DW

DIGITALISATION WORLD

MODERN ENTERPRISE IT - FROM THE EDGE TO THE CORE TO THE CLOUD

ISSUE VI 2022

DIGITALISATIONWORLD.COM

BCAS: What is it and why do you need it?

LOGPOINT
Unified Simplicity

AIOps | Apps + DevOps | Artificial Intelligence | Big Data + Analytics | Cloud + MS
DC Facilities + Colo Digital Business | IT Management + Service | Networks + Telecoms
Open Source | Security + Compliance | Storage + Servers

AN ANGEL BUSINESS COMMUNICATIONS PUBLICATION

NHS
Birmingham Women's and Children's
NHS Foundation Trust
ICT Department
apt
ADVANCED POWER TECHNOLOGY

Editor's View

By Phil Alsop Editor

Human and machine – the perfect combination?

Hardly a day goes by when each one of us has a chance to reflect on the ongoing evolution of what will hopefully be no more than the augmenting of humans with machines – with some worrying signs that automation is seen as the only way forward.

There are many variables when it comes to each individual's preferences when it comes to interacting with other humans and/or machines – based on a whole range of variables, such as age, location, education, socio-economic factors and many more. Although I suspect that many of us can agree on what activities should remain the preserve of humans exclusively and which ones can be handed over full time to machines, there are a surprising number of interactions where there is disagreement. Disagreement either in terms of a straight choice between human or machine or, perhaps more likely, the degree to which humans and machines should both be involved.

Businesses across the globe are trying to understand this landscape, in the hope that they can both improve customer service and their bottom lines. In many cases, these twin objectives go hand in hand. However, in rather too many, it seems that money wins out over the customer experience (CX). For example, certain supermarkets have reduced the number of human-operated tills in favour of self-service checkouts. Those shopping for just a few items, who experience no scanning issues, might well be satisfied with the automation experience, especially if there's no queueing involved.

Those with plentiful items, where the scanning runs less than smoothly, are less than impressed. And those who enjoy the, all be it brief interaction with someone at the checkout, will ignore the machine option altogether. Depending on how far one is willing to travel to shop for groceries, it's more than possible to find a store that offers the preferred shopping experience. And, of course, there's also the online option, with goods delivered to the door – and maybe some conversation with the delivery driver, and the thought that one lorry delivering multiple customers' shopping has top be more sustainable than hundreds of customers driving to the supermarket.

And, right now, a similar range of shopping or interaction experiences is available in most of our lives, whether business or leisure. We can do things the 'old-fashioned way' (although much early automation, such as ATMs, is now an accepted part of 'old-fashioned'!), embrace the digital world in full or navigate our way somewhere in the middle. And this middle path, where we choose our preferred combination of human and/or machine is where most of us sit for now.

How the future develops depends largely on the consumer's willingness to accept automation even where it clearly is not in their interest (ie virtual medical appointments are unlikely to ever be as thorough as face to face ones), alongside the possible change in attitude to business brought about by the journey to Net Zero. We all like to the idea of cheap, plentiful consumerism, but if the price to pay is the death of our planet, maybe attitudes might just change.

In conclusion, organisations of all shapes and sizes need to spend considerable time and thought on understanding the threats and opportunities of digital solutions, with maybe more of a focus on the customer than the company profit margin. If not now, then very soon.

CONTENTS

VOL. 28 ISSUE VI 2022

DW DIGITALISATION WORLD

BCAS: WHAT IS IT AND WHY DO YOU NEED IT?

Given the growing threat, volume and complexity of cyberattacks globally, Business Critical Application Security (BCAS) should now be a priority for businesses seeking to bolster their cybersecurity

32

THE ANALYST

CYBERSECURITY

AR / VR

COMPUTING

APPLICATION

DIGITALISATION

The data centre trade association

DCA News

DATA ANALYTICS

OBSERVABILITY

NEWS

DW DIGITALISATION WORLD

Angel BUSINESS COMMUNICATIONS

Editor
Philip Alsop +44 (0)7786 084559 philip.alsop@angelbc.com
Sales & Marketing Manager
Shehzad Munshi +44 (0)1923690215 shehzad.munshi@angelbc.com
Sales Executive
Jessica Harrison +44 (0)2476 718970 jessica.harrison@angelbc.com
Director of Logistics
Sharon Cowley +44 (0)1923 690200 sharon.cowley@angelbc.com
Design & Production Manager
Mitch Gaynor +44 (0)1923 690214 mitch.gaynor@angelbc.com
Publisher
Jackie Cannon +44 (0)1923 690215 jackie.cannon@angelbc.com

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

Directors
Stephen Whitehurst: Chairman
Scott Adams: Chief Technical Officer
Sukhi Bhadal: Chief Executive Officer

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

Digitalisation World is published 8 times a year on a controlled circulation basis in Europe, Middle East and Africa only. Subscription rates on request. All information herein is believed to be correct at time of going to press. The publisher does not accept responsibility for any errors and omissions. The views expressed in this publication are not necessarily those of the publisher. Every effort has been made to obtain copyright permission for the material contained in this publication. Angel Business Communications Ltd will be happy to acknowledge any copyright oversights in a subsequent issue of the publication. Angel Business Communications Ltd. © Copyright 2022. All rights reserved. Contents may not be reproduced in whole or part without the written consent of the publishers.
The paper used within this magazine is produced by chain of custody certified manufacturers, guaranteeing sustainable sourcing. ISSN 2396-9016 (Online)

AI is A1

Over half of global business leaders believe investing in AI will give them a competitive advantage.

SAMBANOVA SYSTEMS has published the results of its global research on AI adoption within enterprise organizations. It found that business leaders are increasingly deploying AI and progress could be further accelerated by moving beyond a fragmented proliferation of small models. Enterprise leaders are placing AI at the core of a multiyear technology strategy and two-thirds (67%) believe it will be transformational or significantly change how they do business in 12 to 24 months.

The driver behind the change that ai will deliver

When asked about the type of change that AI will deliver, global business leaders cited the top three drivers:

- §80% think that AI will improve the employee or customer experience by streamlining processes and decreasing response time
- 68% think AI will cut costs by automating processes and initiating a better use of head count
- 51% will use AI to increase profit through better use of data or opening new revenue streams

There is another reason behind adoption of AI – it is increasingly becoming a competitive asset. The research found that almost three-quarters (72%) of business leaders believe their competitors are using AI, and of those almost two-thirds (63%) are concerned their competitors will use AI to gain an advantage over their own business.

Marshall Choy, SVP Product at SambaNova commented on the findings: “Enduring enterprises always keep a sharp eye on technology as a way to rise above competitors. Just like railroads, radio, and the internet have done for previous generations, AI is reshaping business as we know it and over the next decade, early investors and adopters stand to yield the greatest benefits.”

Businesses need to consolidate models creating an enterprise-wide strategy based on large models

One of the biggest challenges enterprises face is the number of AI models currently deployed in production. Only 18% of organizations utilizing AI are deploying it as a large-scale enterprise-class initiative. The rest - 82% - are introducing it across multiple programs, which can create unexpected hurdles and a less coherent AI strategy.

However, in the era of general purpose large language models, there is now a better way.

Choy elaborated on the benefits of large language models: “You’ll be hard-pressed to find an enterprise that runs more than a handful of relational databases. Most organizations have consolidated their databases, which means they are well understood, maintainable, secure and auditable. This hasn’t happened with AI models yet.”

“Most organizations that have a significant AI footprint have been left with a myriad of hundreds or even thousands of disparate models,” stated Choy. “They are not easily manageable, and certainly not auditable. This is where a single foundation model for language can be the firms’ AI backbone at enterprise scale as the basis for all AI applications and workflows for the next decade.”

One of the biggest challenges enterprises face is the number of AI models currently deployed in production. Only 18% of organizations utilizing AI are deploying it as a large-scale enterprise-class initiative. The rest - 82% - are introducing it across multiple programs, which can create unexpected hurdles and a less coherent AI strategy

Post-pandemic leaders emerge to reimagine applications and digital delivery

Cisco AppDynamics has released the annual Agents of Transformation report which reveals the emergence of a new class of post-pandemic technology leaders who are reimagining applications and digital services delivery as the lines between IT operations and business strategy blur.

CISCO APPDYNAMICS, a leading provider of Observability and Application Performance Monitoring technology, has published findings from Agents of Transformation 2022, the fourth annual report that analyzes the skills and attributes of elite global technologists.

In the wake of the pandemic, it reveals the emergence of a new class of technology experts stepping up to meet critical challenges that are blurring the lines between business strategy and IT operations. The report also cites the demand to make all products and services digitally available in the Experience Economy amid h eightened security threats, increasing complexity, and the accelerated shift to hybrid work and the cloud.

"The bar continues to rise, and over the last year we have seen a redefinition of what it means to be an Agent of Transformation. These leaders are looking to better understand how issues in their respective domains impact the total experience of users and applications, adapting to change with solutions that positively affect the overall business," said Liz Centoni, EVP, Chief Strategy Officer, GM of Applications.

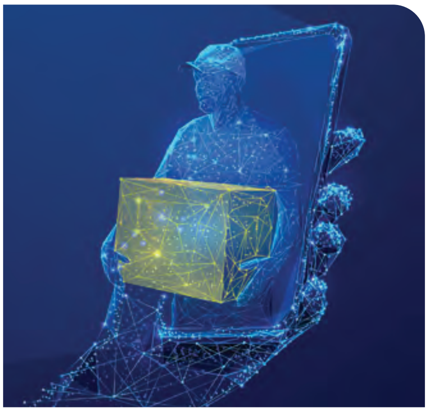
According to the Cisco AppDynamics report, 74% believe that their experiences in recent years—particularly during the pandemic—have accelerated their careers, and 88% now consider themselves to be business leaders. However, just 10% of technology experts have reached the elite status of 'Agents of Transformation'. These individuals represent top-flight leaders who are reimagining and delivering high-value applications and services that create the always-on, secure, and exceptional user experiences now demanded by end users and customers.

Respondents cite a fundamental change in the role of technologists, including the skills and resources required to operate effectively and proficiently. At the same time, they say they now contend with soaring complexity and volumes of data from across the technology stack and must integrate a massively expanding set of cloud-native services with existing on-premises systems and tools.

- 88% believe that what it means to be a technologist has changed
- 84% say the skills and qualities that define an Agent of Transformation have evolved
- 66% indicate that it is now more difficult to be an Agent of Transformation
- One in four say their organization remains stuck in reactive, "fire-fighting mode"

Digital transformation means almost every company and organization interacts with consumers via web and mobile applications, and the transition to hybrid work means more interaction with SaaS tools and web interfaces. While consumers can pivot fast to another brand's app or service, companies that cannot instantly improve digital experiences risk having loyal customers walk away.

"The new Agents of Transformation recognize a need to reimagine applications not just in response to post-pandemic challenges, but also, to create flawless, reliable digital experiences that address some of the world's greatest problems—from meeting critical human needs to giving people the skills and resources to succeed in the digital economy," Centoni said.



While acknowledging the far-reaching consequences of this change, respondents in the Cisco AppDynamics report note that they need help navigating the technical and operational ambiguities of digital transformation. Specifically, they are looking for unified visibility into their IT environments to better manage and optimize application availability and performance. This requires focusing investments on application security, observability over cloud-native applications and infrastructure, and linking IT performance to business decision making.

- 77% believe it will be important to invest in application security over the next 12 months to meet all needs
- 71% think their organization will need to invest in observing cloud-native applications and infrastructure
- 84% say that the need to maintain the performance of business applications is now most important
- 85% state that full stack observability is core to sustainable transformation and innovation in their organization

Intelligent automation will lead companies out of global crises

Automation Anywhere signals intelligent automation will be a strategic lever as businesses brace for a recession.

AS WORLD TENSIONS increase and the stock market faces volatility, business leaders indicate that intelligent automation has become a pivotal strategy to navigate current market challenges and sustain business performance. Of the 1,000 global organizations surveyed, more than 90 percent say automation addresses the impact of supply chain and economic uncertainty, according to the third edition of the Automation Now & Next report from Automation Anywhere and leading research firm Futurum Research.

Consequences of the global pandemic, ongoing trade concerns, and political conflicts have disrupted business operations, which has, in turn, exacerbated existing workforce issues, created supply shortages, and made demand forecasting and customer engagements more complex.

The Automation Now & Next report found that overwhelmingly, organizations are making intelligent automation a foundational technology to overcome these obstacles.

"We're seeing things we never thought we would experience in our lifetime – and that's forcing companies to rapidly adapt and understand how to remain agile for unexpected events and scale their automaton strategies amid ongoing disruptions," said Mihir Shukla, CEO and Co-Founder of Automation Anywhere. "Our third Automation Now & Next Report revealed that intelligent automation is the prevailing technology that is proving to be the most crucial asset for businesses in every sector across the globe. As a result, organizations have dramatically increased budgets to support new automation initiatives."

This is particularly timely due to global workforce shortages juxtaposed with unprecedented product and customer demand. Shukla continued, "It doesn't matter what you produce, or where you produce it. It's vital to get work done and deliver products to customers. And with the speed and agility offered by cloud automation, we can address this need."

Automation Investments are Trending Upwards

Looking ahead to 2023, the report shows automation budgets are dramatically increasing, with more than 77 percent of organizations indicating they will boost their automation budgets in the year ahead and expect to have 500 or more bots deployed within 12 months. A quarter of respondents say they are escalating automation funding by at least 25 percent to help speed up automation deployments.

With automation proving to be core to business operations the report also indicates that:

- 77% of respondents said they've made automation a priority for the next 12 months having achieved an average return on investment of 6.3X
- 94% of respondents state automation is helping address supply chain issues
- 61 % of respondents strongly agree that automation has helped address staffing shortages
- 70% of companies state that 30% of their work across business functions can be automated

The Future of Automation is Cloud

The research also found that cloud-based automations are integral for future-proofing business transformation strategies. Cloud delivers agility and flexibility to rapidly respond to the nature of today's quickly evolving environments, which rings true for the 90 percent who said they're moving from on-premises to cloud automation – and for the 93 percent who said they have already adopted a cloud-first approach for all new automation initiatives.

Research uncovers the cost of work complexities

Wrike has released new findings that uncover the cost of work complexities brought about by the Digital Era and accelerated transformations.

ACCORDING to the research report commissioned by Wrike, "Dark Matter of Work: The Hidden Cost of Work Complexities," up to 55% of the work that takes place within an organisation is not visible to key stakeholders, costing organisations up to $60 million a year in wasted time, delayed or canceled projects, and employee churn. This lack of visibility has created the "Dark Matter of Work," a term coined by Wrike Founder Andrew Filev to describe the vast amount of work that isn't captured, tracked, or measured against goals because it takes place in synchronous applications and unstructured ways.

"The current economic climate has created an urgent need for organisations to increase efficiency and drive up productivity while providing their employees with a genuine sense of purpose in the work they contribute," says Andrew Filev, Senior Vice President and Wrike General Manager, Citrix. "What we're finding, and is important for organisations to note, is that the Digital Era has created a new level of chaos and misalignment, which is exacerbated by the over-proliferation of apps and data. It has actually begun offsetting major projects and losing organisations their best talent. Neither of which organisations can afford as we move into a turbulent economic market. In order to survive this next stage with optimum efficiency, it is going to be critical for organisations to understand the depth of work complexities and what they need to do right now to overcome them."

Wrike surveyed 2,800 business leaders and knowledge workers to determine the root causes of work complexities and the severity of the impact on businesses, teams, and individuals.

The financial and human cost of the Dark Matter of Work is staggering. Organisations with approximately 3,200 employees - the average number surveyed - can lose up to $52 million annually in wasted time caused by unproductive meetings, duplicated efforts, information seeking, and status check-ins; $8.2 million in delayed or canceled projects; and $427,000 in employee churn. Organisations with 100 employees can lose over $1.65 million annually, and those with 100,000 can lose over $1.65 billion.

Work complexities have been growing steadily over the last decade, but it wasn't until recent years that they began to create significant gaps in information visibility and collaboration. This is a result of the surge in applications and data processed, as well as the general pace of work today. Just as CERN, the European Organization for Nuclear Research, identified Dark Matter as the "invisible" content that makes up 95% of the mass of the universe, modern work complexities have generated a significant body of work that teams can't immediately see, but that has a powerful influence on the projects around it.

This Dark Matter of Work lives in synchronous applications and unstructured work, such as instant message threads and video calls, as well as the gaps between systems and applications that aren't integrated.

Without a single work platform in place that is powerful and versatile enough to track, manage, action, and align all work to goals across an organisation, there exists a dangerously low level of visibility amongst knowledge workers and leaders.

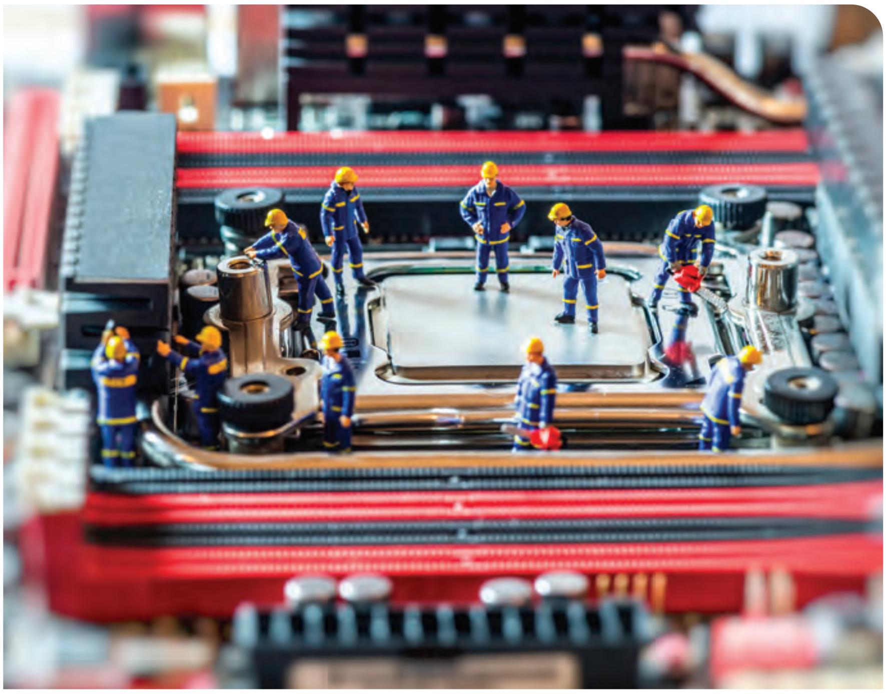
Wrike's survey uncovered data that supports the existence of the Dark Matter of Work, the very real cost it has on organisations, and the path forward toward optimum efficiency:

- 86% of business leaders have had to adopt new communication and collaboration tools to support remote and hybrid working, adding to the complexity of understanding individuals' work.
- Knowledge workers say they use 14 applications every day, and nine new applications were rolled out on average amongst businesses as a result of the pandemic.
- Business leaders say they can only integrate 51% of their applications.
- The average knowledge worker sends and receives 295 work-related messages each day.
- Knowledge workers spend 18 working days a year in meetings.
- 65% of business leaders encounter problems with projects at least every week that could be avoided with real-time insight into project status.
- 59% of business leaders say it is impossible to say how well everyone is progressing because so much of the latest information is in a black hole.
- 78% of knowledge workers find themselves working at cross purposes with their colleagues.
- 62% of knowledge workers say they feel overworked.
- If the Dark Matter of Work is not controlled, this number is expected to grow 53% in the next five years.
- 94% of knowledge workers say that a single source of truth for information would reduce stress in their teams.
- 86% of enterprises are planning to invest in tools, such as artificial intelligence and workflow automation, to create a single source of truth for work in their enterprise.

Survey reveals microservices and service mesh as critical

Solo.io has unveiled survey results that indicate that modern enterprises are standardising on microservices — and that service mesh is a core component powering this architecture. The research also pointed to a strong correlation between success with microservices and faster, more reliable application development — with almost half describing the impact of service mesh as "transformative."

"IT'S NO SURPRISE that Kubernetes has 'crossed the chasm,' with nearly two-thirds of companies using it in production and an overwhelming majority of companies are modernising with microservices," said Idit Levine, founder and CEO, Solo.io. "Enterprises are struggling to manage this explosion of services — and they are turning to service mesh and API gateways to manage an increasingly complex application environment. Meanwhile, Istio is emerging as the Kubernetes of service mesh, with leading companies choosing an Istio-based service mesh by an almost three-to-one margin to boost application reliability and security."



Modernising to Microservices – But Still Feeling Pain

The 2022 Service Mesh Adoption Survey, conducted by Solo.io and ClearPath Strategies, shows that 85% of companies are modernising their applications to a microservices architecture. These companies also report that microservices drive faster development cycles, as 56% of organisations with at least half of their applications on a microservices architecture have daily or more frequent release cycles. However, the uptick in microservices and increased development velocity have led to pain for many organisations as they struggle with microservices and API sprawl as well as added technical debt. Also, more than 70% of organisations report having delayed or slowed down application deployment into production due to application networking or security concerns.

As microservices become a modern enterprise "must," service mesh and API gateways have become viable solutions to address the headaches of managing application reliability, security, and observability. An overwhelming 87% of companies report using or evaluating a service mesh for use. The shift to service mesh technology can be attributed to the broad deployment of container-based architectures and explosion of microservices, which come as a result of companies looking for ways to expedite their digital transformation and move to a cloud-first posture or fully cloud-native development.

Service Mesh: A "Transformative" Solution

Service mesh, which controls service-to-service communication over a network, offers a solution for managing application reliability, security, and observability along with application traffic monitoring and management. The vast majority of respondents (89%) reported a very positive impact on application reliability as a result of using service mesh, including 44% who called the impact "transformative."

While service mesh is still considered a new technology, nearly half of all companies (49%) reported using service mesh at some level. And adoption is greater among companies with a high degree of containerised architectures and Kubernetes usage. Among organisations with more than half of their production workloads running on Kubernetes, 81% use a service mesh, compared to only 45% of those organisations with half or less of their production workloads on Kubernetes.

Critical operations threatened by application incompatibility

New research discovers that many businesses are unprepared for modernisation.

OVER THREE QUARTERS (77%) of organisations have at least one application that is not compatible with the latest version of Windows, with up to a quarter (25%) of all applications incompatible for 89% of organisations. This is according to new research of UK and US CIOs commissioned by Cloudhouse, the application compatibility packaging and configuration management solutions provider.

Despite these findings, almost a third of businesses (32%) reported that between 16-25% of their applications are critical to their business operations, while 36% cited modernisation as an urgent priority. Ensuring application compatibility is therefore pivotal, but organisations are also hesitant to initiate such projects, with almost a quarter (24%) of organisations either not at all or not very confident in their ability to fully upgrade these platforms to be 100% compatible with the latest version of the Windows operating system.

This lack of confidence among CIOs may stem from the fact that half of all businesses (50%) feel that there is a significant amount of work to still be done to modernise applications for compatibility with newer Windows versions. Additionally, 25% believe that they've now ironed out most issues, but there is still some work to be done to ensure modernisation. Only one in five (20%) have a comprehensive plan in place.

"Our research has discovered that application compatibility is, unfortunately, a common occurrence among businesses, and if left unchecked can impact the platforms that are absolutely critical to operations. It's vital for these organisations to make use of specialist tools that allow applications to be transplanted to new Windows operating systems, without losing any functionality or impact on the user experience," Mat Clothier, CEO and Founder of Cloudhouse.

Of businesses with a plan of action, almost one in three (29%) have a primary strategy to replace their application to ensure compatibility with a new Windows version, but this is typically costly, time-consuming and may require additional training for employees to use an unfamiliar platform.

Across other findings, in the area of internal websites, respondents identified almost half (49%) of incompatible applications as desktop versions, creating a negative impact on the user experience. Despite these findings creating a cause for concern, 55% of organisations plan to increase their 2022 budget for application modernisation by more than a quarter (26% or above), with 17% planning to increase it by more than 50%, revealing a clear intent to improve compatibility.

Of businesses with a plan of action, almost one in three (29%) have a primary strategy to replace their application to ensure compatibility with a new Windows version, but this is typically costly, time-consuming and may require additional training for employees to use an unfamiliar platform

Increased IT complexity impacting ROI

SolarWinds IT Trends Report 2022 examines the current state of hybrid IT complexity.

WITH HYBRID and remote work amplifying the challenge of managing distributed IT environments, 84% of IT professionals believe the ROI of their projects has been negatively impacted in the last 12 months. This is according to new research from SolarWinds, a leading provider of simple, powerful, and secure IT management software.

The report, which examines the acceleration of digital transformation efforts and its impact on IT departments, also shows a third (33%) of IT professionals think complexity added between four and seven months of extra work to get their project to completion.

Commenting on the news, SolarWinds President and CEO Sudhakar Ramakrishna said, "Many organisations are struggling to drive forward transformation amidst increasingly distributed and complex IT environments.

"Amplified by a global move towards hybrid and remote work, applications and workloads are now run across both cloud and on-premises infrastructure.

"This is not only hindering the ability to deliver benefits to end users in a timely fashion but also significantly impacting the bottom line.In this challenging landscape, IT professionals are increasingly looking towards observability to manage these growing levels of complexity. By understanding where to prioritise their efforts, teams can manage hybrid IT realities more effectively and achieve the ROI targeted in their planned projects, which spells long-term success for teams, businesses, and their customers."

Majority of European office workers trust that their workplace is investing in future technology

Three-quarters are optimistic that technology will create new career opportunities.

NEW RESEARCH commissioned by Ricoh Europe, which polled 3,000 office workers across the UK, Ireland, France, Germany, Italy, the Netherlands and Spain, reveals that:

- 73% trust that their workplace is investing in technology now to meet the workforce requirements of the future
- 75% are optimistic about the opportunities technology can bring to their career – a 19% increase since 2020
- 34% think they will work with robots or AI at their workplace in the next 5 years – an increase of 24% since last year
- 85% expect their employer to provide the tools and training to help them adapt to new roles as technology changes
- 53% agree that their employer provides the right technology and creates a culture that supports how they need to work
- 35% say it is difficult to feel motivated and engaged while remote working due to communication / technology problems – an increase of 20% since 2020
- 44% think their company culture suffered during coronavirus restrictions

Nicola Downing, CEO, Ricoh Europe, says: "Investing in the right technology for hybrid working is intrinsically linked to its success, as is having a robust future-proof strategy in place.

"Both employees and decision makers are realising the potential for technology to boost careers and workplace culture.

"Using technology to create the right workplace experience is vital to attracting and retaining the best people in a market where digital-savvy talent is in such high demand."

EXAGRID
EXAGRID
EXAGRID

European investments in public cloud services to reach $113 Billion in 2022

According to the International Data Corporation (IDC)'s Worldwide Public Cloud Services Spending Guide, Public Cloud Services (PCS) spending in Europe will reach $113 billion in 2022 and will double to $$239 billion by 2026, growing at a 22% 5-year 2021-2026 CAGR.

INVESTMENTS in Software-as-a-Service (SaaS) will continue to lead most of the spending in Public Cloud in Europe in 2022, but Platform-as-a-Services (PaaS) will be the fastest-growing segment as PaaS delivers enables business agility by allowing companies to quickly test and implement applications they have developed.

Professional services, banking, and discrete manufacturing will be among the top spenders in Public Cloud Services, absorbing almost 60% of the overall Public Cloud Services spend in 2022. Human-centric industries are adjusting their work policies to normalize remote working. This means that more attention to remote employee access to information will drive spending in Cloud solutions. Implementing digital-first and cloud-based strategies will continue to be a focus and the European PCS spend (excluding Russia) will grow 26.4% this year, showing that cloud will be resilient despite the conflict between Russia and Ukraine. Similarly, Russian investments in cloud solutions are expected to grow (7.7% YoY) in 2022, but with many companies pulling out of the country, growth will be slower than the rest of Europe.

“European companies want to automate their processes as they are experiencing market challenges including supply chain disruption and skill shortages. More frequently companies will adopt Cloud to create a solid real-time data analysis foundation that support business agility and resilience,” said Andrea Minonne, senior research analyst at IDC UK.

Public cloud has allowed the organization to focus on its core competencies, while delegating the complexities of owning, operating, and maintaining the actual IT infrastructure to public cloud service providers. As a result, we’re seeing a flurry of innovation that is driven by the ability to put efforts into the development of new products and services without the constraint of organizations’ ability to deploy them.

Companies are more frequently using Cloud services to upgrade and take their operations to the next level to streamline processes and strengthen the value they deliver to customers. Public Cloud Service providers are extending cloud services to edge locations, and this is supporting investments in the technology. Many factors including the conflict in Ukraine, is supporting many sectors including government to migrate to Cloud solutions for security reasons and this is supporting the next wave of cloud adoption for industries that hadn’t yet adopted the technology.

Worldwide Public Cloud Services revenues grew 29.0%

The worldwide public cloud services market, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service – System Infrastructure Software (SaaS – SIS), and Software as a Service – Applications, grew 29.0% year over year in 2021 with revenues totaling $408.6 billion, according to the International Data Corporation (IDC) Worldwide Semiannual Public Cloud Services Tracker.

Spending continued to consolidate in 2021 with the combined revenue of the top 5 public cloud service providers (Microsoft, Amazon Web Services, Salesforce Inc., Google, and SAP) capturing nearly 40% of the worldwide total and growing 36.6% year over year. With offerings in all four deployment categories, Microsoft captured the top position in the overall public cloud services market with 14.4% share in 2021, followed closely by Amazon Web Services with 13.7% share.

“Organizations continued their strong adoption of shared public cloud services in 2021 to align IT investments more closely with business outcomes and ensure rapid access to the innovations required to be a digital-first business,” said Rick Villars, group vice president, Worldwide Research at IDC. “For the next several years, leading cloud providers will play a critical role in helping enterprises navigate the current storms of disruption (inflation, supply chain, and geopolitical tensions), but IT teams will also focus more on bringing greater financial accountability to the variable spend models of public cloud services.”

While the overall public cloud services market grew 29.0% in 2021, revenue for foundational cloud services* that support digital-first strategies saw revenue growth of 38.5%. This highlights the increasing reliance of enterprises on a cloud

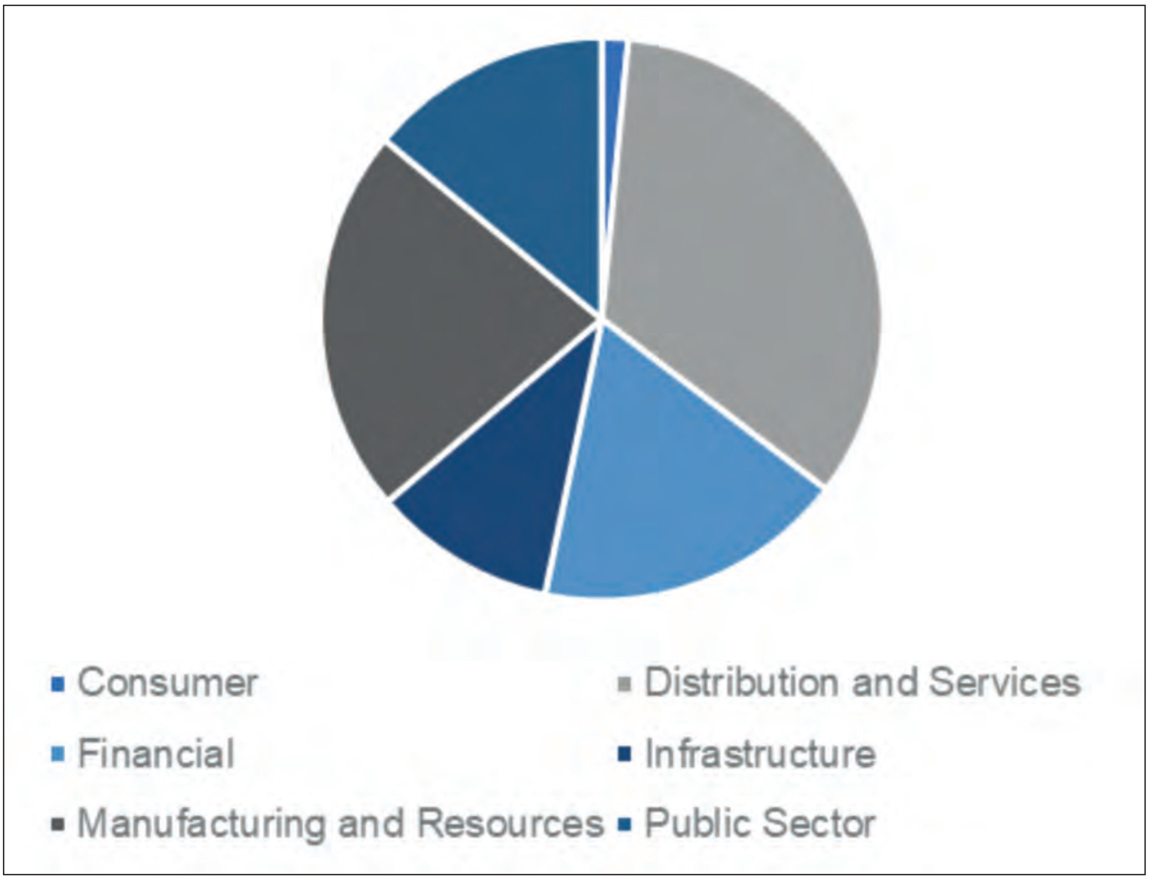
Worldwide Public Cloud Services Revenue and Year-over-Year Growth, Calendar Year 2021 (revenues in US$ billions)

Deployment Category	2021 Revenue	Market Share	2020 Revenue	Market Share	Year-over-Year Growth
IaaS	$91.3	22.4%	$67.3	21.3%	35.6%
PaaS	$68.2	16.7%	$49.1	15.5%	39.1%
SaaS – Applications	$177.8	43.5%	$143.9	45.4%	23.5%
SaaS – System Infrastructure Software	$71.2	7.4%	$56.4	17.8%	26.4%
Total	**$408.6**	**100%**	**$316.7**	**100%**	**29.0%**

Source: IDC Worldwide Semiannual Public Cloud Services Tracker, 2H 2021

While both the foundational cloud services market and the SaaS – Applications market are led by a small number of companies, there continues to be a healthy long tail of companies delivering cloud services around the globe. In the foundational cloud services market, these leading companies account for nearly three quarters of the market’s revenues with targeted use case-specific PaaS services or cross-cloud compute, data, or network governance services. The long tail is more pronounced in the SaaS– Applications market, where customers’ growing focus on specific outcomes ensures that over two thirds of the spending is captured outside the top 5.

Source: Worldwide Public Cloud Services Spending Guide 2022 | Jun (V2 2022)



innovation platform built around widely deployed compute services, data/AI services, and app framework services to drive innovation. IDC expects spending on foundational cloud services (especially IaaS and PaaS elements) to continue growing at a higher rate than the overall cloud market as enterprises leverage cloud to overcome the current disruptions and accelerate their shift toward digital business.

"The last few years have demonstrated that in challenging times, businesses increasingly rely on cloud services to modernize their operations and deliver more value to customers," said Dave McCarthy, research vice president, Cloud and Edge Infrastructure Services. "This trend is expected to continue as public cloud providers offer more ways of extending cloud services to on-premises datacenters and edge locations. These expanded deployment options reduce many barriers to migration and will facilitate the next wave of cloud adoption."

"In the digital-first world, enterprises that are serious about competing for the long term use the lens of business outcomes to evaluate strategic technology decisions, which fuels the fast-growing ecosystem seen in the public cloud market," said Lara Greden, research director, Platform as a Service, IDC. "Cloud service providers showed relentless drive to enhance the productivity of developers and overall speed of application delivery, including emphasis on containers-first and serverless-first approaches."

"SaaS applications remain the largest and most mature segment of public cloud, with 2021 revenues that have now reached $177 billion. The tailwinds of the pandemic continued to fuel expedited upgrades and replacements of older systems in 2021, though company goals haven't changed.

Companies seek applications that will help increase enterprise intelligence, improve operational efficiency, and drive better decision making. Ease of use, ease of implementation and integration, streamlined workflows, data and analytical accessibility, and time to value are the key criteria driving purchasing decisions, though verticalization has also steadily increased as a key priority," said Eric Newmark, group vice president and general manager of IDC's SaaS, Enterprise Software, and Worldwide Services division.

Worldwide spending on ESG Business Services to reach $158 Billion in 2025

Organizations face mounting pressures to improve and document their environmental, social, and governance (ESG) performance. Because the initial steps to a sustainable transformation can be daunting to firms that have not attempted anything similar in the past, sustainability-linked consulting spending has become a high priority.

A new forecast from International Data Corporation (IDC) estimates that ESG business services spending will grow to $158 billion in 2025 with a five-year compound annual growth rate (CAGR) of 32.3%.

“In 2022, all enterprises are being pushed to transform and fundamentally change the way they do business to become sustainable enterprises,” said Dan Versace, research analyst, ESG Business Services. “Owing to increased pressure from customers, investors, and regulators, organizations are beginning to understand the business cases for sustainability. Those organizations that develop and implement plans to better internalize and address their environmental and social impact stand to thrive in the years ahead as leaders in the sustainability space.”

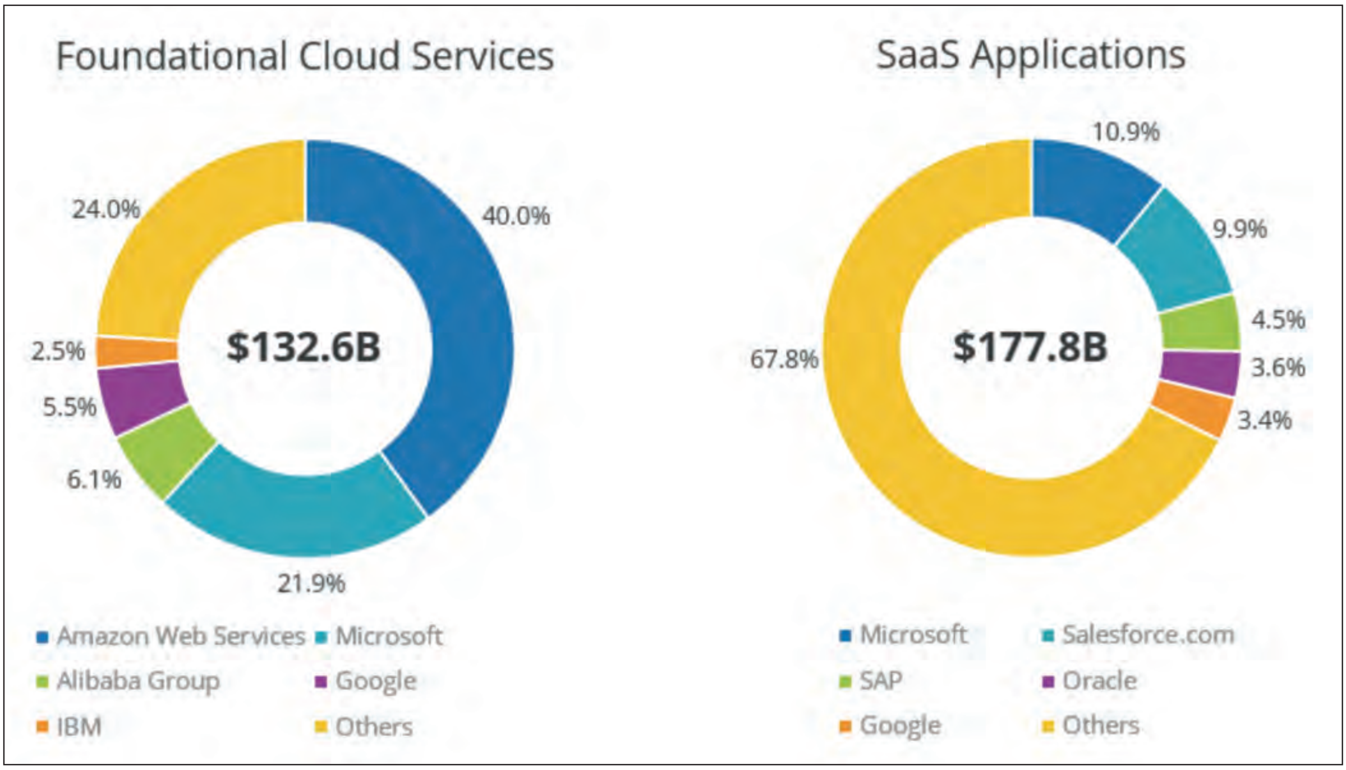
IDC defines environmental, social, and governance (ESG) business services as traditional professional services that are centered around achieving goals related to environmental and social sustainability and the governance of that process. It can also include ESG-enabling services, known as sustainability-linked professional services, that enable organizations to increase their sustainability capabilities through traditional business process improvement, such as services focused on increasing process efficiency or supply chain services to reduce risk.

The main focus areas for organizations’ investment in sustainability are business strategy, human capital management solutions, and risk management. The largest area of spending, strategy consulting, will enable organizations to efficiently embed sustainability into their business strategy, which is the driving force of corporate purpose and in turn sustainable operations. Human capital management will be the fastest-growing area of spending. This is primarily due to the dual challenge of creating large-scale organization-wide training and process efficiency improvements necessary for sustainability efforts to succeed in the future, on top of addressing social pillar topics such as human capital management internally.

The increased spending across functions is forcing organizations to address corporate sustainability in a holistic way, moving away from the ad hoc approach that was present in years past. This imperative to act sustainably in all facets of an organization is becoming more powerful as mandated sustainability disclosures draw nearer. While many organizations are already reporting on their climate-related performance voluntarily (scope 1 and 2 emissions, carbon intensity, etc.), professional services will still be needed to increase the process efficiency as more resource-intensive reporting becomes mandatory. In addition to the recognition of the inherent link between social and environmental sustainability beginning to be understood on the corporate level, more nuanced and pointed services will be needed to address the societal impact of enterprises’ operations in the future.

“By the end of the forecast period, IDC expects sustainability-linked business consulting services to encompass nearly two thirds of the total business services market,” added Versace. “With this market being still in its infancy, opportunities for differentiation are everywhere. Firms should assess their sustainability-linked business services to determine where these offerings can best be utilized and identify other end-user pain points where new offerings will be needed.”

Source: Worldwide Semiannual Public Cloud Services tracker, 2H 2021



Global IT market shows signs of slowing

Global combined market up 9%, but registers first sequential quarterly decline since Q3 2020.

GLOBAL DEMAND for IT and business services remains strong, although the market is showing signs of slowing amid recession fears, finds the latest state-of-the-industry report from Information Services Group (ISG) (Nasdaq: III), a leading global technology research and advisory firm.

Data from the ISG Index™, which measures commercial outsourcing contracts with annual contract value (ACV) of $5 million or more, show second-quarter ACV for the combined global market (both XaaS and managed services) reached $22.8 billion, up 9 percent versus the prior year, but down 7 percent compared with the first quarter.

It was the first time since the third quarter of 2020 that the global market did not grow sequentially – a period of six straight quarters in which quarter-over-quarter growth averaged 7 percent.

“We have been through an 18-month period of sustained high demand that has pushed the global market to new heights as companies accelerated their digital investments,” said Steve Hall, ISG president. “With fears of a potential recession on the horizon, we saw a slowdown in the second quarter and expect the market to be more volatile in the second half of the year.”

Hall said market demand remains high, as companies continue to embrace cloud computing and leverage technology to improve productivity, lower costs and get closer to customers to drive revenue growth. Yet the market faces headwinds, he said, including rising interest rates, lingering supply chain issues, a tight labor market and higher energy prices.

Results by Segment

The cloud-based XaaS market grew 13 percent in the second quarter, to $14.1 billion, but was down 11 percent versus the first quarter, as the market slowed from its average 44 percent quarterly growth rate over the last 12 months. Infrastructure-as-a-service (IaaS) rose 11 percent, to $10.2 billion, but was down 14 percent sequentially, reflecting weakness in China, which was impacted by extended Covid lockdowns and a tighter regulatory environment for the country's technology sector. Software-as-a-service (SaaS), meanwhile, was up 20 percent, to $3.9 billion, and off only 1 percent from the prior quarter.

Managed services spending rose 2 percent, to $8.8 billion – the fifth straight quarter it exceeded ACV of $8 billion. Flat quarter over quarter, the market slowed from its average 16 percent quarterly growth rate over the last six quarters. For the second quarter, IT outsourcing (ITO) declined 8 percent, to $6.0 billion, although it was up 5 percent sequentially. Business process outsourcing (BPO), meanwhile, rose 33 percent, to $2.8 billion, but declined 9 percent from the first quarter. With the historically strong data center business in decline, demand is shifting from large, legacy infrastructure deals to smaller application development and maintenance (ADM), engineering, and industry-specific BPO awards.

A total of 600 managed services contracts were awarded in the second quarter, up 5 percent versus the prior year, though down 4 percent from the first quarter. The awards included nine mega-deals (contracts with annual value of $100 million or more), the highest number in the last three years.

First-Half Results

The combined market reached ACV of $47.3 billion in the first half, up 19 percent over the prior year.

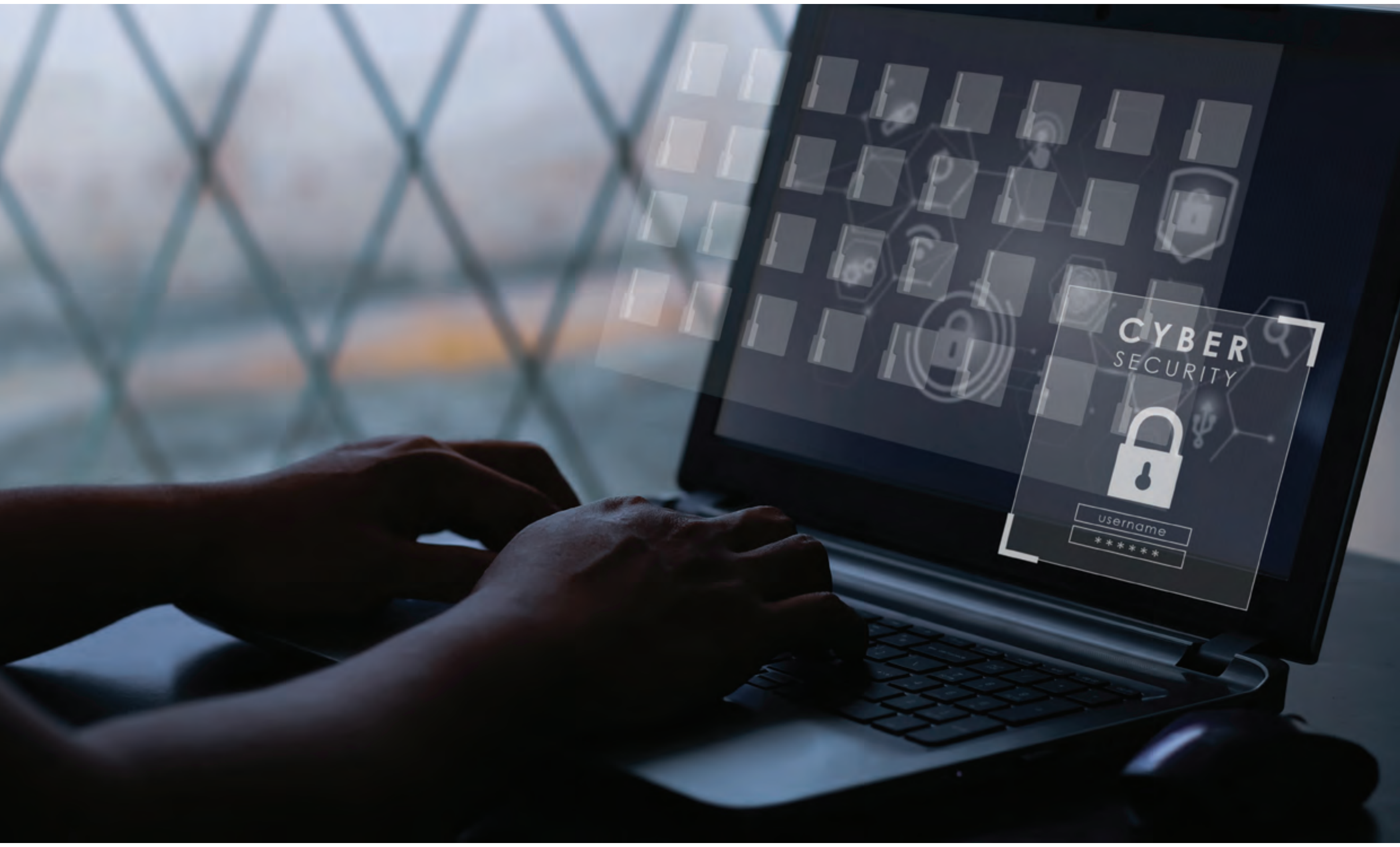
XaaS advanced 27 percent, to $29.8 billion, and now accounts for 63 percent of the combined global market, up from 51 percent three years ago. Managed services produced a record $17.5 billion of ACV, up 8 percent, on record volume of 1,225 contracts, up 12 percent versus the prior year.

2022 Forecast

ISG sees continued economic uncertainty impacting the second half of 2022, even as market demand remains high.

"We are lowering our growth forecast for managed services to 3.5 percent for the year, down from 5.1 percent last quarter, reflecting the negative impact of foreign currency translation and inflationary concerns," said Hall.

On the XaaS side, ISG is lowering its growth forecast to 18 percent, compared with its previous forecast of 22 percent. "We see this segment coming under pressure due to Covid and regulatory headwinds in China, leaving the big three hyperscalers – AWS, Azure and Google Cloud – to support market growth. China is down almost $1.5 billion year to date, and we don't see cloud providers there fully recovering this year."



What executives need to know about SASE

SASE is an invaluable technology for those aiming to streamline functions in hybrid on-premise/cloud environments.

BY ZACHARY MALONE, SYSTEMS ENGINEERING MANAGER, SE ACADEMY, PALO ALTO NETWORKS.

The Origin of SASE

Gartner introduced the term SASE in 2019. The analysts were considering whether there was a better way to preserve security and agility in response to the moving landscape of SaaS delivery for business – cloud computing, critical applications and branch expansion. In addition, they recognised a need for a convergence of such services that functioned in the same way as cloud, SaaS, and other application implementations.

The SASE approach, defined as a tactic that converges cybersecurity and WAN edge networking to overcome key issues companies deal with today, was Gartner's answer to this gap in the market. SASE aims to provide unified, secure access; creating connectivity and securing users as they transition between branches, homes, headquarters, and everywhere else. This will occur whilst accessing resources in data centres, cloud, SaaS, or on the web with a single, unified outlet.

Why is it Important in Cybersecurity?

The principles of Zero Trust, and the concepts of SASE, aim to shift security closer to the actual assets being guarded.

SASE's unique selling point is that it has a single platform focus for delivering services. As a result, the tech stack, policies and administration is simplified, while ensuring all access is stable. This cannot occur when aiming to use multiple disparate products, even from the same vendor.

As companies begin to explore a SASE strategy, specifically during the contemporary shift regarding the remote/hybrid workforce, many companies face a challenge in understanding their employee's day-to-day experiences. Feedback that includes slow systems or bad connectivity has risen massively, resulting in a higher need for in-depth exposure, commonly referred to as 'digital experience management' or 'user experience management'.

What's Driving the SASE hype?

Vendors have caught onto the quick rise in fame of SASE and also understand that they do not have the product portfolio to cover the wide spectrum of everything SASE can do. As a result, many have attempted to cover up the issue, trying to create the idea that the scope of SASE is not as large as the narrative that Gartner is claiming.

A select number of vendors argue that a specific piece of security, like Identity and Access Management and SWG, is "all you need" for SASE. Other vendors believe SD-WAN is the most vital aspect of SASE and the security is a mere addition, leaving it to third parties. These claims show signs of a misunderstanding because SASE is focused on aligning all the underlying features together into a single platform, implementing it "as a service" as much as possible. An approach that tries to isolate pieces or relies on numerous parties to cover all components is not SASE; it's just business as usual – a product of the hype manifested around the strategy.

What Executives Should Consider When Adopting SASE

As SASE is focused on security services and the convergence of networks, each vertical is equally vital for any organisation's SASE plan to succeed. Therefore, the focal point should be on having more services converged into a single service – not just a single vendor, operated from numerous pieces – without compromising effectiveness or visibility. The secondary focus, which is equally as important, is about administration and delivery. Delivery and administration of all SASE services should be as close to a SaaS model as possible. So, while a few assets will continue to be required to direct traffic to the edge, like a WAN edge connector (SD-WAN preferred), all the computation, advanced policy and administration for these should be cloud-delivered. As teams become more remote/hybrid, the user's experience should not diminish, raising a third focus. Experience management is vital and should again converge into the SASE contributions, as much as the network and security technologies.

Here are some questions to ask your team for a successful SASE adoption:

- Has access been analysed broadly enough? Regarding all the places users are working - home, branch, or on the go, and all the resources they are looking to access - across data centre(s), cloud, SaaS, and web?
- Can we deliver security posture consistency that avoids sensitive data loss and malware across all flows of traffic, including private apps? Regardless of the application users' access and where the user is working.
- What stops us from consolidating the tools we use? Especially if we can maintain consistent security while streamlining the tech stack.
- How will we keep visibility of the whole application delivery path? From endpoint to application – making sure we provide a successful user experience.
- How can we decouple the notion or policy of our network edge from the parameters of any one site, so easy scalability and superb experience is achieved?

Overall, it is clear that SASE is an invaluable technology for those aiming to streamline functions in hybrid on-premise/cloud environments. The demands in fluidity, with the focus of unifying users and resources, has rapidly evolved since 2019. SASE can now be the tool that companies in 2022 use to simplify and stabilise cybersecurity. This single platform service is an evolving and exciting strategy, with the potential to revolutionise cybersecurity uncertainties, and is therefore one organisations would be wise not to ignore.

> As SASE is focused on security services and the convergence of networks, each vertical is equally vital for any organisation's SASE plan to succeed. Therefore, the focal point should be on having more services converged into a single service – not just a single vendor, operated from numerous pieces – without compromising effectiveness or visibility

Digital workplaces and security, the difficult balance

It is important to properly anticipate the security challenges associated with digital transformation, or risk falling victim to the next data breach.

BY CHRIS VAUGHAN, AREA VP AND TECHNICAL ACCOUNT MANAGEMENT, EMEA AT TANIUM

DIGITAL WORKPLACES, or virtual collaborative spaces, represent the new modern digital HQs, enabling companies to navigate the COVID-19 crisis and successive lockdowns while limiting the damage to their organisation. As we look to the future, it's clear that work will be hybrid and digital workplaces now have their place in the information systems of organisations worldwide. But to take full advantage of their benefits, it is necessary to anticipate and respond to the associated security challenges presented by this new era of work.

Benefits and challenges of digital workplaces

While digital transformation was already underway for many companies depending on maturity and sector, the pandemic accelerated this process significantly. It is now inconceivable to turn back the clock, given the numerous advantages for employees: flexibility in terms of work location and hours, transparency and fluidity of exchanges, and ease of connection. The adoption of digital workplaces and introduction of collaborative platforms like Slack or Teams has freed employees from the constraints of office work only policies.

That said, expanding beyond the traditional on-premises work environment has significant impact on the boundaries of IT networks, with a large number of devices geographically distributed. While employees' ability to work remotely allows organisations to ensure continuity of service during lockdowns, this new paradigm raises important security issues.

> While employees’ devices and the software they use are at the top of the IT system pyramid, it is important to remember that they might be connecting to other servers. Bottom line is that wherever these devices are, the IT department needs to be able to see and manage them to secure them

Visibility and control

While employees’ devices and the software they use are at the top of the IT system pyramid, it is important to remember that they might be connecting to other servers. Bottom line is that wherever these devices are, the IT department needs to be able to see and manage them to secure them. What’s new is that these assets, which used to be located only on the company’s premises, are now widely distributed across private homes, semi-professional coworking spaces, etc. and are often connected to unsecured Wi-Fi hotspots.

This poses several challenges for IT managers. First, you must be able to identify all your assets, wherever they are, even if they only connect temporarily and change location regularly.

Once identified, you must be able to know their configuration: has this machine that only connects remotely from time to time received and installed the latest critical patch? Remote or not, operating systems and applications need to be up to date to maintain cyber hygiene and reduce the risk of cyberattacks. This means having the ability to intervene if needed on a multitude of networks, with very different bandwidths and security levels depending on where you are.

The problem arises again when employees then return to the company’s offices. It is imperative to be able to check the security level of the workstation and, if necessary, isolate it until it is brought into compliance.

License management

Another key consideration concerns service and license management. IT departments must be able to identify and adapt the digital applications and services available to employees according to their actual needs. For example, an employee working in a store will not need the same servicesas an employee in charge of inventory or supply chain, even though both need digital services that are integrated into the company’s overall digital workplace.

This approach to streamlining applications and services can result in significant savings on licensing costs, which are too often overlooked. Indeed, under the guise of small monthly expenses, the addition of these license costs can represent a very significant expense item.

Controlling assets in the event of an international crisis

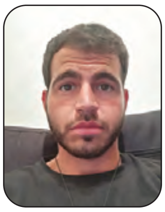
The last question to be asked has been raised by recent international crises, whether pandemic or geopolitical conflicts. It is a question of ensuring that we always have visibility and control over all assets, even if they are distributed in other parts of the world. While we can hope that this type of crisis rarely happens, it is the responsibility of IT departments to anticipate and prepare accordingly. International organisations should be able to quickly identify and, if necessary, isolate or even erase critical data from these desktops and servers, or risk having it fall into potentially hostile hands. And this must often be accomplished with few local human resources and degraded internet access. This should be a key consideration for any global organisation when choosing asset management and security tools.

Not only do digital transformation and digital workplaces represent excellent growth opportunities for organisations, but they also meet the level of service that users now expect from their employers. However, it is important to properly anticipate the security challenges associated with these evolutions and to prepare your organisation accordingly, or risk falling victim to the next data breach.

Keeping third party application secure in the cloud

In recent years, organisations have become increasingly aware that running third-party applications in their cloud environment exposes their workloads to greater risk. This is especially the case when this third-party software exposes some API functions to the public web.

BY GAL SINGER, SECURITY RESEARCHER AT AQUA SECURITY



TODAY'S MODERN CLOUD native workloads are proving an all too tempting target for attackers whose techniques are constantly evolving. Alongside exploiting web APIs to unleash cryptomining campaigns, they're also abusing free tier offerings of popular cloud CI/CD platforms to easily convert compute power into digital coins. To understand how vulnerabilities in third party scripts enable cybercriminals to infiltrate and hack, it's worth getting to grips with the attack practices bad actors employ to mask their activities and the steps they take to avoid being detected.

Anatomy of an attack Part 1: Initial access and defence evasion

Apache Struts 2 is a popular open source cross-platform web application framework used by many developers in their day-to-day work. Here at Aqua Security, we recently dissected how attackers went about exploiting an Apache Struts 2 vulnerability that allows remote code execution (RCE) under the privileges of the Apache web server.

Having initiated an HTTP GET request to check if a server is vulnerable, the hackers launched a second HTTP GET request containing an execution command line that downloads and runs a shell script into an organisation's container.

With the initial access attack completed, the shell script's first goal is to undermine security defences and prepare the ground for its next actions. Alongside disabling firewalls, allowing traffic, and deleting LD_PRELOAD, the script executes multiple kill commands to eliminate any competing malware or processes such as cryptominers and cloud agents.

Having completed all these tasks, the attackers next delete log files in a bid to cover their tracks and avoid detection after the fact.

Anatomy of an attack Part 2: Execution

Having cleared the way for the overall attack, the script now sets up variables and a 'get' function which is used to download and execute the main malware binary – a cryptominer. Packed by UPX to avoid detection via hashes, this binary has two functions.

Alongside performing cryptomining, it also actively looks to run more cryptominers on more container instances. It does this by gathering all available credential information held within the container itself and using a loop to connect to neighbouring systems, so it can download and execute the same malware script on these lateral systems. The analysis we undertook on this specific attack found the malware executed a massive scan in a bid to find open SSH (port 22) and Redis (port 6379) ports in the internal container network, sending over 24,000 packets to those two ports.

Anatomy of an attack Part 3: The payload

Now safely ensconced in the container, the malware next runs a different instance of the same binary with a different process name, connecting back to the attackers' command-and-control (C&C) server to download and execute a 'coinminer' variant. To support and enhance cryptomining efforts, the attacker also attempted to load an MSR kernel module to boost the overall speed of the mining process.

Understanding the risks

Today's threat actors are continually looking for ways to exploit known vulnerabilities in third-party software, so they can install cyptominer malware on unsuspecting organisations. Using someone else's processing resources to conduct the mining process and generate profitable digital treasures is on the rise; last year incidents of cryptomining malware soared by 300%. While this may sound innocuous, crypto currency mining software can result in significant performance issues in servers, databases and application development frameworks and even Denial of Service (DoS) scenarios. But that's not all. Having gained an initial foothold into an organisation's environment, there's little to prevent bad actors from pivoting their attack efforts to focus on other higher value assets.

Today's attackers are constantly honing their tactics to hide their cryptomining activities. Alongside disabling firewalls, they're also deactivating the non-maskable interrupt that signals attention for non-recoverable hardware errors and system resets. Plus, they're downloading encoded and obfuscated shell scripts to prevent security tools from understanding their intent. Ultimately, the aim of the game is to evade detection for as long as possible and maximise the potential for a return.

Securing the environment

The relentless speed of the modern DevOps cycle means keeping track of all workloads and software running in the organisation's cloud environment is a big task. Best practices to improve security include enforcing two-factor authentication for all users, setting branch protection restrictions, and restricting forked pull requests to run on the CI platform. Alongside finding and fixing known CVEs and security flaws, constantly monitoring containers and troubleshooting suspicious behavioural patterns is now a must have. Utilising runtime analysis, with tools that feature in-built rule sets, on third-party applications like Apache Struts 2 will help flag up potential runtime attacks and exploits.

Getting your house in order: minimising the insider threat

The dangers posed by external threat actors have become increasingly evident in recent years. Surging ransomware incidents have helped make cybersecurity a household topic.

BY DOMINIC TROTT, UK PRODUCT MANAGER, ORANGE CYBERDEFENSE

HOWEVER, while it is vital for businesses to protect their valuable assets from malevolent third-parties, mitigating the risk posed by company insiders can take a back seat as a result. Employees can make or break a business' security posture as no matter which or how many defences are put in place, they can often be subverted by a malicious link being opened or an insecure device being connected to the corporate network.

It's important to note that there are two different classes of insider risk. First, there are malicious insiders, employees who intend to inflict damage on their company from within for vindictive or exploitative reasons. However, there are also unwitting insiders, employees who may not know what good security behaviour looks like. These unwitting insiders undermine security controls unintentionally, but the end result can be equally damaging.

Businesses must take steps to defend against both malicious and unwitting insider threats. If adequate action is not taken to reduce the risk posed by insiders, they can be exploited by cybercriminals as they present a weak point in a business' defences, or can cause damage of their own making. Unfortunately, the issue is enormously challenging. As genuine users, insiders possess genuine credentials for accessing often private or sensitive information. There is also the challenge of protecting against any threat staff may pose without hindering their work by removing access or erecting additional digital barriers. However, there are some key steps that can be taken to combat insider threats.

Prevent and protect

It is vital that security teams invest in getting the basics right first, which includes being able to protect against security breaches, or even to prevent them from happening at all. Perimeter controls such as endpoint protection, network firewalls, web content filtering and email gateways represent a first layer of defence. These tools work by, for example, applying security policies to prevent insecure behaviour and/or by blocking 'known threats' for which security companies have already developed signatures. In this way, large amounts of security good practice can be automated, reducing the burden of expectation on genuine users – who generally are not security specialists – to understand and consciously exhibit good security hygiene behaviour.

Detect and respond

As a next step, organisations should adopt security approaches that detect unusual, unwanted, and outright malicious activity. Detection-based solutions often rely upon machine learning (ML) and artificial intelligence (AI) to analyse large data sets of security logs and feeds to detect activity classified as outside the baseline of 'normal' activity.

A key theme for detection and response solutions is automating resource-intensive elements of the workflow to provide skilled security analysts with additional time to conduct investigations or analyse how and why attacks are occurring to prevent them in the future. However, it is important to remember the response side of the equation, not just the detection part. Therefore, it is important that detection feeds into response in a timely manner
Detection is only step one. If malicious activity is discovered, security teams must have robust incident response processes in place to address any breaches or attacks that do occur. Rapid response is crucial to minimise any potential reputational, financial and legal damage that might otherwise be incurred.

Identity: security's post-perimeter front-line

While it's vital that security teams are prepared to react to malicious activity, the priority should be preventing it from occurring at all. Classic perimeter controls are geared towards this, but rising digital transformation means the concept of a corporate perimeter is increasingly porous. Attack surfaces are growing and diversifying thanks to, for example, the rollout of IoT devices and the convergence of IT and OT environments. Meanwhile, cloud migration and remote access means that ever more applications and data are hosted within (and accessed across) cloud infrastructure. Therefore, digital identity increasingly represents the first line of defence for the enterprise. Ensuring that only authorised users can access the network and the sensitive information it holds is key to stopping insider threats. Solutions such as Privileged Access Management (PAM) and Multi-Factor Authentication (MFA) are important tools for achieving these goals.

However, some of these approaches can cause friction for users, so solutions such as Single Sign-On (SSO) and Customer Identity Access Management (CIAM) need to be incorporated to reduce friction where possible. This is especially pertinent when adopting a Zero Trust approach. A Zero Trust architecture uses "never trust, always verify" as its guiding principle, requiring users to verify their credentials to access the corporate network, every time. While Zero Trust excels at blocking malicious activity at the endpoint and network levels – which is vital as staff continue to work remote – it requires users to re-authenticate whenever they connect to corporate assets.

Adapting to hybrid work

Two years into the pandemic, organisations across the globe have successfully adapted to hybrid working patterns. However, there is no avoiding the fact that hybrid work opens the door to malicious activity, with cybercriminals eyeing un-patched endpoints and staff letting their guard down in their home environments. Acknowledging that hybrid working increases exposure to risk, and responding accordingly, is crucial for business continuity and security. Much has been made of the use of VPNs to support remote working, but this is a basic technological response to what has become a permanent shift in working behaviour. Organisations need to move towards more transformational solutions, including Zero Trust and Secure Access Service Edge (SASE) approaches to secure access.

Training and awareness

While security teams may implement all the recommended tools, it only takes one insider to cause a breach. To minimise the threat and prevent an unwitting employee from causing damage, organisations must equip staff with the knowledge required to make the correct security decisions. By offering ongoing training and awareness building, security staff can empower employees to be an extension of their team, identifying and reporting threats such as phishing and the risk of human error.

Third-party data

Finally, it is not just employees that have the power to bring down a business from the inside. Third-party partners and other organisations that are privy to a business' valuable assets need to be taken into account. To do this, businesses need to prioritise data visibility across their entire partner ecosystem and manage the data lifecycle accordingly. Only by maintaining visibility of data throughout their organisation's entire ecosystem can security teams and the tools they've invested in block and detect malicious activity within even unstructured data.

While attention must be paid to mitigating the threat of malicious external actors, security teams can't afford to underestimate the human element of cybersecurity. The insider threat can be hugely damaging to a business so it must also be a priority for security teams. Whether that is through additional training or prioritising secure network access with approaches such as Zero Trust, it is possible to reduce the vulnerabilities posed by employees, both malicious and unwitting, with the right actions.

Building a better SASE

As businesses embrace digital transformation, there is more need to secure cloud-based resources. The rise of Secure Access Service Edge (SASE) promises a network architecture that combines VPN and SD-WAN capabilities with cloud-native security functions, such as secure web gateways, cloud access security brokers, firewalls, and zero-trust network access. Yet SASE deployments can be incredibly complex and make end-to-end visibility challenging for IT.

BY JOHN SMITH, FOUNDER, AND CTO AT LIVEACTION

Growing need

WHY SASE has quickly become an important technology and enjoyed a recent surge in demand requires an understanding of a chain of related factors. The starting point is the massive growth in cloud adoption, especially during the pandemic. Having fast, reliable access to cloud resources has become critical for employees, partners, and customers - with a particular focus on helping work from home (WFH) users access critical applications operating in a hybrid cloud.

Recent studies have shown that the remote workforce has more than quadrupled. Nearly 65% of enterprise employees are regularly working from home, compared to just 14% prior to the pandemic. This shift to remote work has transformed the requirements of the Wide Area Network (WAN) to deliver a more dynamic experience able to adapt to varied use cases – which in turn has driven more adoption of Software Defined WAN.

SD-WAN drivers

SD-WAN is a methodology and technology stack that completely changes how traffic is routed. A traditional direct connection or hub-and-spoke model likely has robust connections that are easy to track. But SD-WAN may use alternate paths, and if there are poor centralized policies, traffic could be routed through a branch office that was not meant to be a transit site or a host of other resource constrained processes such as encryption/decryption and content inspection. The result is a poor network experience for the remote worker. This can get even more complex if an organisation is cataloguing hundreds or thousands of sites – and mixing traditional WAN and SD-WAN – and tracking how they are communicating with each other.

SASE growth but still few deployments

With the context of more cloud demand and growth in SD-WAN, the need for SASE has never been more necessary. SASE is a relatively recent technology that integrates SD-WAN, secure remote access, and cloud-based security into a single solution. If done well, it can offer increased flexibility for cloud infrastructure, lower costs, reduced complexity, improved performance, and better protection for enterprise users, devices, and data. While many SD-WAN and security vendors have begun to offer SASE solutions, few have delivered a complete approach. According to a recent EMA WAN Transformation Report, 10% of organisations report they've completed a SASE deployment and 28% claim partial implementation. Given that there are so few complete solutions available, EMA believes overmarketing by SD-WAN vendors is actually inflating these numbers.

At any rate, SASE offers incredible benefits for enterprises and the future is bright for this innovative technology category. In fact, the increased need for remote user support during the pandemic has spurred much of the sudden acceleration around SASE deployments. EMA's report showed that a massive 51% of respondents have accelerated their SASE projects over the last year alone. In addition, Gartner predicts that by 2024, at least 40% of enterprises will have strategies in place to adopt SASE, up from less than 1% at the end of 2018.

Understanding SASE

There are many vital elements to consider when adopting a SASE strategy, but let's explore a couple of key criteria outside of the obvious cyber security requirements. The first is integrated operational visibility. It's important to have network and security visibility across all the ways users access applications and resources throughout the enterprise. This means remote, public cloud and traditional network environments, and everywhere in between. Respondents ranked this attribute as the most important in EMA's WAN Transformation Report. Next, we have secure remote access. This has become an increasingly urgent priority during the COVID-19 crisis, and a primary element in supporting business continuity for the modern enterprise. Whether accessing cloud applications for work, such as Salesforce or Office365, or accessing proprietary applications such as call center systems, having secure access for WFH employees has become essential alongside the need for robust security controls.

Visibility and SASE

SASE deployments can be incredibly complex and make end-to-end visibility challenging for IT. There are many components at work, and if something goes wrong, isolating it down to a single source or domain can be tough. Is it the local network, SD-WAN device, cloud presence, security device, etc.? Is it a problem with network traffic, applications, and users? Today, enterprises are using analytics platforms that work alongside SASE to provide a vendor-neutral view into deployments with the ability to analyse telemetry for network, security, and compliance purposes. These solutions also offer end-to-end views once the traffic exits SASE into the branch, data center, colocation, or public and private cloud.

> SASE offers incredible benefits for enterprises and the future is bright for this innovative technology category. In fact, the increased need for remote user support during the pandemic has spurred much of the sudden acceleration around SASE deployments

Granular visibility allows IT to better understand network and application traffic and verify that policies and their intent are working as designed. It also enables troubleshooting and the remediation of network and/or security issues. So as issues arise, IT can identify the root cause and understand the most appropriate remedial action to take. Finally, establishing comprehensive, end-to-end network visibility allows IT to understand how application traffic and data flow through the SASE system.

SASE starting point

Due to the fact that SASE solutions are the product of multiple integrated technology categories, we're seeing many network security, cloud-based security, and SD-WAN vendors entering the space. You often hear grand promises and phrases like "silver bullet" and "single solution." In reality, you'll need to work with at least two solutions, and sometimes more, to deploy SASE today.

Deciding how to build your SASE is the single biggest challenge and when selecting, consider the following questions:

- **Is the technology mature?** Are the network or security features fully baked? Is it completely integrated, or separate, or does it allow integration with other solutions?
- **What is the management setup?** Is all of the functionality easily managed through a centralized cloud-based service? If so, how is this done? This can be important for reducing the complexity and management of a SASE solution.
- **Do the cloud integration capabilities suffice? –** Does it easily provide access to the public cloud and offer private cloud connectivity through colocation and remote sites? This is important as more applications live in a hybrid cloud model.
- **Is there scalable, secure remote access?** Does it include a scaled approach to remote user access with respect to points of presence that allow for better performance from various locations mapping to customer needs?

Security Policies

The heart of SASE is the ability to implement new security policies across the SD-WAN and connected devices that are more unified than the legacy network it replaces. For instance, SD-WANs allow encryption as traffic moves from one site to another and network segmentation for layered protection. Thus, everything from employee and guest access to creating DMZs to internet access to architecting site-to-site connectivity may need review. Moreover, it will be important to ensure that you're capturing audit data and performing policy validations to ensure the network is operating as intended from a security and performance perspective. Understanding the key obstacles and having the proper tools to help circumvent those challenges is vital to success.

Financial Markets Network

Global Connectivity Throughout the Trade Lifecycle

Worldwide Data Connectivity

Cloud Computing

Infrastructure

www.ipc.com

BCAS: What is it and why do you need it?

Given the growing threat, volume and complexity of cyberattacks globally, Business Critical Application Security (BCAS) should now be a priority for businesses seeking to bolster their cybersecurity.

BY TIM WALLEN, REGIONAL DIRECTOR UK&I AT LOGPOINT

BUSINESS CRITICAL APPLICATIONS are the backbone of departments, acting as digital hubs of business-critical assets, data, information and productivity. From enterprise resource planning (ERP), to supply chain management (SCM) and customer relationship management (CRM) software to human capital management (HCM), product lifecycle management (PLM), business critical applications (BCA) offer comprehensive support to almost every facet of the organisation. Such platforms reduce operational costs and administrative complexity, streamline data collection and management processes, and provide flexible scalability.

Their importance, however, is not reflected in the protection being afforded to them. A recent poll surveying IT and cybersecurity professionals across the US and UK revealed insecure and unmonitored business-critical systems, with four in ten noting that they do not include business-critical systems in their cybersecurity monitoring. Additionally, 27 per cent were unsure if it was included in their cybersecurity monitoring at all. Given the dependency upon BCA, this is a problem.

A major problem with BCAs is that they are often long established and cater to the needs of specific departments ie finance, HR, logistics so therefore become siloed and are not integrated into central security strategies. Consequently, BCAs are often not monitored by security teams, making it difficult to patch and maintain them, let alone spot emerging threats. But not including them in centralised security monitoring leaves the organisatios vulnerable and exposed to cyber threats. It's a problem further exacerbated by BCA moving to the cloud, with almost three quarters of businesses admitting they lack visibility within the cloud environment leading to challenges over managing configuration.

The risks associated with BCAs

Perhaps unsurprisingly, malicious actors are now increasingly targeting these data-rich, critical applications. The same reason why BCAs have become indispensable to specific departments is why they represent highly lucrative targets for cyber attackers.

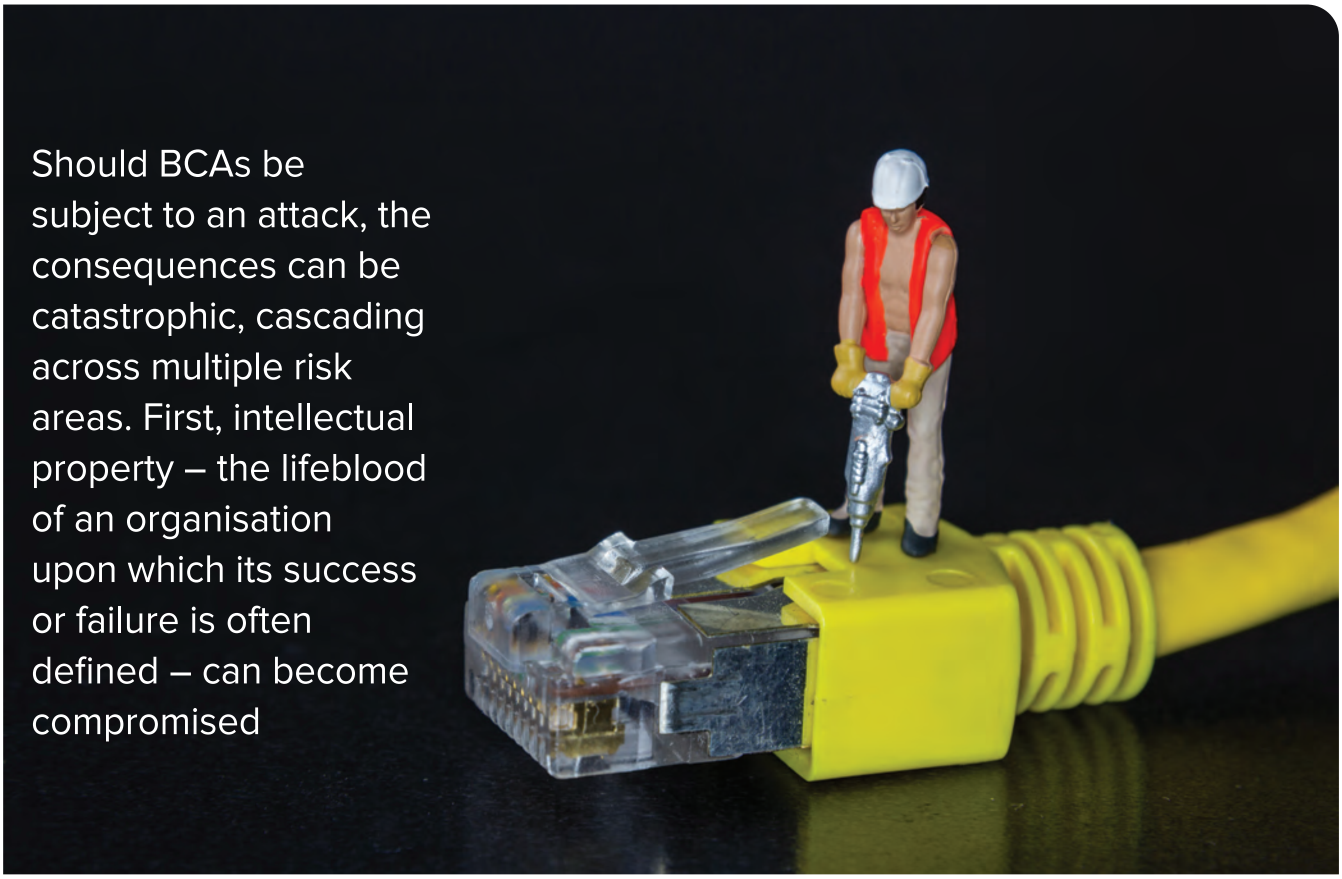
Should BCAs be subject to an attack, the consequences can be catastrophic, cascading across multiple risk areas. First, intellectual property – the lifeblood of an organisation upon which its success or failure is often defined – can become compromised. Trade secrets, financial data and customer data can in turn end up in the public domain, while firms may also face potential penalties stemming from the loss of customer and financial data. And that's before we mention the impact of reputational damages or disrupted innovation cycles.

Companies which fail to handle data correctly can also face significant penalties. In the case of GDPR, organisations may be fined up to 4% of their annual turnover for a lack of compliance. Further, if third-party data (be it from business partners, suppliers or subcontractors) is compromised, the Copyright Act expressly provides cause for claims for imposed damages, which can be substantial. With BCAs, there is also an operational risk to consider. Providers of such applications will often audit systems, requesting information on settings, data integrity and processes to determine if key regulations are being adhered to. A failed audit can lead to a shutdown in systems, requiring the use of expensive resources to remediate. Equally, it may also result in personal liability against leadership teams and even heighten the potential for fraud.

Security is typically separated

Given these risks, effective operational and security practices are both vital. In terms of the latter, many firms opt to secure BCAs with separate security solutions, further adding complexity with more external solutions, software and applications. Yet this is far from an optimal approach.

SIEM and BCAs operate in separate worlds. SIEM grew out of IT network technology, designed to monitor events in the interconnected IT network layer, collecting logs and event data on everything from origin/destination IP addresses, user IDs and device IDs to normal/abnormal traffic patterns and other network-layer information. It employs IT rule sets and controls to analyse network activity and report back to security analysts. As such, SIEM focuses on the security of network infrastructure, not on specific applications.



Should BCAs be subject to an attack, the consequences can be catastrophic, cascading across multiple risk areas. First, intellectual property – the lifeblood of an organisation upon which its success or failure is often defined – can become compromised

Take SAP, for example – one of the most common BCAs (or more precisely, a suite of software applications). SAP systems comprise something of an independent network with its own unique rules. A single SAP application, such as NetWeaver, uses multiple logs to capture security-relevant events. However, these logs use varied formats and structures, not just between different SAP applications but within these single applications themselves. Further, the company has its own specific vocabulary to describe IT network equipment.

This lack of standardisation or conformity with the wider security market makes it very difficult for SAP to be part of the central security strategy. While SAP had developed its own SIEM, this only siloes the security approach, preventing the ability to monitor attack patterns enterprise wide.

The statistics speak volumes. As part of the Logpoint poll, respondents were asked how they currently review SAP logs for cybersecurity events or cyberthreat activity. Almost 30 per cent admitted to not reviewing SAP logs in any way, and again, nearly 30 per cent said they didn't know if this was being monitored. Meanwhile, only 23 per cent said the process of reviewing SAP logs for cybersecurity events or cyberthreat activity was automated through SIEM, with almost 19 per cent still doing so manually.

Developing a BCAS strategy for transformed visibility

To unlock the benefits of BCAs while also mitigating the potential security risks, firms must adopt a comprehensive business critical application security (BCAS) strategy.

Effective BCAS will establish best practices that ensure these critical software applications are monitored thoroughly and centrally, aligning people, processes and technologies to increase visibility of activities. Only with complete transparency can the business monitor and secure its data irrespective of which systems it resides in, necessitating the integration of BCAs into the wider cybersecurity strategy.

When this divide is broken down, BCAs are empowered to benefit from an arsenal of security solutions including SIEM, SOAR and UEBA, helping to unlock transformative threat insights.

These technologies provide automated threat detection, investigation and response capabilities as well as accurate, risk-based analytics, guiding security teams in combating advanced threats and empowering them to protect themselves properly. So, just how easy is it to implement an effective BCAS strategy? Where can you begin?

Fortunately, there are solutions on the market that undertake much of the heavy lifting, effectively bridging the gap with limited effort. Some have been specifically designed to successfully solve the challenge of SIEM-SAP separation, for example, by efficiently and effectively integrating SAP data into any SIEM system.

Data from the SAP system(s) is first normalised, and then stored in the SIEM system, providing real-time analysis of internal SAP activity as well as allowing firms to correlate SAP data with the other events in the IT network.

Indeed, this benefits both parties, improving threat visibility and insights by monitoring all elements in the network. Through continuous, automatic and transparent auditing of BCAs, firms become empowered to yield greater value from the SIEM systems and enhance their security posture.

Given the growing threat, volume and complexity of cyberattacks globally, Business Critical Application Security (BCAS) should now be a priority for businesses seeking to bolster their cybersecurity. The merits of breaking down the technological siloes between operating departments and security setups are no less than transformative.

StorPool
DISTRIBUTED STORAGE

www.storpool.com/msp-storage

StorPool Storage - Agile Storage Platform for Managed Services Providers

The ideal foundation for cloud infrastructure serving the primary workloads of SMBs and Enterprises.

- Build powerful and robust clouds for your users.
- Retain control over your cloud infrastructure and ease the load on your people.
- Simplify your cloud Infrastructure and streamline your IT operations.

Your Data Storage Partner

Architect

We help you select the ideal architecture for your cloud at the physical, network, and logical levels, using only standard hardware.

Deploy

We install StorPool Storage in your servers and connect your storage system to one or more Cloud Management Platforms.

Fine-Tune

We analyse and tune your StorPool Storage system so that it runs optimally and reliably for your customers' workloads.

Monitor

We monitor hundreds of metrics per second to proactively open support tickets and deal with any issues that arise.

Maintain

We ensure that your storage system always runs optimally by installing non-disruptive updates and adding servers when needed.

StorPool Storage helps you get your data in order. It enables you to deploy and grow reliable, agile, speedy, and cost-effective clouds that meet the needs of your users. Bring your data home using the technologies you need, and pay as you grow – with no fixed term commitments.

Elevate Your Cloud by Building a Reliable and Speedy Storage Foundation!

Get Started

www.storpool.com/msp-storage | ☎ +44 (0) 20 7097 8536 | ✉ info@storpool.com

Why are so many companies in the cloud falling foul of security breaches?

You've been told time and again cloud is secure. And it is, but only if you treat it appropriately. Too many companies move their workloads to the cloud and think all the work is done. They often forget that their usual security measures don't work in the cloud. The reality is that your cloud estate needs appropriate cloud security in place, then it needs constant monitoring and analysis to ensure it stays secure.

BY JAMES HUNNYBOURNE, CLOUD SOLUTIONS DIRECTOR, ULTIMA

WE'VE ALL HEARD OF the infamous breaches that Yahoo, Alibaba, LinkedIn, Sino Weibo and Facebook have experienced in the past few years. But you›d be wrong to think it›s just the big boys under attack.

The 2021 Thales Global Cloud Security Study reported that 40% of organisations had experienced a cloud-based data breach in the past 12 months. Despite these incidents, the vast majority (83%) of businesses still fail to encrypt half of the sensitive data they store in the cloud. And in a recent study, Sysdig found 75% of companies running containers (in the cloud) have high or critical vulnerabilities which can be fixed with patches but aren›t.

I'm not surprised by any of this, nor are my cyber security colleagues, but if companies – even small ones – don't sit up and listen, there is a 50/50 chance they will be next. If your cloud estate isn't configured correctly, constantly monitored, and updated, it will likely leave your business open to attack.

So, how can you ensure your cloud estate is secure? Here are my top five tips.

1. Build a secure cloud infrastructure

If your IT infrastructure isn't built and configured correctly, you leave yourself open to attack. But building a secure cloud infrastructure goes beyond the traditional IT infrastructure where it was all about a corporate network accessed in the office. Remote working and cloud technology mean every part of the network needs to be secure and protected – from the infrastructure, network, apps and data to endpoints.

Everyone will be using your cloud services, so when building out your cloud infrastructure, it's key to involve all departments and understand how they will use the cloud and what impact this is likely to have on security. IT teams are used to managing and updating their on-premise IT infrastructure with anti-virus software and implementing the latest patches, but cloud security is different, and IT departments need to recognise this. How staff access the network and use their apps are key considerations when ensuring your infrastructure is secure.

I would recommend any company operating in the cloud or moving to it does an audit and assessment against industry best practice benchmarks to assess their cloud vulnerabilities. And working with a cloud consultant who understands all the possible security risks is a good way of informing this process.

2. Update security to make it cloud appropriate

A typical scenario is for a business to keep existing security solutions when they move to the cloud, layering it over the top as best as possible. This gives some form of protection, but visibility over the whole environment is reduced because the cloud works in a very different way to on-premise. For example, traditionally, the in-house IT team would do a true-up of that environment once a month or quarter. This works fine in an on-premise service, but when you are in the cloud scaling up and down quickly, you can end up creating a void if the true-ups only occur infrequently.

Having the right security that manages and monitors your entire cloud estate 24/7 is the only way to help prevent security breaches. There are now software solutions like MDR (Managed Endpoint Detection & Response) that continually monitor your endpoint devices beyond the scope of anti-virus software. It will continuously monitor for anomalies or suspicious activity across your cloud estate. If an incident is detected, it can act upon it for you 24/7, down to machine isolation or automated playbooks.

3. Test, monitor and analyse the estate continually

Things will slip through the net if you aren't testing, monitoring, and analysing your cloud estate 24/7. It's worth employing consultants to assess and test your cloud estate to help provide actionable insights to improve your security. This will allow you to align with industry best practices and help you understand your vulnerabilities, and potentially reduce your operating expenditure.

For example, one services company that did this found they could reduce costs by moving from four to two operational regions, orphaning services not in use, and downgrading their storage disks without loss of service quality. Their assessment has saved them £18,000 per year, representing a 30% saving against their annual cloud consumption. But most importantly, the review highlighted their VPN was in a 'failed' state, and their WordPress websites were not secure, so both needed immediate updating to prevent vulnerability to attack. The assessment led the business to implement more robust security policies and align better with ISO27001.

Once your estate has been assessed and tested for vulnerabilities and any immediate remedial action taken, it's then a case of monitoring and analysing activity 24/7. There are some excellent cloud management platforms that will do that for a business and don't cost the earth.

> Once your estate has been assessed and tested for vulnerabilities and any immediate remedial action taken, it's then a case of monitoring and analysing activity 24/7. There are some excellent cloud management platforms that will do that for a business and don't cost the earth

These automated security and monitoring solutions are automatically applied to existing and new workloads. They scan the collected data and include proactive monitoring around security events to let you know what's happened in clear-to-understand alerts and where action should be taken if needed, covering critical areas such as anti-malware.

4. Educate users

While you may have the best cloud infrastructure in place and all the right security and monitoring tools in place, with poorly educated users, that is irrelevant. Human error is still the leading cause of cyber security failures. Recently, researchers from Stanford University found that employee mistakes cause approximately 88 per cent of all data breaches.

It's critical to have the right security policies in place – for remote access, mobile phone and BYOD, password use, and data transfer and disposal. Then you must continually educate, educate and re-educate all employees from the CEO down.

Everyone needs to understand and buy into the concept that cyber security for your business is about shared responsibility – not just of the IT department or HR, but of all departments and all staff.

5. Have a disaster recovery plan in place

You’ve got the best infrastructure and monitoring and analysis tools, and your employees are regularly trained. But that still isn’t enough to guarantee 100% safety from cyber security breaches. It’s just not possible. To ensure your business can still operate at a time of breach or attack, you need to have proper disaster recovery (DR) plans in place and test them regularly. A remote date backup system is a must for all organisations. 80% of businesses affected by a major incident either never re-open or close within 18 months, partly because they don’t have an effective DR plan in place.

And yet, 41% of businesses haven’t tested their DR solution in the last six months or don’t know if it has ever been tested. But there are now autonomous DR solutions on the market that include security protection and non-disruptive testing of virtual machines. As this is built in the cloud, costs are significantly reduced compared to on-premises DR solutions as you pay for the services you use. If you haven’t got a good plan in place and it’s not tested regularly, make it an action today to find a company that can help you change this.

It’s hard for small and medium-sized enterprises to keep up to speed with all the latest regulatory requirements and potential vulnerabilities in their cloud estates and focus on cost optimisation.

Working with a good cloud and security managed service provider will give you access to deep expertise to improve your cloud estate management, optimise your cloud costs, and ‘test’ how secure your estate is. Please don’t leave it too late, though, or you might become a statistic yourself.

Jacky
VP Power Solutions
EMEA / France
Kathy
Sr. Operations Manager
China
Jitendra
DGM Sales
India
Meet your
GLOBAL POWER PARTNER
Generators, power solutions and 24/7 support.
Dedicated to data centers.
Kohler-sdmo.com/EN/application-data-centers
KOHLER®
IN POWER. SINCE 1920.

Remote work has disrupted office work but it has disrupted enterprise security too

Mass Remote work is here and it's not going anywhere. While that might have seemed unthinkable only a few years ago - it looks as though what was a fringe benefit for some is becoming a daily reality for many.

BY RICHARD MELICK, DIRECTOR, PRODUCT MARKETING FOR ENDPOINT SECURITY AT ZIMPERIUM

How we all became remote workers

When the world locked down, workforces were sent home and ordered to stay there until further notice. During these trying times, many businesses were forced to shutter, being unable to sustain themselves under the strictures of the pandemic. Those that did manage to successfully enable and secure mass remote work capacity for their tens, hundreds, and sometimes thousands of employees.

This went along with a whole series of digital transformations that fundamentally changed businesses worldwide. As CEO of Microsoft Satya Nadella said early in the pandemic, “We've seen two years' worth of digital transformation in two months.”

In this herculean effort of mass-bootstrapping, enterprises started rapidly moving to the cloud, implementing BYOD schemes, and trucked in Virtual Private Networks (VPN) to help secure connections between workplaces and their quarantined workforces.

Now, as the pandemic recedes - remote work is solidifying itself as a fixture of modern business. Still, these rushed short-term measures are ultimately insufficient to protect remote work in the long term. The explosion of mass remote work has meant that workers are now accessing corporate data outside of the traditionally office-bound network perimeter. As a result, they're working without the benefit of enterprise-grade security controls which could otherwise protect them.

It's of no particular surprise that in our 2022 Global Mobile Threat Report, nearly 50 percent of security professionals said that their work from the home strategy was a significant part of their cybersecurity incidents. Instead, they're using home endpoints, networks, and personal mobile devices. This, in turn, can lead to exposure and potential theft of data by malicious actors as they penetrate the often pitiful protections that non-enterprise networks and endpoints maintain.

While remote work might be a stubborn reality, secure remote work seems harder to achieve. We also found that 61 percent of security professionals believe that applying corporate cybersecurity policies in the age of mass remote work is nearly impossible. Mobile devices are central to remote work
Remote work has thrust mobile devices right into the centre of modern working. They capture the flexibility and geographic neutrality that many now expect of their jobs. Now, it's quite normal to answer emails, attend meetings and collaborate on documents via a mobile device.

Now that so many of us are remote workers, those mobile endpoints are becoming more and more critical to our everyday jobs. As a result, the line between personal security and enterprise security is blurring. Personal devices can become corporate espionage devices, and remote workers can become insider threats without them ever knowing about it.

Cybercriminals are seizing the opportunity. In 2021, Zero Day exploits against mobile endpoints skyrocketed by 466 percent year over year. Over the same time period, mobile-specific phishing websites grew by 50 percent.
However, many of the attempts to enable mobile computing in a remote work setting don't get to the heart of the problem and in some cases, actually, introduce risks.

Productivity apps

One of the ways in which companies enable remote work is through productivity apps. These are the applications - like Slack or Monday.com - that allow workers to collaborate, communicate and remain productive, whatever the geographical distance between them.

Our survey showed that 56% of technology leaders use between four and eight enterprise applications on their mobile devices. A further 17% use over eight. Cybercriminals know that and these kinds of applications have become a key attack vector for mobile threats. Office 365 is just such an example. The app is the cornerstone of many workplaces, hosting a whole suite of Microsoft applications including Word, Excel, and Teams. In fact, a recent Zimperium poll found that 84% of security professionals had enabled it on their phones. It also appears to be a cornerstone for cybercriminals too. One report says that this software suite alone accounts for more than 72% of exploits, compared to browsers which account for just 13%. It's the very popularity of this particular application that makes it such a popular target for mobile threats too - the broader the attack surface, the more chances to infiltrate the target.

Securing mobile devices

Along with the introduction of various productivity tools, companies have also tried to secure remote work with a range of measures.

VPNs have become a critically important part of remote work, allowing secure connections between mobile devices and their workplaces. BYOD uptake has been healthy and it appears as though the pandemic has forced many enterprises to get serious about personal mobile devices. This is especially important, considering that most mobile devices - 66% according to our survey - used in an enterprise setting are personal devices. Others are using Mobile Device Management to give them some form of control over the mobile devices that make up so much of their attack surface and have encouraged their workforces to start using MFA on their devices.

The truth is that BYOD schemes, MFA, or VPNs are useful but ultimately insufficient to protect against mobile threats and fall short when it comes to phishing, network vulnerabilities, mobile application vulnerabilities, or zero-day threats.

Protecting the mobile endpoint

On an office computer, you might have been able to turn it off and walk away when the day ends but mobile devices are ever-present parts of our work and private lives. The problem with many of these attempts to secure and uphold remote work is that they don't account for the fact that the mere presence of personal mobile devices in enterprise work, takes visibility and control out of security teams' hands.

To protect against the mobile threats to remote work, security needs to go where the work is actually being done: Mobile devices. With that in mind, organisations must build on their new security measures by introducing Mobile Threat Defence (MTD) capabilities which can assess device security posture continuously, detect threats as they arise, and block access when they do.

Furthermore, any attempt to secure remote mobile endpoints must be always-on and on-device. It can't call back to the cloud and must continually protect the device even when it's not connected to the internet. Remote work is a reality. Whether or not that's good for security is beyond the question. Security teams need to adapt to and protect this new reality, wherever it lies.

An introduction to virtual production

Virtual production is revolutionising the way film and video content are being created, providing far more scope for innovation, rapid development, reduced costs and a sustainability benefit. Nor is virtual production just for movies, advertising and AV pros: it opens the door for more organisations to explore the visual arts to engage with employees and external audiences.

BY KATIE COLE, GAMING & VIRTUAL PRODUCTION EVANGELIST,
PERFORCE SOFTWARE

ACCELERATED BY THE PANDEMIC, virtual production is fast becoming mainstream. It is expected to be a huge growth market in the coming years, with multiple studios and vendors already on board. According to research from Technavio published in April 2022, the virtual production market share is expected to grow by USD 1.85 billion from 2021 to 2026, and the market›s growth is anticipated to accelerate at a CAGR of 16.85%.

Virtual production has been around for a few years, with probably the most famous milestone being the release of the Mandalorian in late 2019. In addition to wowing viewers, that film also made a massive impression on film and video professionals who realised that by combining software with on and off-set components, the only limitation now was the imagination.

Then came along the pandemic, and to carry on making films, TV ads, and other video content, more studios turned their attention to virtual production. One of the earliest pioneers was Final Pixel, a global creative studio founded in 2020 by film & TV industry veteran Michael McKenna, his brother Christopher, and executive producer Monica Hinden. Today, the studio has an impressive virtual production track record, including projects for Shutterstock and Dancing With The Stars.

On its website, Final Pixel states “We believe that we are on the verge of a technological shift of greater magnitude than the move from celluloid film to digital cinema. The advantages to virtual production are so numerous it is inevitable that a significant amount of film and television production will soon become virtual.”

Big benefits

The benefits of virtual production are powerful. Barriers to creativity are removed (as Final Pixel says on its website, ‘If you can think it, you can build it’.)

Also, as the crew can see in-camera VFX, post-production time is saved, and it becomes easier to iterate, with revisions made earlier in the process while actors are still on set. This leads to less rework and reduced post-production effort. And in post-production, since virtual production supports remote contributors, team members and vendors from literally anywhere in the world can access assets to work on.

Multiple ‘locations’ can be covered in one day (simply swap out the background), and what the film industry calls ‘the golden hour’ is no longer dependent on whether or not there is natural light. The turnaround between virtual locations can be fast, with less travel and expensive physical sets required. Furthermore, compared to physical sets, virtual set components can be reused time and again.

Plus, virtual content can now be created by decentralised teams around the globe without delays. Filmmakers can build up their teams with creatives and technical specialists anywhere they are located. The possibilities widen without increasing the cost.

Virtual production seems a natural for film and advertising studios, but it also opens up the potential for businesses to be more creative with AV. For example, create more engaging training material for employees, communicate content to customers in a visually compelling way, and even launch a new product range.

Virtual production components

Virtual production has multiple elements, but the main three are camera tracking, an LED wall, and a game engine, which runs on a high-specification PC to render and animate a 3D model in real-time. Games engines have become the bedrock of virtual production because the game industry’s use of high-quality 3D rendering was ahead of anything else. Unreal and Unity seem to be the most popular for virtual production so far.

The environment is played from the game engine software and displayed on the LED wall. Each camera’s position is tracked in 3D, changing the perspective in the video game environment displayed on the LED wall as it moves. When done well, the net effect is that the viewer’s perspective changes and everything is related, creating a realistic effect.

Data-dependent

Virtual production depends on talented people, great ideas, high-quality cameras and LED walls, and choosing the right game engine. However, given its digital nature, virtual production is also very dependent on managing data assets, of which there could be a vast volume dispersed across multiple locations. Having simplified and universal visibility and control over all these assets is vital. This is why several techniques and tools well-established in the enterprise IT world are now being used in virtual production.

For example, adopting a hybrid or cloud model will make it easier for teams to quickly access virtual production assets they need without the wide-area network (WAN) wait that can easily create delays. Cloud provides file access, but virtual production teams also need data management tools: putting files into Dropbox is not sustainable in this environment. Data asset management tools (such as Helix DAM by Perforce) secure assets and assist with collaboration.

In addition, version control is used to make it easier for teams to catalogue assets and track their evolution, regardless of where people are located or what tools they use (such as Photoshop, Maya, and 3DS Max to build visual assets).

For Final Pixel, version control can also dramatically speed up real-time changes to game engine files. For instance, the team can be on-set, and the director says they need an object in the background to be moved. An off-set artist can make the change to the file, sync the file change to Helix Core by Perforce (the version control system), and then render it on the LED wall within minutes. Final Pixel’s team of remote contributors can work with the on-set team, making it feel like everyone is in the same room. With the changes loaded, they can keep on filming.

Another helpful category of tools is project management, which can be used to keep the objectives on course and people on task. Global artists, supervisors, producers and engineers can be united to help track, manage, discuss and review visuals in real-time.

While virtual production has many benefits, there is also much to take on board, representing a learning curve for teams. Fortunately, there is an increasing number of knowledge resources, including Perforce U College of Virtual Production, a free online resource of training content. Again, there may be a lot to learn, but given the potential benefits, especially the creativity that can be unleashed.

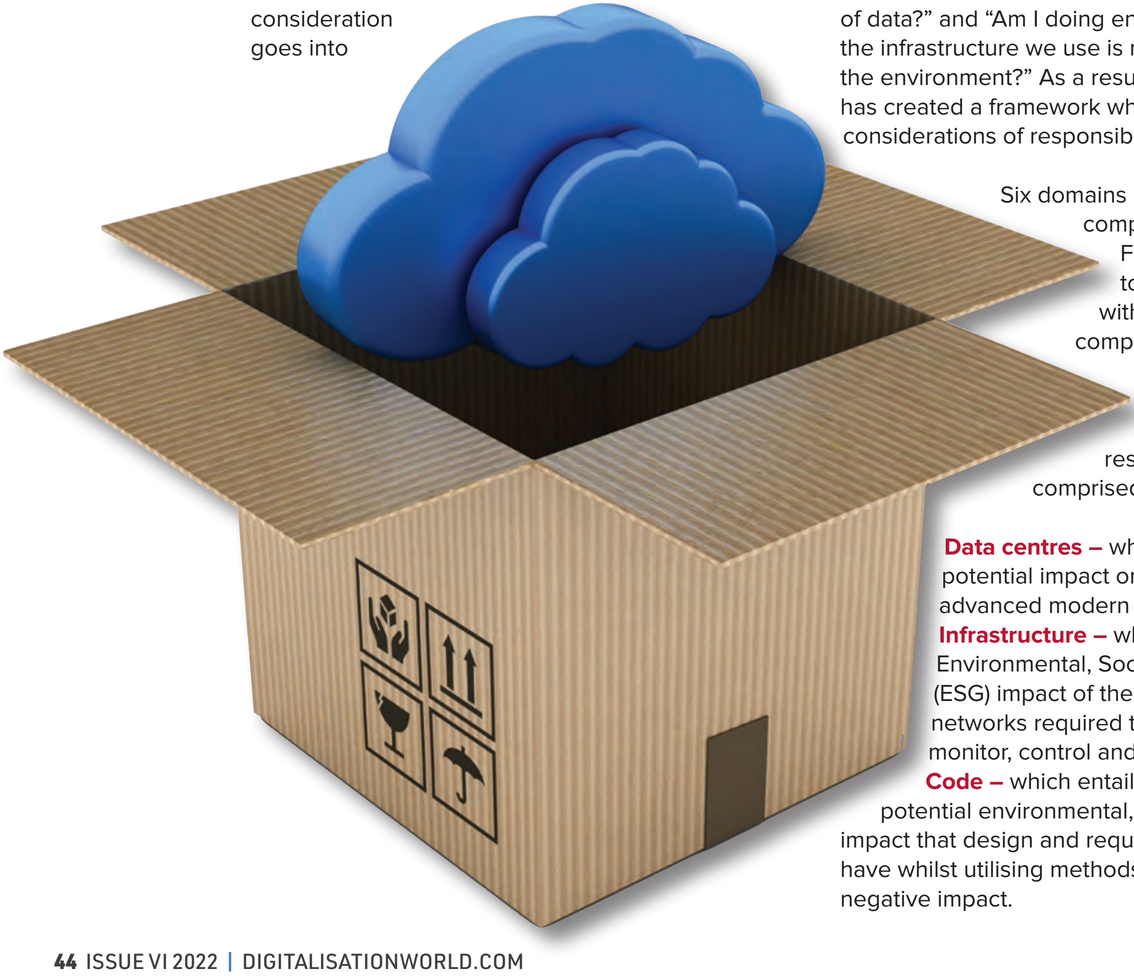
> virtual content can now be created by decentralised teams around the globe without delays. Filmmakers can build up their teams with creatives and technical specialists anywhere they are located. The possibilities widen without increasing the cost.

Responsible computing isn't just about moving to the cloud

How much real consideration goes into calculating and demonstrating responsible computing in business today?

BY NICK WESTALL CTO, CSI

IT DEPARTMENTS are being asked by their boards to demonstrate improved sustainability. Often, they attribute their move to the cloud as a way of showing commitment to the reduction of their carbon footprint and the green agenda. While it's a good example of carbon offset, is it just a way to pass the buck to the cloud provider rather than look in more depth about being a responsible user of IT? How much real consideration goes into calculating and demonstrating responsible computing in business today?



In 2020 the IBM Academy of Technology (AoT) brought together experts in many fields to discuss responsible computing. They analysed the anxieties of over 100 CTOs and looked at all aspects of IT to answer questions such as, "Am I doing enough to be sustainable?", "Are we being ethical in our use of data?" and "Am I doing enough to ensure that the infrastructure we use is minimising its impact on the environment?" As a result, the IBM AoT initiative has created a framework which outlines important considerations of responsible computing.

Six domains of responsible computing

From the more obvious topics associated with running your computing infrastructure to its wider impacts, the AoT framework summarised that responsible computing comprised of six main domains:

Data centres – which looks at the potential impact on the environment of an advanced modern data centre.
Infrastructure – which considers the Environmental, Social and Governance (ESG) impact of the hardware, software and networks required to develop, test, deliver, monitor, control and support IT services.
Code – which entails being aware of the potential environmental, societal and economic impact that design and requirements choices could have whilst utilising methods to minimise their negative impact.

Data Usage – which involves the duty to deal with and have control over data and its lifecycle as well as being accountable of its mindful, effective and efficient usage.

Systems – which summarises the need for developing systems that everyone, including the company itself, can trust. A "system" is an integrated set of technologies that provide a service to human beings. It can be composed of hardware, data, code, models and services.

Impact – which encompasses the use of technology to change the world for a better future.

Being a responsible CTO

The reasons for needing to be a responsible CTO are just as strong as the need to be a tech-savvy one if a company wants to thrive in a digital economy. There are many facets to being a responsible CTO, such as making sure that code is being written in a diverse way and that citizen data is being used appropriately.

In a BCS webinar, IBM Fellow and Vice President for Technology in EMEA, Rashik Parmar, summarised that the three biggest forces driving unprecedented change today included post-pandemic work, digitalisation and the climate emergency.

With many organisations turning to technology to help solve some of the biggest challenges they're facing today, it's clear that there will need to be answers about how this tech-heavy economy will impact the environment. It makes sense that this is often the first place that a CTO will start when deciding how to drive a more responsible future.

Responsible computing is much more than a move to the cloud

When you consider that each of the six domains above will make a huge difference to how responsible an organisation is deemed, it's easy to see why it's about much more than a move to the cloud.

If we focus on the environmental considerations, it's becoming more commonly known that whilst a move to the cloud may be better for reducing an organisation's carbon emissions than running multiple on-premises systems, the initiative alone isn't going to spell good news for climate change.

In fact, if everyone were to move to the cloud in droves the internet would need to quickly find a way of being more sustainable.

A large part of this is the requirement for major cloud providers to switch most of their data centres to more renewable energy sources. This is an area that falls outside of a customer's control. But in fact, the issue of reducing emissions can be influenced far more greatly by the activities undertaken by the organisations themselves. It can all come down to understanding how their workloads are running and whether it is driving high levels of utilisation.

Making more efficient use of the computational resources available

When it comes to running at high levels of utilisation, the answer isn't necessarily all cloud driven. For example, the performance and scale of the new IBM Power server, the E1080, delivers the benefits of consolidation at levels far higher than is possible with x86-based alternatives.

When compared with the cloud hyperscalers, such as Azure and AWS, it offers a greater ability to scale. In a recent webinar, David Spurway, IBM Systems Technology Architect, modelled IBM's Power10 against Azure and AWS, looking at the largest of their offerings which could then be filled up with workloads such as multiple containers*.

*In the model, David used the conservative performance metric of the IDC QPI, which gives relative performance across architectures but does not consider advantages for specific workloads. For example, the new Power10 cores can hold over four times more containers per core than x86, so the real values may be even higher.

> If we focus on the environmental considerations, it's becoming more commonly known that whilst a move to the cloud may be better for reducing an organisation's carbon emissions than running multiple on-premises systems, the initiative alone isn't going to spell good news for climate change

This is how the performance of the virtual servers, bare metal server, and physical IBM Power servers look when considering their maximum capacity:

When dividing the server performance rating by the number of cores, David then demonstrates a rough estimate of performance per core:

This demonstrates that by doing much more per core, fewer cores are needed, which leads to less energy needed.

Whilst Virtual Servers in the Cloud can run at high levels of utilisation – near the 90% mark - the average utilisation is much lower. This is because the number of workloads that smaller servers can hold is lower, and that means more servers are

needed. With IBM's large E1080 server, average and peak utilisations demonstrate a more efficient use of the computational resources available. When utilisation is combined with scale and performance it provides a very powerful and efficient option.

Can cost savings be a by-product of energy efficiency?

If an organisation is on a software licencing model that adjusts depending on the level of utilisation and usage, it is also possible to achieve significant cost savings. The ability to turn applications on and off when not in use will reduce the number of processors needed. If the organisation is charged by the processor core this could be as much as five times less expensive because of the software savings when running fewer cores.

> While it's true that cloud infrastructure does deliver carbon savings, organisations should also think about the environmental and cost saving benefits in other on-premises measures

Environmental considerations that organisations should make

There are detailed methodologies available that help organisations establish where they are today in terms of responsible computing. As sustainability is such a relatively new factor, it's important for an organisation to understand where it is so that it can measure what improvements are being made in the form of Key Performance Indicators.

The three main considerations can be summarised as:

Are you using latest infrastructure components?
This has a real impact because as technology advances, newer components deliver better performance and require less energy for a given workload.

Are you consolidating workloads?
Consolidation allows workloads which peak at different times to complement each other and make more efficient use of resources.

Are you running at high utilisation?
High levels of utilisation (which can be improved by consolidation) delivers more efficient use of energy and resources.

The responsible computing deliverables include methodologies for all six domains to help companies understand where they are today and demonstrate how they are improving and delivering against their KPIs. While it's true that cloud infrastructure does deliver carbon savings, organisations should also think about the environmental and cost saving benefits in other on-premises measures.

EXAGRID®

Tiered Backup Storage

The Future of Backup Storage:

Tiered Backup Storage

Scales to 2.7PB without forklift upgrades or performance degrades with ExaGrid scale-out architecture.

3X
faster backups than dedupe appliances

20X
faster restores than dedupe appliances

Backup window that is **fixed length as data grows**

5YR
Price Protection Plan

New Retention Time-Lock for Ransomare Recovery

Set up with a
Proof of Concept
to experience the difference.

TEST IT TODAY ➤

exagrid.com

Using APIs to be data driven to the last mile

APIs enable retailers to make more intelligent business decisions through their omnichannel strategies.

BY JOEL REID, UK&I VP/GENERAL MANAGER, AXWAY

From TikTok to the last mile

RETAILERS' biggest priority is allowing customers to shop wherever they are. When the world shifted online during the pandemic, linking online to offline was critical for retailers to deliver outstanding customer experiences. In-person shopping still has its draw, with younger mobile shoppers showing a strong preference for more hybrid off-and-online shopping experiences. Yet social commerce spend has been driven up by the rapid rise of fashionable product influencers, with almost a quarter of shoppers in the UK finding products first on social media.

Retailers realise they need to invest in technology to ensure seamless synchronisation between in-store, online, fulfilment, and last-mile delivery. It's critical to have an omnichannel strategy which centralises data across disparate physical and online systems to obtain that single customer view, from marketing through to delivery.

With increasingly efficient store-to-door services during the pandemic, the retail world is fixated on creating efficiencies for converting orders. This means moving from marketing a product as a mere idea on TikTok to fulfilment and delivery to the door within sometimes hours.

Using APIs to deliver what customers want
Retailers are investing in application programmable interfaces (APIs) to bridge the gap between the virtual world and the last mile by connecting to third party applications. For instance, click and collect, same-day delivery through partner services, and real-time delivery tracking. In connecting market intelligence from social media sites with supply chains, brands are assured their last-mile services will quickly and easily deliver stock to customers' doors.

APIs and API management platforms enable retailers to create the seamless and frictionless shopping experiences today's consumers expect. They optimise the delivery of relevant and personalised product information to customers, wherever they are on the customer journey.

Customers need constant reassurance and guidance through the delivery process, which means that ensuring successful receipt is vital. It could mean linking product pages to social media platforms, giving personalised suggestions, or providing a 'find in store' service for when, frustratingly, it's out of stock online.
Using APIs in three key phases of the customer journey can build a strategy for remarkable customer experiences:

Pre-purchase – relevant and timely customer targeting

Shoppers need information and support from retailers at multiple contact points, and retailers are tactically using APIs to be able to provide this information. They might link product pages to social media platforms such as Instagram and Facebook, keeping these up to date with product information. APIs can also be used to link shoppers with detailed product information, for instance on sustainability credentials, such as whether a retailer will recycle your old sofa when bringing the new one.

Or a retailer may use API-enabled access to a real-time inventory for shoppers to discover if their preferred size and colour is available at a local store. It could be to offer 'low-in-stock' alerts about items they have previously browsed and are yet to purchase.

By allowing customers to create profiles and store wish-lists during shopping, retailers gain valuable insights from this data for cross-selling and up-selling.

API-powered apps can enable local branch managers and staff to submit insights and surveys which builds a rich data source, enabling intelligent business decisions, such as regional inventories.

Purchase – streamlining fulfilment

Each unique customer journey might involve browsing on social media before checking price and product features on the website or checking availability in store to see in person. But there are other key factors affecting a purchase decision.

Shoppers want to be able to choose how they receive the item, opting from a selection of Ship from Store, Click and Collect, Reserve and Collect, and Order in Store. They value regular communication updates during the delivery journey. APIs perform the vital role of linking disparate offline and online channels so customers can buy anywhere they choose and receive products by preference too. Customers expect no less than rapid delivery. According to McKinsey, 90% of consumers expect a two to three day delivery minimum and 30% expect same-day delivery. Utilising APIs can streamline order processing for in-store pickup or delivery. It can also give customers reassurance by connecting, retrieving and passing on delivery updates from logistics partners to customers, keeping the flow of communication as a package moves through different stages of its journey.

Post-purchase – becoming memorable

The post-purchase experience is paramount, as building satisfaction with customers might send them straight back online or into a store. Returns matter, and retailers that do it well can boost long term customer loyalty. A process that is easy, fast, and free and makes the customer's life easier, will make a retailer memorable - whether it's returning online purchases in store, printing a returns label, or using a home collection service.

Retailers can invest in APIs to streamline their returns process. This keeps customers happy and turns around stock fast for resale. Through empowering store assistants with the right customer information, retailers can leverage this data to address issues and reduce future returns.

Omnichannel all the way

APIs enable retailers to make more intelligent business decisions through their omnichannel strategies. It's vital to allow a customer to shop from anywhere and receive consistent personalised communications, whether they are on social media, the website or in-store; the brand experience should be the same. Retailers using tech like APIs will engage more effectively with customers, build a seamless shopping experience and make better business decisions.

Revolutionising the way we work

As our ways of working continue to be redefined by a digitally native workforce and external global factors, an agile, scalable, democratised tech stack is only going to continue to rise in importance.

BY GERT-JAN WIJMAN, VP EUROPE, MIDDLE EAST, AND AFRICA AT CELIGO

ORGANISATIONS are in a continuous process of change. They have become more horizontal, less hierarchical and more entrepreneurial. The workforce and management have become more diverse and technology has become critical in the way we communicate and collaborate, which has been accelerated by the pandemic.

New generations have joined the workforce with different expectations because they grew up with technology and are more IT savvy than older generations. They are more impatient because they can see on social media immediately what is going on in their world and they also expect more flexibility when it comes to work hours and location from where they work.

What does this all mean for the way organisations work when it comes to information technology and how does it impact the role of the CIO? Organisations need to be able to trust their data and business processes otherwise there cannot be effective collaboration especially across different functions and geographically dispersed (remote) workers. While the shift to the cloud has allowed basic collaboration across the globe it has also caused more data and process silos across the organisation. CIO's need to empower the business and to democratise IT to meet the new expectations of the business. Outside of formal IT departments, there is an increase in I&T talent and technical capabilities. Untamed and untapped, this can lead to a surge in an uncontrolled technical sprawl. But, the CIOs who are able to provide leadership, direction, and structure for this growing talent pool can utilise it to enhance organisational engagement, reduce risk, and increase enterprise value.

The power of iPaaS

An iPaaS (integration platform as a service) can connect (cloud) applications, integrate business processes and automate tasks to ensure data integrity and make processes scalable. This allows workers to have a similar (user) experience independent of location and to collaborate effectively with co-workers. It also allows them to focus on non-repetitive tasks and add more value to the organisation.

Automation through an iPaaS solves scalability issues in an environment where inflation rises and new hires are sometimes hard to find at acceptable costs. It provides an infrastructure to build a horizontal, scalable organisation. This is however not enough. In order to deliver on the promise of democratised IT the iPaaS must be implemented in a federated model where IT and the business work in a partnership to deliver technology across the company. This is where the real power of a modern iPaaS comes in as it caters to both IT and business users in the horizontal enterprise. By enabling a partnership between IT and the business, this also facilitates better process and data outcomes and provides long term organisational adaptability.

Especially for the departments that run like a start-up and for the impatient, IT-savvy younger generations, the federated model is the best of both worlds. The CIO and their organisation can now drive more value while leveraging the business instead of using a platform that can only be used by specialists in IT or by external specialists.

The future of automation

While integration solutions have been around for some time, a true platform approach for the whole organisation is becoming more relevant in an age where employees are more empowered. Not only does it provide a framework for control and ensuring compliance while allowing flexibility and scalability, a modern iPaaS also provides insights and error handling that allow optimal processes to be built over time. Using machine learning and AI, an iPaaS can create logs of errors and determine the best means to resolve issues. It can learn what processes work best and make suggestions about optimising other processes. It can provide real-time data and analysis to the business user who needs to make critical business decisions without waiting weeks for IT involvement.

Redefining the role of the IT leader

The shift in the way we work is also redefining how CIOs and other IT leaders must adapt to meet the new needs. Rather than starting with technology and retrofitting business processes into it, the modern CIO is a business leader who empowers the business to solve problems and drive value for the organisation.

CIOs are now challenged with balancing security and data integrity with democratisation, agility and flexibility. They must become partners with the business leaders who are driving technology decisions. And, while they must maintain some oversight of the processes and technology being implemented, they also have to relinquish some control to the hands of the people who know the process the best. In the end, this allows IT departments to focus on more strategic company priorities rather than implementing and managing hundreds of individual applications and processes. As our ways of working continue to be redefined by a digitally native workforce and external global factors, an agile, scalable, democratised tech stack is only going to continue to rise in importance.

Scaling cloud analytics: can governance keep pace with the democratisation imperative?

Cloud is one of the most discussed – and arguably least understood - topics of the last decade. The move to cloud was the ultimate catch-all term for a long period of time – something that could deliver health, wealth, happiness, a better hairline, or even that endearing sports car that caught your eye.

BY DAVID SWEENOR, SENIOR DIRECTOR OF PRODUCT MARKETING AT ALTERYX

THE REALITY – of course – is that cloud is a tool like any other... a tool with a highly specific remit. Today's cost of storage and compute is incredibly low and continuing to decrease, making the value proposition of creating and storing data an easy equation. Due to early-stage hype, however, many organisations integrated cloud technologies and systems without a fully operationalised plan of what to actually do with it. Some organisations learned the value of robust governance processes, legal compliance, and widespread training the hard way.

Despite being seen as the ideal tool to break down siloed ways of working, the reality of cloud integration at the time was disparate, segmented, and completed without a future-proofed use case roadmap for the business. This means that organisations that traditionally hoarded their data in-department continued to guard the keys to their kingdom... the only difference was the location their data was stored. Cloud was used as just another storage cabinet, and the true benefits left at the wayside.

Data driving competitive advantage

Data is one of the key drivers behind competitive advantage. Globally, we are now forecasted to see 180 zettabytes created each year – up from just 64.2 zettabytes in 2020. (For context, the largest hard drive available to consumers today is 24 terabytes, and one zettabyte is equal to one billion terabytes.) With enough data, converted into contextualised and relevant insights, and delivered into the hands of decision makers, organisations can sidestep disruption, seize opportunity, and predict the emergence of both well in advance.

Gartner notes that, by 2023, data literacy will become an explicit and necessary driver of business value. Today, we are seeing the emergence of those organisations that have been able to scale their compute resource and employee skillsets alongside vastly increasing data volumes.

Each of the most profitable companies in the world today have one thing in common - they are able to collect, analyse and act on the data they hold – at scale – to refine value and make effective decisions through analytics and automation.

For other businesses, facilitated by cheaper storage and in-cloud analytics, this highly effective end-to-end data culture is not only possible… it's actively feasible with the right strategy in place.

Cloud is a technology roadmap with huge potential for business efficiency. There are now three key facts to consider. Namely,

- Data literacy is a core driver of business value.
- The most profitable companies are also the ones making the best possible use of data.
- Cloud adoption – and storage availability - is rapidly increasing as cost-of-storage falls, and the volume of data created increases exponentially.

To summarise, data literacy correlates with business profitability. Further, greater data accessibility facilitates profit driving initiatives when driven by data literate staff.

Accessibility vs. Governance: why both need to work in tandem

The data accessibility potential that cloud technology brings is something that can cause IT teams to shudder – particularly where governance processes are not as robust as they could be. The combined factors of an increasingly data literate workforce and non-scaling governance policies present a unique challenge.

Considering the business requirement for fast insights, combined with a global business environment defined by disruption, simply locking down access – as we saw during the first wave of cloud adoption – is not an option. Instead, data workers need to be enabled and facilitated to mine the data for insights within the right corporate governance framework.

> Data is one of the key drivers behind competitive advantage. Globally, we are now forecasted to see 180 zettabytes created each year – up from just 64.2 zettabytes in 2020. (For context, the largest hard drive available to consumers today is 24 terabytes, and one zettabyte is equal to one billion terabytes.)

When delivering data insights, there are three core requirements. First is the need for data. Second is for that data to be high quality. The third requirement is to have a team that is upskilled and educated on what data factors and attributes are specifically needed.

Within these specific actions, however, sits the need for a data governance process across the entire business; one that defines how, where, and when data could – or should – be used, as well as if it should be used at all. In the EU, the GDPR specifies an overarching framework. This requirement for data fairness, ownership, and transparency, however, requires governance and specific processes to be adopted internally at individual businesses.

Without effective governance processes, the insights generated can be of questionable veracity. Without an upskilled and enabled team able to actually access the data they need, there won't be any insights generated at all.

As more and more employees are able to access data and use analytics, and as the accessibility of data increases globally through the use of cloud technologies, we see four pressing needs to deliver on the future promised through cloud analytics: Breaking down old silos; integrating well defined and contextualised governance processes; making analytics a more collaborative process, and upskilling the "domain experts" in your organisation are all vital steps to make use of cloud's turbocharged capacity.

Observability for all – why your organisation needs to upgrade its IT Stack

Observability is no longer only desirable, it is business critical.

BY NEW RELIC

THE DIGITAL WORLD is getting more complex by the minute. With every new innovation and service, tech stacks become more complex, and businesses are kept on their toes trying to maintain a seamless and convenient customer experience, no matter the roadblocks they cause. In turn, more time is required to manage digital infrastructure, maintain uptime, and keep on the front foot of innovation – critical operations that are costing businesses more time and money than they should.

Even as tech stacks become more complex, so too will the complexity of finding and fixing where something has gone wrong. With bugs and outages still very much an inevitability, IT leaders must be on their A-game to minimise the risk this poses to an organisation and its end users. This is a particular problem for large enterprises whose departments are traditionally siloed. And with each bug or attack, and every resulting minute of downtime, businesses lose their hard-earned credibility and trust with their customers.

With so much at stake, observability has never played such a crucial role.

Observability 101

In short, observability helps to cut through the challenges of complex IT stacks. Instead of monitoring each part of an IT application separately, observability provides users with 360-degree visibility of an organisation's full stack in real-time from a single platform. This means that when a bug occurs, developers are instantly able to home in on what's going wrong and fix it before it becomes a larger issue.

While observability is often used to monitor already operational tech stacks, it is vital across all parts of the software lifecycle. From initial conception, where it allows developers to understand whether they need to update previous products or start creating new ones, right through to deployment, when it is easy to monitor how well new products are operating.

At every stage, observability helps to improve productivity. It supports teams through data-led development decisions, leaves more time for innovation or provides the visibility that helps to significantly reduce mean time to repair (MTTR).
Understanding the full potential of observability
The real genius of observability platforms is their ability to provide complete visibility from a single pane of glass. Being able to view their entire stack from a unified platform means engineers can speed up operations and deploy software that protects their business from one place.

However, there are several barriers observability developers and users face. For developers, the main issue is compatibility. By their very nature, observability platforms must be able to be integrated with a wide range of products, from cloud services to open-source tools and enterprise technologies.

And despite the critical services it provides, according to New Relic's 2021 Observability survey, almost three quarters (74%) of respondents claim they do not have a mature observability practice. The survey found that the most cited barriers to observability success were a lack of resources (38%) and skills gaps (29%).

New Relic's Instant Observability offers almost 500 integrations, with more regularly added. The platform was designed to break down these barriers to use, integrating with common tools developers use so that every organisation can reap the benefits of observability. Postman, for example, is one of the recent tools integrated into New Relic and is used by over 20 million developers to build and consume APIs. Now each one of its users has the potential to gain full visibility over their APIs to increase the quality and speed of production.

Building teamwork

Securing an organisation's infrastructure from bugs and cyberattacks is vital for any company that wants to remain operational. However, the sprawling nature of software experiences makes this a difficult task. They all comprise thousands of components, spread across multiple clouds and open-source projects. And each one is operated by different internal and third-party engineering teams working in silos with limited working knowledge of what others are doing. This lack of visibility leads to an increase in blind spots, a range of security and business risks, and it can be difficult for the individual teams to then identify and fix the problem. Observability platforms that focus on vulnerability management are designed to combat this exact issue. Through the aggregation of all security signals, every engineer can work together to manage security risk at scale and accelerate software delivery and operation, regardless of the team or speciality. This level of collaboration works to keep organisations safer, helping them to address security problems quicker, and often even preempt them.

Business-critical observability

Observability is no longer only desirable, it is business critical. Consolidating all the data into one platform allows developers and the wider team to view the performance and status of an organisation's software stack in one go. This does not just reduce downtime, but enhances developer productivity, giving them more time to work on innovating their technology, enhancing the customer and user experiences, and strengthening product roadmaps. Observability is a win for all – empowering IT teams to innovate and building customer trust through the creation of better digital experiences.

DCA Data Centre Energy Efficiency SIG

By DCA CEO Steve Hone

AS THE Trade Association to the Data Centre sector the DCA understands that it is imperative that key issues affecting the sector have a point of focus. The DCA SIG's (Special Interest Groups) / Working Group regularly come together over shared interests to discuss issues, resolve problems, and make recommendations. Outcomes can result in best practice guides, collaboration between group members, participation in research projects, this includes clarification and guidance for decision and policy makers. Members find these groups are a great way to ensure their opinions and views are considered in a positive and cooperative environment.

The DCA currently facilitates nine Special Interest or Working Groups. DCA members can join any of the groups and contribute find out more here: https://dca-global.org/groups

The DCA Energy Efficiency SIG

The DCA Energy Efficiency SIG has members that sit on the EU and UK Standards Development Organisations and provides a two-way conduit for the discussion and development of the ISO TS 22237 series, the EN 50600 series and the ISO 30134 series of data centre design, build and operate standards and data centre key performance metrics.

The Energy Efficiency Steering Group is chaired by John Booth. John is also an author and committee member of the EU Code of Conduct for Data Centres (Energy Efficiency) best practices and requests applications from members for new, amended or deletion of best practices on an annual basis for discussion at the European wide EUCOC best practices meeting held in September/October every year.

This SIG looks at emerging concepts for the sustainability of the data centre building in terms of energy flexibility and waste heat reuse as well as alternative on and off-site energy generation for primary and backup purposes. This year the SIG has produce a Data Centre Energy Efficiency Guide which is available here

The group work very closely with the sustainability group to provide DCA members and Partners with an entire overview of data centre energy efficiency and sustainability.
To request to join this group please contact the DCA - mss@dca-global.org

Energy Consumption / Energy Efficiency In Data Centres

By Mike Goodwin, Partner Dunwoody LLP

DATA CENTRES consume power in what is commonly grouped under 2 headings. IT power and Systems Supporting the IT operation.
The primary measure of assessing energy in data centres (Energy Efficiency) is commonly focussed upon the PUE value whilst this can provide an indication, it does not provide the full understanding of a good facility.

The principle consideration is the measure of the parasitic component and not the base 'I' value of IT power, it is also correctly titled as Power Usage Effectiveness and does not call itself an efficiency matrix.

Whilst focusing on the smaller parasitic element, the power consumed by the IT installation also needs to be considered and improved. Most facilities would have improved their IT efficiency by undertaking operational assessments and optimised their systems but an assessment of processing efficiency, processing output per kW consumed would be beneficial. Many ongoing studies are considering this element, one being RISE (the Research Institute of Sweden).

However, significant quantities of energy are consumed in the IT process and supporting the IT process.
Entropy's first law is that power cannot be destroyed, and that it only changes state. For example, lighting installations convert electricity into light and heat and both enter the Universe, and are summarised as Entropy.

The goal is to produce a low energy data centre, highly efficient and emitting no carbon to the Atmosphere and many are focused on the generation of Carbon Free Electricity to achieve this. This generation of electricity by wind farms, PV panels, tri-generation etc is commendable but can be considered as offsetting and not correcting or improving and is therefore a global contribution or tax on operation. Is this the best method of progressing and how do we address the heat rejection that continues to occur, Entropy?
Heat is only waste if you don't use it. Keynes (Economic Thinker) discussed the Neutrality of Money. It is the Store of Value linking different people at different times. It removed the bartering system of one on one transactions and permitted transferable transactions.

Energy should be considered a commodity with value, that needs to be made available as a transferable product.

The most commonly discussed solution considers instantaneous complimentary events e.g. waste hot air – adjacent green houses and require simultaneous supply and demand. These solutions are few, often of differing magnitudes and only occurring simultaneously on few occasions. The optimum solution is most likely found in developing phase change systems.

Phase change systems are common place in data centre environments. They are present in the refrigeration cycle where refrigerant gasses change from liquid to gas absorbing and releasing energy at different stages of the cycle. They are present in evaporation / adiabatic systems where water evaporates that is liquid to gas, phase change.

Elsewhere there is the development of this concept to the use of Novec within immersion cooling systems. The adoption of Heat pipes (thermal cooling) where heat drives the refrigeration cycle without the use of compressors.

These systems remain within the boundary of the data centre.

However, to address the transferability of energy we need to consider the medium, gas, liquid, electricity, other, the location of the conversion plant and the transfer of energy to that location. Heat to electricity for use on site would be the first choice, this benefits from omitting any distribution losses and links availability and demand, however the likeliness of converting heat to electricity at an on-site conversion plant is currently extremely low.

The way forward therefore requires water or air transmissions – water with its greater density and higher specific heat value leads in the choices.
We then need to understand the temperature we can transmit and consider the "grade of heat", the higher the temperature the greater the use and the less water we need to circulate, but potentially introduces high distribution losses.

Capturing the IT process, heat at the highest temperature via water jackets / in rack heat exchanges or by immersion systems is good. Extracting heat from any refrigeration cycle at the hot gas stage of the cycle has the potential for high grade heat recovery, and capturing heat through hot aisle containment is also a possible but a lower grade solution. Elevating the heat to a transferable commodity can require a further process of using heat pumps. Within these actions a number of phase changes are occurring along with increases in grade (quality).

Once hot water is available, it can be applied to further applications – District Heating, a direct transfer, or one day possibly used as part of a Hydrogen production plant, generating Hydrogen from water, a phase change and a more fully transferable solution.

It's only Waste if you throw it away.
The issues remain

- Entropy constantly grows.
- Off set electricity still leaves surplus heat
- Use of surplus heat reduces someone else's carbon emissions

Rethinking Efficiency: How Hardware Assessment Saves on Cost, Carbon and Energy

Rich Kenny, Managing Director - Interact

HOW CAN data centre owners and managers assess their energy and carbon efficiency, improve financial performance and report this accurately to their customers and stakeholders? Rich Kenny, Managing Director of Interact, takes us through how accurate analysis of the server hardware can provide valuable savings on energy, carbon emissions and costs.

No-one likes bad press, and no-one likes increasing costs. As a high energy user, the data centre sector seems to be on the receiving end of both at the moment. Rising energy prices are an additional reason to do more with less. This is against the backdrop of the race to Net Zero, which is becoming faster and more intense.

The digital handprint – the carbon and energy savings technology can facilitate – is potentially larger than any other sector. However, growth is increasing its footprint at the same time. We need to demonstrate that we are delivering the highest computational output we can with the lowest energy draw. That begins by measuring what the machinery is doing and carrying out proper analysis of the hardware. By hardware, I mean the servers, which are responsible for the highest energy draw and for too long have been considered the black box no one dares open.

The data conundrum

There is an ironic lack of data in the data centre sector. For example, we have no absolute figures on how many UK data centres there are and no absolute definition of what a data centre is. Given this, there is no agreed upon figure of the exact energy usage of the sector in kWh.

Estimates exist based on the mandatory reporting for large energy users. Small and medium sized facilities, government and public sector data centres, those run by universities, enterprise and telecoms have not been historically captured. Even legislation such as Streamlined Energy and Carbon Reporting only requires an overall energy usage report, not anything that relates to the data centre share of this. The alternative path of estimating by data transfer is no less illuminating. Internet exchanges record spikes and growth in traffic but have no way to capture aggregated network energy as a result of internet use and data streaming, nor internal data transfers within organisations. The macro picture is pretty opaque. So, we need to look at the energy usage of individual data centres and groups for detail on how we make efficiency gains.

Stripping back to first principles

Servers are the machines that power the digital revolution, and their energy draw is significant. The IEA estimates data centres use around 1% of the world's energy. 65% of that energy draw at least is as a result of the servers; 100% is because the servers exist. The best way to reduce overall energy draw is to reduce the number of servers whilst simultaneously maintaining or increasing compute power.

You do this by analysing the energy usage and energy efficiency of each make and model of server in the estate and either replacing or modifying the worst performers with specific makes and models that improve performance. You can also use this information to select the least carbon intensive location to run workloads if you have multiple sites.

Assessing the impact of software operations within the data centre is a huge challenge and requires understanding the energy draw on the physical servers as a starting point. From there, you can make calculate on energy draw associated with virtualisation, containerisation and the like.

Outsourcing the issue

Cloud service providers are improving their ability to articulate cost and energy savings for customers using their services. They are publicly reporting their own energy and associated carbon usage and demonstrating reductions. However, it is difficult for stakeholders to understand the intricacies of this. Power Usage Effectiveness (PUE), Carbon Usage Effectiveness (CUE) and water usage effectiveness (WUE) are all ratios across the entire business. However, their data on the server estate is vague and imprecise.

Without understanding how much of the estate is idle, how much is overprovisioned to cater for traffic spikes and how far the facilities are from each other (so how much energy is lost in data transfer), it is difficult for customers to understand the precise impact of their digital usage. If they want accurate data, they need to know the physical server utilisation, efficiency at that level of utilisation and physical location where it is operating. These measurements will give a realistic figure of how much compute the server is giving for the energy that is being drawn. They will also tell users how carbon intensive that energy draw is.

Doing your homework

General best practice on IT is to understand what the hardware is doing first and then build up from there. Hardware draw feeds virtualisation, containerisation and application choices. All of these later will have an impact on the energy draw, but the hardware is the base layer you need to understand first.

The Server Energy Rating Tool (SERT) by SPECpower is the accepted benchmark for energy star rating for server manufacturers. This measures a variety of workloads and applies a geometric mean to them in order to produce a standardised metric of performance per watt. It is a great starting point but does not allow for direct comparisons of real-life server estates.

The next step is to run software that analyses energy draw of each server and collates this into a complete picture of the server estate, where utilisation, configuration and PUE are factored in. Interact is the only solution on the market that does this. Interact combines the published data from SPEC with thousands of hours of benchmark tests carried out by the research team. It identifies the worst performing servers and suggests a series of replacements for energy or cost optimisation over time.

The methodology has been validated by a peer-reviewed study in Elsevier's Sustainable Computing: Informatics and Systems and represents the first opportunity for data centres to ensure hardware is providing the lowest energy usage for unit of compute power. The team, co-funded by Innovate UK, also published a ground-breaking paper in the IEEE Transactions on Sustainable Computing called Optimizing server refresh cycles: The case for circular economy with an aging Moore's Law early in 2021.

Savings are eye watering: Interact analysed over 120 Data Centres in 2021, resulting in recommendations that average 5-year savings of £880,000 and 8.3m kWh per data centre and a reduction of 2,800 tonnes of CO2e emissions during use phase.
Large cloud providers, credit card providers and colocations are beginning to use it to optimise their server estates because the software offers them a scientifically verified method of optimising the hardware whilst at the same time report energy and carbon usage. Applications for data centres include optimisation of sites and consolidation of sites.

Managed service providers can pass on the savings to their customers to increase market share. For large international operations, the application is more around deciding which workload to migrate to which part of the world. Drawing the best value from IT hardware on a single site and across locations is one of the most beneficial things the world can do for sustainable digital growth. Software like Interact enables us to do this.

> Cloud service providers are improving their ability to articulate cost and energy savings for customers using their services. They are publicly reporting their own energy and associated carbon usage and demonstrating reductions

Six Simple Yet Effective Ways to Optimize Data Centre Energy Efficiency

By James Giblette, Director of Digital Infrastructure - UK & Ireland, Legrand Data Centre Solutions

IN THE CURRENT DIGITAL AGE, it is expected that data centres will continue to rise in both power consumption and complexity. In fact, it is predicted by IDC that the global datasphere will have expanded to 175 zettabytes by 2025. As the age of big data continues to grow, the challenge for data centre operators will be to discover how they support additional data whilst also meeting targets like those set out in the European Green Deal, an initiative to achieve climate-neutral, high-energy efficient, and sustainable data centres by 2030.

So, what can organizations do to reduce energy wastage in the data centre and meet sustainability initiatives? Here we review six core areas for consideration.

1. Power monitoring and measurement

It's so cliché, yet so true: You can't manage what you don't measure. The growth in data has resulted in an increased challenge for many in how to manage data centre power usage. Intelligent rack power distribution units (PDUs) can help address these challenges by allowing you to identify rack power consumption at the inlet, outlet, and circuit breaker level. Inlet metering is crucial for determining overall server power usage and availability at the rack. Metering at the outlet can help you understand the power consumption of a specific device or server, and metering at the circuit breaker provides early warnings if a circuit becomes heavily loaded and runs the risk of tripping.

Intelligent PDUs offer granular remote power monitoring of current (amps), voltage, power (kVA, kW), power factor, and energy consumption (kWh) to +/– 1% accuracy, providing you with the most critical information to help your data centre remain stable and efficient.

2. Identifying underutilized or idle servers

According to a recent survey by the Uptime Institute, approximately 30 percent of global data centre servers are either underutilized or completely idle. Idle servers are troublesome for the simple fact that they are inefficient and in large numbers can be highly expensive. Fortunately, intelligent PDUs with outlet level metering can help you to determine which servers are currently underutilized or inefficient and better understand how a specific server (or device) is consuming power. Through detailed power consumption metering, you can not only effectively monitor usage, but you can ultimately reduce your costs throughout the entire year.

Locating and correcting an idle server is made easier when you combine a DCIM solution with your intelligent rack PDUs, which will give you real-time insights into your data centre's assets. From owners to location, application information to power utilization trends, the DCIM software allows you to analyse all of your intelligent PDU data through a single pane of glass. By using the DCIM you can easily identify where you have an idle server.

3. Deploy environmental sensors to your racks

With the IT industry's increased focus on remote operations, more rack PDU manufacturers have begun offering environmental sensors. These include sensors to measure rack air temperature at the server inlets, as well as the humidity, airflow, vibration, smoke, water, and air pressure. Some PDUs may have pre-installed sensors; while others provide for optional, plug-in external sensors. Another approach is to deploy a completely independent intelligent sensor management solution, which provides an all-in-one intelligent device, with the minimum change required to the configuration of existing power distribution or IT infrastructure.

Coupling environmental sensors with intelligent PDUs answers the call for efficiency. Here's why:

- Ensure uptime by monitoring racks for potential hot spots
- Save on cooling by confidently raising data centre temperatures
- Maintain cabinet security with contact closure sensors
- Improve data centre availability by receiving environment alerts
- Make strategic decisions on cooling design and containment
- Set thresholds and alerts to monitor onsite or remote facilities

Sensors are an easy-to-install, cost-effective way to reduce energy costs, improve reliability, and increase capacity for future data centre growth. By using environmental sensors, you can optimize your data centre ecosystem to ensure that you are

The cooling setup in a server cabinet has a big influence on the PUE: a lower PUE results in lower total energy consumption of the data centre

meeting equipment guidelines, reducing operational costs, deferring capital investments, and improving your power usage effectiveness (PUE).

Additionally, Asset Management Tags (AMTs) and Asset Management Sensors (AMSs), provide data centre operators an accurate, automated, real-time inventory of all IT assets and their locations, down to the 1U level. Integrated with DCIM software, you can easily track assets, determine capacity in several areas, and manage adds, moves, or changes.

4. Implement remote power control

You wouldn't leave the lights on at home all day while you went to work, so why leave IT equipment that's not mission critical on during nights and weekends if no one is going to be using them? Test and other non-production servers can often be powered off to conserve power during non-peak hours. To begin a remote power cycling program within your organization, start by metering your current servers to determine the most common times during which they are not in use.

An intelligent PDU with the right capabilities will: A) Only perform a graceful shutdown of equipment to eliminate the risk of data loss or corruption, and B) Allow you to power cycle equipment with one or more power feeds on or off in a set order to minimize the risk of setting off a breaker due to an excessive inrush current.

5. Optimize airflow management in server cabinets

The cooling setup in a server cabinet has a big influence on the PUE: a lower PUE results in lower total energy consumption of the data centre. It is therefore extremely important that air leakage and recirculation is minimized so that the cool air is guided exclusively through the IT equipment. To do this, the space between the frame of the cabinet and the steel profiles must be perfectly sealed.

Airflow management packages can be used that consist of a bottom, top, left, and right plate. These plates connect the cabinet with the profiles in which the IT equipment is installed. Special accessories have also been developed by leading cabinet manufacturers to perfectly seal the spaces between the cabinets. Properly applied airflow management will bring forth higher efficiency and will lengthen the life span of your servers.

6. Remote working and the shift to the cloud

According to a recent Gartner report, by the end of 2023, more than 90% of infrastructure and operations (I&O) organizations will have the majority of their staff working remotely. This shift towards 'anywhere operations' challenges the traditional thinking of providing infrastructure and supporting operations from one central location. Enterprises now require remote power management solutions that enable staff to control data centre IT devices from multiple remote locations.

A further Gartner report, states that by 2024, more than 45% of IT spending on system infrastructure, infrastructure software, application software, and business process outsourcing will shift from traditional solutions to the cloud. The result is what Gartner calls 'cloud shift.'

Organizations can often benefit from the cloud provider's more energy-efficient infrastructure and presumably more optimized environment but many also fear the loss of access to their systems. The reality is however that a growing number of colocation providers can provide access to data centre power monitoring software so that clients can be sure they're being billed for actual power usage. Working with a colocation provider that allows clients to build out their racks and include KVM-over-IP switch access for remote administration will give organizations peace of mind that they still have access that's just like being at the rack.

Conclusion

Reducing carbon costs and energy consumption within the data centre is at the top of many organizations' sustainability, CSR, and efficiency agendas, in order to achieve the European Green Deal's goal of making data centres climate neutral by 2030. Adopting one or more of these simple energy-saving initiatives in your data centre can be made quickly and economically and could see your IT energy wastage drastically improve.

James Giblette is Director of Digital Infrastructure - UK & Ireland at Legrand Data Centre Solutions, which includes the Raritan, Server Technology, and Minkels brands. An expert on data centre solutions for the white space, James has 25 years of experience in the IT industry.

DCA Energy Efficiency SiG Update June 2022

All Data centres use energy, in some cases significant amounts, and globally there is an increasing focus on data centre energy consumption and as a result, pressure from consumers, business and governments to do more to reduce data centre energy use.

The Energy Efficiency SIG (one of the longest standing DCA SIGs) has in the past kept a close eye on ISO standards (ISO30134, ISO22237), European Standards, (the EN 50600 series) and the EU Code of Conduct for Data Centres (Energy Efficiency) best practices. Committee members represent the DCA on the appropriate standing committees for all the standards mentioned.

The EE SIG published an energy efficiency guide to coincide with Data Centre World 22 back in March and it can be downloaded from https://dca-global.org/groups/profile/4315/the-dca-energy-efficiency-sig.

The Energy Efficiency SIG is the first port of call for all thing's energy related in the Data Centre and works closely with other SIGs such as the Sustainability, Thermal Management, Commissioning and Certifications Groups.

In this update we'll provide the latest information on current standards, impending standards, an overview of the Climate Neutral Data Centre Pact and its relationship with the EU Code of Conduct for Data Centres and the European Commission.

Current Standards

The EE Chair maintains seats on the EU Code of Conduct for Data Centres (Energy Efficiency) and has recently been appointed as the Chair of the BSI TCT7/3 committee, and as such communicates pre-publication draft documents to the membership for comments and dissemination.

The Current Published Standards portfolio is listed below but is also contained in the DCA Energy Efficiency Best Practice Guide, as is our usual practice, standards are listed globally, regionally and then nationally, additional guidance such as industry best practices are listed at the end. It should be noted that standards development has not been curtailed by the Coronavirus pandemic, but activity has definitely slowed, most meetings now take place virtually but that we expect things to get back to normal by Q4 2022

Global

ISO 30134 Series – Data Centre KPIs

ISO TS 22237 Series – Data Centre, Design, Build and Operate (EN50600)

Regional

EU Code of Conduct for Data Centres (Energy Efficiency) – 13th Edition

EN 50600 Series

EN50600 – 1 General Principles

EN 50600 -2 Building Construction Power Supply and Distribution, Environmental Control, Telecommunications Cabling, Security systems

EN 50600-3 Management & operational information

EN 50600 -4 Data Centre KPIs (ISO 30134 Series)

EN50600-5 Data Centre Maturity Model

EN 50600 Technical Reports

TR-99-1 Energy

TR-99-2 Sustainability

TR99-3 Guidance to the Application of the EN 5060 Series

Impending Standards

Standards are in a constant phase of development, normally on 5-year refreshment cycles, so work to review and edit a standard commences in year 3/4 of its life ready for the next edition, the following standards are in either in public consultation phase, the last phase before publishing, or in development.

ISO 30134 -6, 8 & 9 Energy Reuse Factor, Carbon Utilisation Effectiveness, and Water Utilisation Effectiveness.

Some of the earlier EN 50600 are in the process of being updated.

Climate Neutral Data Centre Pact

The Climate Neutral Data Centre Pact was announced in late January 21 and at the time of writing consisted of 22 European Data Centre Trade Associations and 72 Data Centre or Cloud operators agreeing to adhere to 5 pillars, being energy efficiency, clean energy, water, circular economy and circular energy systems. The methodology and reporting requirements are still yet to be agreed with the European Commission, but the DCA has input into these discussions via the EU Code of Conduct for Data Centres (Energy Efficiency) committee and via the DCA's relationship with the EUDCA and will report progress at the next EE SIG meeting or via the Newsletter.

DCA SIG Energy Efficiency Guide

The energy efficiency guide was published in March 22 and to be honest is now out of date, a revision will be drafted and present to the SIG at the next meeting.

EU Taxonomy/Corporate Sustainability Reporting

The EU Taxonomy regulations are now in force and requires an independent 3rd party audit to be carried out every 3 years (EU Member States) to some parts of the EUCOC, this as you can imagine has caused some angst in the DC community, with the result that meetings to discuss the issue were called in May by DG CNCT.

The end result of these meetings was that a "Technical Committee" would be set up under the auspices of the TIC Council, more information on the TIC Council can be found on their website https://www.tic-council.org/ to develop an "auditable" assessment framework for use by auditing bodies to assess applicable data centres against the requirements of the EU Taxonomy regulations, this in turn would be overseen or married with a "Steering Committee" chaired by the EU-JRC. Both committees are expected to have developed an auditable assessment framework by Q4 2022. There is also a revision due to the EU Energy Efficiency Directive, this has been substantially "beefed up" as a result of the EU Green Deal and will no doubt be further amended as a result of the Ukrainian/Russia War, currently there is a proposal for a mandatory data centre registry to be set up in each members state and applicable data centres will be required to report energy consumption, origin of energy (% of renewable energy), water usage, and waste heat reuse. You will note the overlap between these proposals and the pillars of the Climate Neutral Data Centre Pact. The EE SiG will keep a very close eye on the CNDCP, EU EED and EU Taxonomy regulations.

> There is also a revision due to the EU Energy Efficiency Directive, this has been substantially "beefed up" as a result of the EU Green Deal and will no doubt be further amended as a result of the Ukrainian/Russia War, currently there is a proposal for a mandatory data centre registry to be set up in each members state and applicable data centres will be required to report energy consumption

Looking forward

Data Centres and Electricity have a unique, almost symbiotic relationship, data centres certainly cannot exist without electricity in some form, but in the future, where the electricity comes from will be an interesting debate, will it be on-site generation using renewable energy (wind, solar, biomass) or hydrogen networks with the associated fuel cell plant or the old fashioned direct utility connection or something else, no one knows for sure, but you can rest assured that the DCA EE SIG will be keeping an eye on it.

The regulatory regime looks to be getting tougher, more reporting and perhaps more carrots and sticks may be in the offing, the collection of data from data centres in terms of energy use, the origin of that energy, water usage and the use of waste heat data will allow policy makers to target the data centre sector like never before, this could develop into something like the Large Combustion Plant Directive (LCPD), essentially allowing a period of operation (LCPD was 20,000 hours) before measures are installed to reduce consumption, in the LCPD, it was the installation of Carbon Capture & Storage, but it did cause older more inefficient coal-fired power stations to close (most of the coal-fired power stations in the UK did close, but it did allow us to meet our climate goals and decarbonise the grid). However, now we are no longer part of the EU it remains to be seen if the UK will adopt or propose similar legislation for our market.

Conclusion

The EE SIG is one of the oldest groups in the DCA SIG portfolio, which clearly represents the importance of energy efficiency to not only the Alliance, but to its members, those that run data centres and those that supply products and services into data centres, and the future is bright or could be dim, depending on your viewpoint.