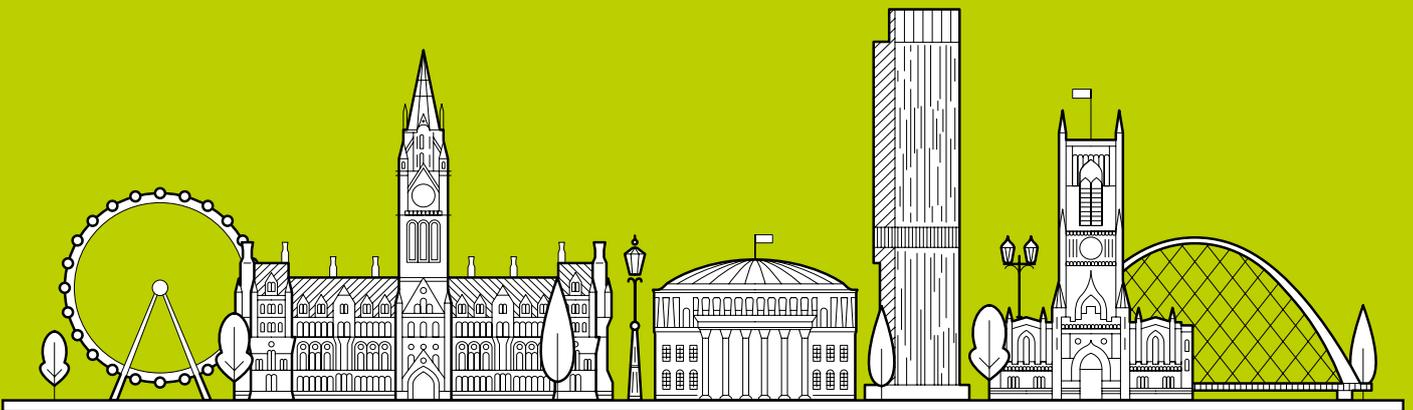
Managed Services Summit North (sister events in London and Amsterdam) are the leading managed services events for the UK and European IT channel. Featuring conference session presentations by major industry speakers, the Summit provides opportune networking breaks for delegates to meet with potential business partners. The unique mix of high-level presentations plus the ability to explore and debate the most pressing business issues with sponsors and peers across the industry makes this a must-attend event for any senior decision maker in the IT channel.

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://north.managedservicessummit.com/

How Open XDR is setting the stage for the future of cybersecurity channel

By providing vendor-inclusive, open XDR platforms, channel partners will help deliver value that will see companies become safer and more secure, despite ongoing turbulence.

BY SIMON GODFREY, VP SALES EUROPE FOR SECUREWORKS

THE GLOBAL cyber security market is projected to grow from $172.32 billion in 2023 to $424.97 billion in 2030. The rising threat of breaches, combined with increasing regulatory oversight and risk of fines is pushing cybersecurity further up the corporate agenda. Almost every IT stack has a cyber component now.

And we can see there is great optimism within the channel on the promise of cybersecurity. According to Canalys, 54% of channel partners expect double digit growth in their cybersecurity business in 2023, while over a quarter (27%) believe their cybersecurity business will grow more than 20%.

While cybersecurity presents a great opportunity for the channel, it is not an easy sell. Cybersecurity is complex, requiring increasingly hard to find specialist skills. Furthermore, cyber buyers are well informed. They have preferred technologies and complex organisational needs. And with budgets tightening, many CISOs need to do more with less. The challenge for the channel is hitting the balance of helping customers effectively reduce risks with less expenditure, while still protecting margins. Could Open XDR hold the answer?

With threats on the rise, customers need a partner they can trust

As the complexity of IT increases, the attack surface widens. It's harder than ever to defend against would be attackers. Exacerbating this problem is the lower barrier to entry for potential threat actors. Almost anyone with an internet connection and a bit of technical knowledge can just hop on the web and download a hacking kit. Customers really are getting hit from all sides.

In a bid to stay ahead of the threats investment in cybersecurity tools has increased. Often in a piecemeal and siloed approach, heading off one area of concern at a time. It isn't uncommon for large organisations to have upwards of 50 cybersecurity tools in operation, often from dozens

of vendors. Add on top, not enough people then to monitor and maximise use of the tools purchased. With customers struggling to make the most of the investments they already have, it can be difficult to get them to consider new ways to improve their security posture. This is where the channel can play a vital role in advising customers on new ways they can improve their security posture, while consolidating their environments and use of vendors. This is driving the need for Extended Detection and Response (XDR), offering a single platform for threat prevention, detection, and response.

The open or closed debate

The XDR market is now being valued at $1.4 billion, and estimated to register at a CAGR of 19% between 2023 and 2032. Why? Because XDR platforms can distil millions of security alerts across environments – from endpoints and emails to cloud – into just a handful of real threats requiring investigation. This holistic view helps to target resources in a more effective way, reducing complexity and giving security teams a more comprehensive view via a single platform.

But how can the channel select the right XDR platform for them and their customers with so many to choose from? Partners may be tempted to offer native (closed) XDR platforms designed as an all-in-one platform from a single vendor, that includes all native security controls monitoring network, endpoint, cloud, email and other business applications. While it is a platform, it is a single vendor approach for all telemetry.

However, closed platforms of this kind are restrictive, limiting options for the channel to sell best-in-breed third-party solutions. And as CISOs are already likely to have invested in multiple security solutions, recommending an XDR platform which forces them to overhaul their entire stack is likely to hit with significant resistance. Not to mention,

it restricts ability to make changes in the future as the business needs change. This closed approach also limits the channel's ability to build trust with customers who may be better off with a best of breed solution for their specific security needs.

Open up to Open XDR

Open XDR platforms provide channel partners with the flexibility to create security bundles which incorporate their existing investments, or to fit in with their stack as an additional overlay. This also gives the channel the option of upselling by offering third-party integrations and automated playbooks to accelerate response actions.

In addition, as Open XDR platforms sit across the entire security infrastructure, they collect data on the effectiveness of those tools. Armed with this data, partners can have a deeper conversation about which investments have the most impact and where customers may want to improve. This will be particularly helpful with more cybersecurity mature organization, where you need to be able to provide them with value beyond selling them a license. As a result, the channel can work with customers to create their own security ecosystems now and in the future, without being limited to one vendor or overhauling existing security solutions. This is not only a huge plus for the customer, but also gives channel partners an opportunity to gain trust and increase margins.

The future is open

In a difficult economic climate and a growing threat landscape, the channel can become a trusted partner to ensure businesses' cybersecurity investments are both cost-effective and offer an extensible, approach to threat prevention, detection and response. By providing vendor-inclusive, open XDR platforms, channel partners will help deliver value that will see companies become safer and more secure, despite ongoing turbulence.

Delivering environmental value – the SI opportunity

Countries globally are coming together to address the financial implications of climate change and deliver solutions for those communities most at risk. It is now vital to deliver ubiquitous access to smart technologies that will mitigate the effects of environmental change, especially in developing nations and why innovative Systems Integrators (SIs) have a key role to play.

BY ERIC MENARD, VP OF STRATEGY AND BUSINESS OF ASTROCAST

THE FINANCIAL IMPLICATIONS of climate change are taking centre stage. One of the biggest issues raised during COP 27 was reparation for the three-and-a-half billion people living in countries highly vulnerable to climate impacts, with the UN chief making a call for progress on adaptation and building resilience to future climate disruption. He insisted that countries need to build on the promises made in COP26 of $40 billion in adaptation support by 2025, with needs estimated to reach more than $300 billion dollars a year by 2030.

Adaptation will require far more than handing over funds to devastated communities. From improving food security and providing clean water to reducing the environmental impact of farming and tracking the risks to life associated with weather events, innovation is now essential.

But how can effective change be achieved without a detailed understanding of the current situation? How can farmers manage the transition to a different climate and embrace smart farming or agriculture 4.0 practices without the information required to support more effective methods or the ability to remotely monitor livestock, equipment and soil?

Capturing Knowledge

IoT has a key role to play in supporting change and innovation. Farmers, for example, are exploring IoT to remotely monitor soil moisture and temperature as part of the move to reduce water consumption while optimising productivity, as well as track animal health and well-being. Environmental tracking is allowing climate experts to monitor the speed with which change is occurring – from the reduction in emissions created by farming to the recovery of deep-sea habitats and remote snow, glacier and permafrost monitoring stations in Central Asia.

Further, monitoring is transforming lives in countries with limited clean water resources. Access to Water has distributed more than 150 million litres of clean water to Senegal, where around 20% of the population has no access to clean water. The charity uses filtration devices that not only treat

dirty, polluted or brackish raw water but also collect vital information about water quality and equipment usage to support both proactive maintenance and strategic planning.

When 15% of the world is covered by terrestrial communication networks, far too many of the most vulnerable communities remain unconnected and unable to benefit from this innovation. For SIs, the addition of Satellite connectivity to IoT solutions is hugely powerful, enabling companies to take tried and tested solutions quickly to new markets.

Proactive Approach

The availability of a satellite connection designed specifically for widescale IoT deployment has transformed the opportunity. But does the business case stand up, especially when the cost/ benefit argument is under incredible scrutiny?

Most operational IoT applications do not require the continuous or real-time communication associated with high-cost, power hungry satellite links that have made such solutions completely unaffordable. Instead, critical solutions such as tracking the location of farm animals, measuring the earth moisture content or monitoring the health of vulnerable habitats, can be delivered with lower cost intermittent satellite communication.

Minimal power consumption and the ability to link to solar power are key considerations when attaching an IoT sensor to a water filter, to livestock or farm equipment many miles from maintenance services. Ten-year battery life is a significant factor in building a powerful business case, as is antenna design and robustness of equipment and battery life. Two-way communication is also valuable, for example if the SI wants to increase the frequency of recording in a specific location from once to twice a day.

Powerful Business Case

The model is working. Affordable, reliable connectivity across the globe is extending the use of intelligent farm control systems, for example, allowing existing sensors to be used to record and control information remotely over long distances. Using sensors that are connected to the cloud, and IoT-based digital agriculture, factors such as weather, temperature, humidity, rainfall data, water level, water quality and soil moisture are helping to transform the effectiveness of farming and maximise plant health.

Satellite IoT (SatIoT) is enabling farmers to digitise animal tracking, so that they can accurately establish the location of their herds, allowing them to better manage livestock. For example, they can track movement patterns and create geo-fences to establish when livestock has drifted into the wrong areas.

Commercial beekeepers, meanwhile are using SatIoT for colony management, ensuring continual information irrespective of the hives' locations, such as remote areas of California where farmers rely on rented bee colonies to pollinate the majority of the world's almond harvest. Real-time data from active hives, including temperature, humidity, movement, and even sound frequencies is passed to the cloud for monitoring and analysis, providing beekeepers with the information required to track hive health.

Conclusion

Change is happening. Countries and organisations globally are actively investing to support change, especially within agriculture. With funding commitments of $8 billion, The Agriculture Innovation Mission for Climate (AIM for Climate), for example, seeks to accelerate innovation in "climate smart" agriculture especially aimed at small-holder farmers in developing economies, new technologies, agro-ecological research and methane reduction.

However, without ubiquitous access to network connectivity, there will be an unfair difference in the speed with which countries, organisations and individuals can make changes and adopt innovations such as smart farming or agriculture 4.0 practices. This will create even greater disadvantages in populations already disproportionately affected by climate change.

With the addition of low-cost SatIoT, innovative IoT solutions previously restricted by the lack of terrestrial/cellular connectivity in locations that are, by their very nature, outside the mainstream areas of network coverage, can now be quickly and effectively delivered to accelerate essential and equitable change.

Embracing digital transformation to reshape your growth strategy

The growth of a Managed Service Provider (MSP) usually follows a distinct pattern. It starts with a modest number of customer accounts and a high ratio of support agents, essentially over-servicing the customer to make sure they stay happy and have no reason to go elsewhere. Most of the tasks and processes remain manual and laborious but, in recognition of the error-prone nature of working in this way, the team is dedicated to fixing any problems immediately and demonstrating fast response times.

BY ANDY VENABLES, CTO AT POPX.

THE SMALL MSP will typically run disparate internal systems and applications to serve those customers, and although this means effort is often duplicated, it's not operating at full capacity, so the situation is manageable, although far from efficient. The objective is to serve the customer in any way they can, which may include a high level of customisation to serve specific customer needs. This may even develop into a deep understanding of one or a small number of industry sectors.

However, as the MSP grows and acquires more customers, it becomes apparent that over-servicing each one will start to put the engineering and support teams under significant pressure, which will negatively impact their performance. Maintaining the standard of service established with early customers would require a significantly sized engineering operation that would have to grow exponentially in line with customer demand. This

operating model is simply not affordable or sustainable.

Changing ways of working by streamlining processes and automating tasks have huge benefits for tech service providers. According to research from MIT, digitally mature organisations are 26% more profitable than their less mature peers. Yet, while MSPs make it their business to advise clients on their digital strategies, it's clear they also need to adopt the same practices in-house, if they haven't started already.

How customers drive the need for change

Savvy customers frequently assess MSPs on their level of digital maturity before buying from them. Customers put a significant focus on the quality of their experience and according to Forrester, companies that lead in customer experience outperform competition by nearly 80%.

The technological capabilities of an MSP can be better understood by prospecting customers by examining its portfolio of services, customer reviews, and success stories. However, customers want to work with MSPs that also use the latest technology, tools, and software solutions to run their business internally. It's simply not enough to offer the latest products and services. Internal factors are

so important that they are considered of equal importance to understanding an MSP's pricing structure and value proposition.

How can digital transformation ease the burden?

There are many operational and financial performance benefits to digital transformation for companies in all industry sectors, but especially for tech service providers. Perhaps the most significant improvement is the ability to stay ahead of the competition.

By embracing new technologies and implementing more efficient automated processes, service providers can differentiate themselves, offering clients better and more innovative services with an unmatched customer experience.

Improving efficiency by adopting a scalable and integrated operating model that embraces service automation helps reduce costs, while improving service levels, resulting in high levels of client satisfaction. It is also a pathway to sustained profitability for the long term, because as the business continues to grow its customer base, it no longer has to exponentially increase costs to serve them.

Tips on how to approach transformation

Getting to grips with digital transformation can be a daunting task. However, with the right approach and strategy, it is possible to get it right the first time. Here are some steps that MSPs can take to implement digital transformation and create a blueprint for success in the process:

- **Assess your current state:** The first step is to assess your current state. This includes looking at your technology stack, business processes, and service offerings. Identify areas where you can improve and prioritise these areas based on their impact on your business.
- **Define your goals:** Once you have assessed your current state, you need to define your goals. This includes identifying what technologies you want to implement and how they will improve your service offerings and business processes.
- **Create a roadmap:** With your goals in mind, create a roadmap that includes timelines, milestones, and key performance indicators (KPIs) to measure progress.
- Implement your plan: When implementing your plan, you may need to find a partner to work with that is experienced in the MSP sector. You may also need to hire and assign resources to the project and invest in new technologies. It's important to monitor progress and adjust your plan as needed.
- **Continuously improve:** Transformation is a never-ending process of continuous improvement, so remember to factor this into your cultural and organisational development. It will be important to help staff develop existing and new skills, as well as create defined career paths for them.

Get to value quickly

Executing a transformation plan requires dedicated time and resources, but how do you manage it? You can go it alone, taking full responsibility for the outcome as well as all the risk, or you can find help from a specialist partner that knows your industry and can help de-risk the project. In either case, it is important to demonstrate value to your customers and back to the business in terms of increased performance as quickly as possible. Once this is done, you can then continue to improve operations from there.

Digital maturity allows tech service providers to quickly adapt and respond to changes in the market. Your digital capability can redefine your operations and efficiencies to give you that competitive edge. When assessing digital maturity, consider the needs of all who are connected to your business, internal and external stakeholders, customers and third parties, and then develop a strategy that has growth and collaboration at its core.

Navigating cloud diversity

How MSPs achieve neutrality in a multi-provider world.

BY LEE THATCHER, HEAD OF CLOUD, CLOUD COCO

SIN TODAY'S ever-evolving landscape of cloud computing, managed service providers (MSPs) play a pivotal role in assisting businesses as they make the transition to the cloud. However, MSPs face a significant challenge in striking a balance between the diverse needs of their clients and the offerings provided by major cloud providers, often referred to as hyperscalers. This challenge has given rise to the concept of being "cloud agnostic," a strategy aimed at offering services that are independent of any specific cloud provider.

Being cloud agnostic, in essence, means providing cloud services that are not tied to any particular hyperscaler. MSPs embracing this approach have the flexibility to operate across multiple cloud providers, free from the constraints of a single provider's offerings. This approach empowers MSPs to leverage the strengths of various cloud providers to craft tailored solutions that align perfectly with their clients' requirements.

So, what are the advantages of this approach? Organisations pursue being cloud agnostic because it offers a wide array of benefits for both MSPs and their clients. Each hyperscaler brings its own unique advantages to the table:

- Google Cloud excels in analytics and AI c capabilities, making it an ideal choice for data-driven applications.

Huntsman®
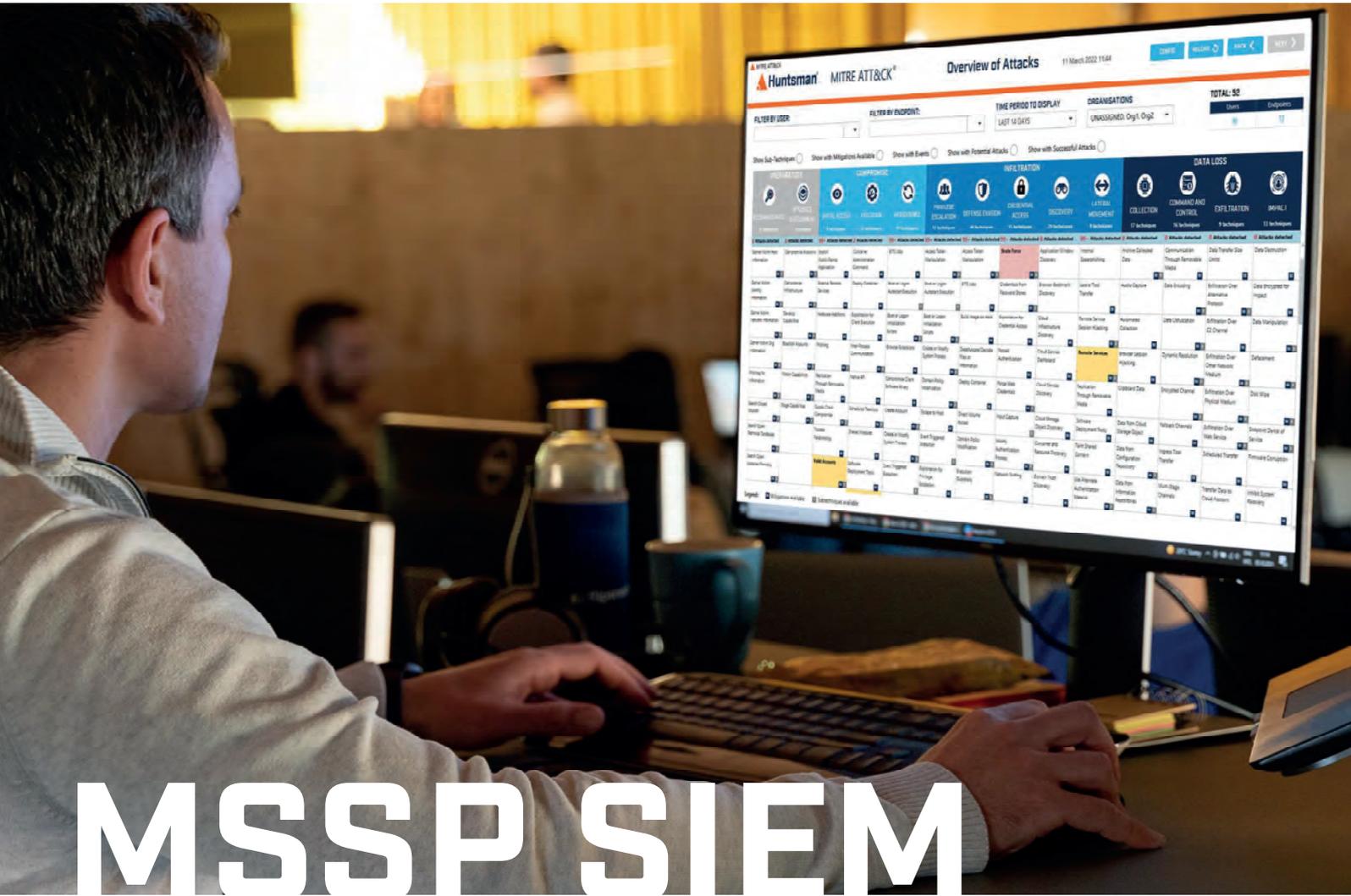
MSSP SIEM

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
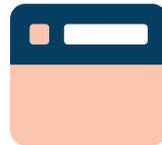
FULLY FLEXIBLE, INCLUDING DATA SOURCE SUPPORT
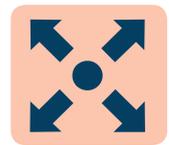
SCALABLE AS YOUR BUSINESS GROWS

BOOK A DEMO
huntsmansecurity.com

- Microsoft Azure offers enhanced security features, catering to industries with stringent compliance requirements.
- Amazon Web Services (AWS) boasts the title of the largest cloud provider and offers extensive scalability.
- Alibaba Cloud stands out for its cost-effectiveness.
- Oracle Cloud caters to enterprises in need of robust database solutions.

By not limiting themselves to a single hyperscaler, MSPs can tap into these strengths to meet the diverse needs of their clients.

One of this approach's primary benefits is avoiding vendor lock-in. By not relying on a single hyperscaler, MSPs ensure their clients retain the flexibility and autonomy to shape their cloud strategy. This empowerment enables clients to make informed decisions, reducing the risks associated with being overly dependent on a single vendor. Additionally, being cloud agnostic contributes to cost optimisation. MSPs can select the most cost-effective solutions from different hyperscalers and negotiate based on performance, ensuring that clients get the best value for their investments.

Challenges with multi-cloud approaches

However, there are challenges on the technical and operational fronts when it comes to remaining cloud agnostic. MSPs need to build and maintain a highly skilled technical team capable of offering services across multiple cloud platforms. This unique skill set can be a hurdle in itself, requiring continuous training and updates to keep up with evolving technologies.

Moreover, managing different cloud platforms comes with operational hurdles, including the need for a workforce with diverse skill sets, efficient issue resolution across platforms, and selecting the right technology for each client's unique requirements. To effectively manage relationships with various cloud providers while maintaining neutrality, MSPs often rely on a central portal through which all interactions are conducted, ensuring consistency and fairness.

Strategic client advice without favouritism towards any particular cloud provider is a complex task. MSPs must possess in-depth knowledge of each hyperscaler's offerings to provide the best-fit solutions. This means maintaining a versatile skill set across all major cloud platforms, ensuring clients receive well-informed advice tailored to their specific needs.

In interactions with cloud vendors, MSPs should uphold principles of fairness and transparency. Recommendations should be driven by client needs rather than any vendor preference. This transparency fosters trust with both clients and cloud providers, leading to better collaboration and mutually beneficial outcomes.

A multi-cloud future

Looking ahead, the concept of being truly cloud agnostic is expected to continue evolving within the MSP landscape. The trend of multi-cloud usage is gaining momentum as organisations recognise the benefits of leveraging different hyperscalers for specific needs.

MSPs will likely evolve into facilitators, assisting clients in navigating the complexities of multi-cloud environments and facilitating seamless integration. Emerging technologies like AI and business automation are anticipated to play a significant role in the future. These technologies enable streamlined management of diverse cloud platforms and efficient allocation of resources, ultimately enhancing the client experience.

The pursuit of true neutrality represents a critical step forward for MSPs. By operating without allegiance to any specific hyperscaler, MSPs can harness the strengths of multiple cloud providers to deliver tailored solutions.

While the journey is not without its challenges, the benefits of being cloud agnostic – flexibility, cost optimisation, and risk mitigation – are driving MSPs to strive for neutrality, empowering both themselves and their clients in the ever-evolving landscape of cloud computing.

How cloud can help Managed Service Providers serve more customers in less time

In recent years, the availability of managed services has grown exponentially with customers being more informed than ever on new IT possibilities.

BY DOMINIK BIRGELEN, CEO OF ONECLICK

ACCORDING to the UK Government over 65% of medium-sized businesses and 75% of large businesses across the UK utilise at least one managed service provider (MSP). With new innovations emerging every day, MSPs offer companies a great opportunity to stay up-to-date on technology and have access to the appropriate skills and solutions required.

However, rising costs and security problems have hindered the progress of MSPs within this sector. According to Statista, over 40% of MSP owners and technicians have reported difficulties with acquiring more customers due to business and operational challenges. MSPs have also found it difficult to scale customer outreach due to a lack of know-how and resources for the subsequent operation of the cloud environment.

As technology continues to evolve, organisations need to accelerate their digital trajectories to provide measurable benefits for their customers. But, to constantly innovate and drive their strategy, most MSPs do not have the IT capabilities, bandwidth, or resources to strike the perfect balance between their business and technology needs.

Companies that provide managed services of the latest cloud-based solutions to simplify the provisioning of infrastructure, applications and services can not only support MSPs to administer more customers in less time but can also enable them to implement infrastructure projects seamlessly.

Cloud Solutions in an MSP's Infrastructure

Leveraging cloud-based solutions is crucial for MSPs to develop a scalable and secure infrastructure. With advanced solutions, MSPs can reduce provisioning costs by up to 50% for both themselves and their customers. Utilising cloud advancements brings about scalability, cost-effectiveness, remote access, automation and quick deployment capabilities. These factors enable MSPs to effectively support clients by optimising resource allocation, automating tasks and strengthening security measures.

Additionally, MSPs find it difficult to scale performance and customer-service capabilities due to technical, business, and operational issues which often stem from cybersecurity and data storage compromises. Data continuity, a critical aspect of cloud migration, is also a key pain point with many corporations facing data loss or downtime challenges which could lead to financial and reputational damages. Companies can address this through advanced cloud solutions which provide

increased business and cyber resilience, helping MSPs overcome underlying issues.

Why Cloud Innovation is Fundamental to Boost Efficiency

In addition to gaining infrastructure support, MSPs need to leverage cloud solutions to improve their disaster recovery, rapid response times and network security. Through cloud services, businesses can access increased control over service levels, performance, and maintenance. Furthermore, enterprise-wide monitoring and automation allow regular monitoring and maintenance of IT functions. Cloud MSPs are also able to support business operations through a regular backup of data onto the cloud, which helps corporates protect sensitive information and makes disaster recovery possible while ensuring employees and customers continue to enjoy uninterrupted service.

Advanced cloud offerings also enable MSPs to provide robust cybersecurity support seamlessly through zero-trust architecture (ZTA), antivirus software, encryption, and multi-factor authentication. This allows businesses to safeguard themselves from the growing number of cyberattacks while bolstering their IT foundations.

Cloud for Different Operating Concepts

Today, companies leverage cloud technology as per their unique needs. Some utilise managed public cloud whereas others take advantage of managed hybrid and multi-cloud. All of them have individual challenges related to costs, implementation, complexity and more. MSPs need advanced solutions that can help them address these challenges.

For example, MSPs can leverage automation and orchestration tools to automate day-to-day repetitive tasks. This saves time, maximises efficiency and reduces human error. As a result, businesses need fewer resources to manage their tasks and can save significant costs. What's more, based on the unique requirements of companies, MSPs can use cloud tools to seamlessly integrate multiple technologies into one platform. This can help them simplify implementation, streamline their operations and manage more customers in less time.

Organisations providing managed services need to manage multiple tasks for several different customers. Leveraging the cloud to increase efficiency and reduce time spent on time-consuming tasks is an effective way to maximise profitability. Finally, MSPs can partner with a cloud provider and take advantage of the cloud as a service.

This will allow them to pay based on their cloud usability, and leverage the latest updates and maintenance, allowing them to save unnecessary additional expenses.

Unlocking business transformation:
The power of a customer-centric partner ecosystem

In today's rapidly evolving digital business landscape, customers are raising the bar for their partners and vendors.

BY MARILYN MOODLEY, COUNTRY LEADER FOR SOUTH AFRICA AND WECA AT SOFTWAREONE

CUSTOMERS no longer settle for basic support; instead, they demand effective assistance to expedite their digital transformation and overcome industry-specific challenges. As these projects become more intricate, it's clear that no single provider can cover all bases.

In response to these escalating customer expectations, it's imperative for businesses to recognise and harness the potential of partner ecosystems. Marilyn Moodley, Country Leader for South Africa and WECA at SoftwareOne, emphasises that the collective value generated by these ecosystems surpasses what individual players can achieve.

Meeting the demand for holistic customer solutions

Customers are no longer content with standalone products or services; they seek comprehensive solutions that yield tangible business outcomes, underpinned by genuine support. They prefer to collaborate with companies committed to ensuring customer success, rather than mere product or service suppliers.

Establishing a network of trusted partners who prioritise customer needs is pivotal. These partners, working together, form an ecosystem – a collective of players from diverse industries or verticals collaborating to develop and deliver solutions. This

transforms them from passive suppliers to active contributors to their customers' businesses.

Embracing collaboration over competition

A partner ecosystem represents a network of businesses collaborating to provide more extensive solutions to customers. This model is increasingly prevalent in the digital technology sector, especially when resources are limited, and companies need to expand their reach and scale.

Creating a partner program offers mutual benefits, particularly for smaller partners in South Africa who can thrive with the support of larger distributors. By pooling resources and knowledge instead of directly competing, businesses can efficiently reach and serve more customers as a collective, rather than attempting individual customer outreach.

Defining a partner ecosystem: unity in diversity In our increasingly complex work environments, no business can tackle every challenge in isolation. The abundance of service providers offers both obstacles and opportunities for customers. The era of limited choices among a few established players is over; customers now enjoy the freedom to select providers based on value, compatibility, and shared core values.

In this customer-centric market, partners must unite to demonstrate trustworthiness, credibility, and the ability to deliver outstanding services, setting them apart from competitors.

Furthermore, knowledge sharing within the partner ecosystem is crucial, as no single partner or organisation can offer all-encompassing solutions. Collaboration among resellers, distributors, and partners paves the way for more effective market service. Cultivating trust, transparency, and collaboration.

Establishing robust relationships and trust between partners and the organisations they serve is pivotal for mutual success. When contemplating the creation or joining of a partner ecosystem, several factors must be considered.

Firstly, identifying the right partners is essential, with an emphasis on complementarity in business, shared values, and aligned goals. Secondly, clear value propositions for these partners must be outlined to ensure mutual understanding of the benefits derived from ecosystem participation. Effective ecosystem management, encompassing transparent expectations, regular engagement, and accessible conflict resolution mechanisms, is also vital.

Transparency and trust are the cornerstones of successful partner programs. Incentives, targets, and transparent communication of value are integral components of every partner program, with partners having access to a shared portal for tracking their share of gross profit. However, a customer-first

approach is indispensable within these ecosystems to facilitate cooperation, ensuring faster delivery, higher service quality, and exceptional customer satisfaction.

Driving satisfaction, innovation, and efficiency

When customers take center stage within an ecosystem, businesses are more inclined to develop products and services tailored to their needs. This can result in heightened customer satisfaction, loyalty, and advocacy.

A customer-centric approach also fosters innovation, as businesses prioritise meeting customer needs, inspiring the creation of new products and services that cater to those requirements. This, in turn, positions businesses to lead in the competitive landscape and expand their market share collectively.

In this customer-centric market, partners must unite to demonstrate trustworthiness, credibility, and the ability to deliver outstanding services, setting them apart from competitors

Another significant benefit of a customer-centric approach is the potential for cost reduction. As businesses focus on meeting customer needs, they are more likely to develop efficient and effective products and services, ultimately leading to cost savings and improved bottom-line results.

Uniting for greatness

In a customer-driven market, trustworthiness, credibility, and outstanding service delivery are the hallmarks of a great partner ecosystem.

The importance of a robust partner ecosystem should not be underestimated. SoftwareOne leverages a global ecosystem for access to a collective of various industry professionals. Such collaborations ensure that the company can approach challenges with a diverse set of insights and resources. It's not merely about providing services; it's about leveraging a vast network to deliver well-rounded solutions that add value.

By nurturing strong relationships through knowledge sharing and collaborative efforts, businesses can harness the collective strength of resellers, distributors, and partners to offer comprehensive solutions that meet customer needs and drive their success.

The role of cloud in UC - and the opportunities it presents to the channel

Imagine if the technology industry was designing business communications for the first time today: it would look very different.

BY IAIN SINNOTT, HEAD OF INTERNATIONAL CARRIER SALES, ENREACH FOR SERVICE PROVIDERS

FLEXIBILITY would likely be at the centre of the wheel, giving customers individuality, with far more options and control based on their requirements, circumstances, points in time, and place. More rigid room or desk-centric capabilities would be on the outside, and mobility at the heart instead of a traditional PBX environment.

Communications would also seamlessly blend multiple contact streams, such as voice, chat, video, collaboration tools, CRMs, ERPs, vertical market applications, and more. All these contact streams would work together to create a seamless environment regardless of location, whether in the same room or connecting virtually, available across different devices, networks and apps. That is true unified communications.

Cloud communications is the enabling consumption model for that ideal world, pivoting in an agile way around customers and the needs of their businesses. Of course, cloud-based UC is nothing new: it has been talked about for many years and successfully deployed by service providers worldwide. However, the market is at an exciting tipping point, where it has the potential to embrace more widely this more customer-centric, flexible approach to business communications. For the channel, it represents massive potential and the technology components are available. While we cannot start from scratch, we can certainly think about and approach the opportunity in a fresh way.

User scenarios

Also, next-generation, future-facing cloud-based UC can significantly enhance businesses' own customer engagement strategies, such as providing an omnichannel choice of contact methods, like web chat, voice or WhatsApp.

Imagine a hair salon's loyal customer who spends an average of 600 Euros annually. The customer has a big event and so needs an appointment quickly. However, they cannot get through to speak to someone directly, only to a basic voice mailbox, with no indication if and when they will get a response. So, acting on a friend's recommendation, they book with another salon in the same town, have a great experience, and never return to the first salon.

Conversely, with converged UC, the caller could receive a friendly message saying they will get a response in a couple of minutes and that the salon knows they are waiting. They also have options of a callback or booking immediately via IVR or WhatsApp.

Team members in the hunt group for missed calls also get an alert on their mobile phones that someone is waiting. Through integration with the salon's CRM, they see it is regular customer Jill, so when the call is answered, they greet her by name (and may even have time to get her records up on screen). However, head stylist Joe is busy with a tricky hair colouring, so he has set his presence as

unavailable and, therefore, temporarily opted out of the hunt group. That said, he is also expecting an urgent call from his wife. By having different personas able to exist on his mobile, her call gets through while others are diverted. Finally, at the end of the month, the salon owner can access missed call reports, average waiting times, and call recordings to monitor and improve the quality of staff and customer interactions.

Successful implementation

Plus, beyond giving SMBs these benefits, cloud-based UC has enormous potential for resellers to engage with much larger enterprises without necessarily having to invest in additional in-house technical expertise, ideal for IT resellers who want to add comms to their portfolios.

Even though the Unified Communications as a Service (UCaaS) market is increasingly competitive, especially with hyperscalers like Google and Microsoft getting in on the act, there is a lot of potential, especially by putting some best practices in place.

For instance, based on what we have seen work across Europe, starting small with the achievable wins and building on those is recommended. After all, while there are some fantastic innovations on the near horizon, many organisations still need to adopt some of the already widely available UC features, such as call queues and recording.

While PBX replacement is just one element of the broader UCaaS opportunity (and voice is just one of multiple contact streams), it is still a helpful door opener. This might mean a service provider combines traditional PBX telephony features with virtual meeting and collaboration tools and some simple contact centre functions for customer service. Features could include call recording, call back, chat queues, and IVR, plus smart inbound voice routing. Consider integrating mobility so that all those features and services are available on smartphones because helping customers mobilise their businesses is also a massive opportunity for the channel.

The result? An enhanced customer experience, a more productive workplace, and technology that works around employees, regardless of time or place. However, those SMB customers can continue

using legacy services, even if ultimately they tend to migrate away from them, further contributing to near-term ROI.

Once that foundation is in place, then it becomes possible to build out even more, perhaps integration with more business apps, adding an automated onboarding and provisioning portal, or integration with specialist vertical market solutions. This is where APIs come into play, acting as the intelligent glue bringing everything together into one environment. APIs are also evolving and are becoming easier to access and use, acting as gateways to create larger ecosystems, choice, and reseller differentiation.

Similarly, we are seeing a move towards having multiple, often competitive technologies available in the same platform, enabled by intelligent API layers, giving both the reseller and its customers far more choice. The days of inflexible, one-size-fits-all UC platforms are numbered. Rightly so: modern UCaaS should be all about delivering business customers access to technology that fits around the way they work (or want to work), helping them to improve productivity, communications and collaboration in one seamless environment with tech that enhances their lives rather than getting in the way. And if that is not a compelling argument for exploring what the latest developments in cloud-based UC have to offer, then I don't know what is.

Even though the Unified Communications as a Service (UCaaS) market is increasingly competitive, especially with hyperscalers like Google and Microsoft getting in on the act, there is a lot of potential, especially by putting some best practices in place

CELEBRATING 13 YEARS OF SUCCESS

Announcing the 14th edition of the premier IT awards: The Storage, Digitalisation + Cloud Awards 2023.

In what has been, and continues to be, extraordinary times for the business world, it seems doubly important to recognise the projects, innovations and individuals which have made such a huge difference during 2023. Almost overnight, employees switched from office working to working from home, and the new, or next, normal, means that, into the future, what might be called a 'hybrid work' model looks set to evolve, with flexible working very much the order of the day. What was already becoming a trend as part of many organisations' digital transformation programmes, has been accelerated.

The SDC Awards 2023 will celebrate the achievements of end users and the IT community as they have innovated like never before to ensure business continuity in these challenging times. This year more than any other, please do make sure that you enter our SDC Awards. There's no limit to the number of entries, all of which are free of charge, and we'll be promoting all the short-listed entries via Digitalisation World's multi-media platform over the coming months, ahead of the awards ceremony. We really do want to celebrate and recognise the many amazing achievements which have come about in response to the coronavirus.

THURSDAY 30 NOVEMBER

ROYAL GARDEN HOTEL, KENSINGTON, LONDON

BOOK YOUR TABLE NOW!

CONTACT
Sukhi Bhadal: sukhi.bhadal@angelbc.com
Peter Davies: peter.davies@angelbc.com

SDC AWARDS 2023

www.sdcawards.com