DW DIGITALISATION WORLD

Modern enterprise IT - from the edge to the core to the cloud

SEPTEMBER / OCTOBER 2020

digitalisationworld.com

The Future for 400G Networking

WITH RAY HAGEN, PROLABS GLOBAL PRODUCT LINE MANAGER

ProLabs
Unlock your connectivity

enel x

Energy management solutions that deliver commercial and environmental rewards

Global resources, local market knowledge and specialist technological expertise make Enel X the trusted energy management partner for data centres and large scale enterprises all over the world.

Join us as we pave the way for a cleaner, more dynamic future.

enelxuk@enel.com | www.enelx.co.uk

Editor's View

By Phil Alsop

Data privacy – should we be worried?

WITH FACEBOOK and, no doubt, other social media giants, under pressure to ensure that any data they gather on European users doesn't find its way across the Atlantic (I believe it's to do with the fact that the company cannot guarantee that such information won't fall into the hands of the US government, who might use it for surveillance purposes), and with various coronavirus track and trace applications in use (or about to be!), the issue of data privacy is very much centre stage.

Until recently, many of us may well have taken the basic view that: 'If I'm doing nothing wrong, why would I worry about what information the government, or any other organisation for that matter, might hold on me?'

But it's increasingly apparent that, no matter what laws may or may not be in place, our personal data is being used by an increasing number of organisations to try and interact with us for a variety of reasons, most of which have to do with understanding our behaviour so that we can be targeted commercially. At its most basic, and annoying level, any search that one conducts, is then used to promote apparently relevant products and services to me, in a fairly random, and often surprising way.

For example, I spend much of my time searching for IT-related information. At the weekend, when I'm then looking at various sports-related websites, the banner advertising is often about servers, storage and data centres. I'm not remotely interested in purchasing any of these, but a database somewhere believes that I am a potential purchaser.

Exaggerate such a misunderstanding, and change the context to something rather more important – taxation, employment, law-related issues, for example – and suddenly an algorithm (much like the one which so spectacularly failed to deliver fair exam results for many youngsters in the UK recently) could play havoc with an individual's life.

I've no doubt that the AI-based algorithms will improve over time, but it's unlikely that they will ever be able to understand human behaviour to a level required for 'safe' decision-making. Regulation of data is, therefore, a vital issue and one where self-regulation clearly won't work, but where the legislation that does exist seems rather inadequate, bearing in mind the global nature of the problem.

I would add that there is an important moral angle to the data issue, but as big business routinely tramples over any such concept where profits are at stake, let's leave that to one side and agree that the major issue is one of trust.

For example, when the UK track and trace app is introduced later this month, how many citizens will be happy to download it without a moment's thought, and how many will be nervous that, in so doing, they are potentially allowing the Government to intrude into their lives to an unacceptable extent? If one trusts the Government to use the data safely and reasonably, there should be no problem.

Many folk are, more or less, oblivious to the potential dangers of exposing their digital profile to organisations anywhere from a government, through social media, and down to the high street level.

Add in the very obvious dangers of an individual's data being used to facilitate criminal behaviour (there's more than a suggestion that a chat show host's recent pre-programme tweet about who would be appearing on his programme, alerted thieves to the fact that a certain celebrity would be in a TV studio on a certain data and at a certain time, hence said celebrity's house was burgled), and the data issue needs handling with a great deal of care.

I'm not sure that I have any earth-shattering words of wisdom (no change there, I hear you cry!), just the observation that far too many of us are far too willing accomplices in the growth of digital data, without carrying out a proper risk assessment. As with so many digital issues, there's a balance to be struck between the pluses and the minuses.

Where the duty of care lies in understanding this (online banking being a great example) is debatable. But, as with so many aspects of life, individuals and businesses need to be aware of the small print and the apparently so generous gift-bearers' motives.

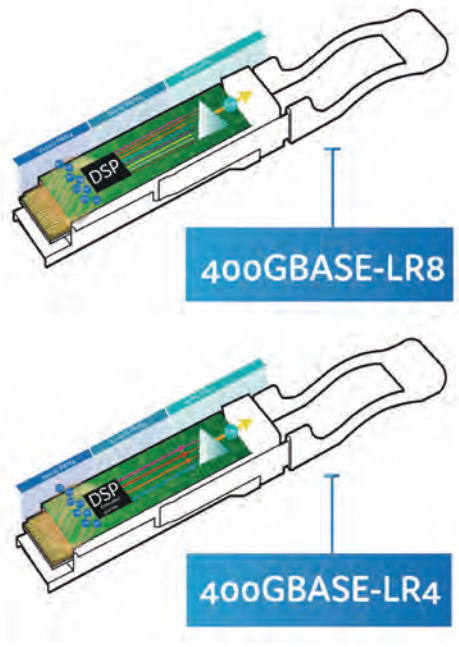
We live in volatile times. In such an environment, digital data has the possibility to both add to the problem and be a part of the solution. How data is used, when, where and by who will shape rather more than an individual's Internet-inspired purchases over the coming years.

Contents

20 COVER STORY

PAM4: A fundamental shift for 400G networking

Four-step Pulse Amplitude Modulation (PAM4) in pluggable fibre optics is expected to be the biggest shift in networking since its introduction to the network in the last decade



DIGITALISATION WORLD

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

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

Sales Manager
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 – CEO
Scott Adams – Joint - Managing Director
Sukhi Bhadal – Joint - Managing Director

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

Angel BUSINESS COMMUNICATIONS

recycle When you have finished with this magazine please recycle it.

Re-thinking the future

SMARTSHEET says that the business disruption caused by the pandemic is forcing organizations to rethink their future implementation of tools, tech and practices, according to a survey of global business professionals conducted by Harvard Business Review Analytic Services in association with Smartsheet.

COVID-19 uncovered the benefits of enabling an agile workforce, but also revealed the inefficiencies many organizations were facing due to technology. In fact, over three-quarters (76%) of respondents agreed the pandemic revealed major gaps in their internal technology strategy citing inefficiencies across the technology stack, from flexibility and speed to user friendliness and functionality.

Combined with the finding that 93% agreed it's necessary to provide teams with the software and tools needed to produce successful work, two-thirds (67%) of respondents stated their organizations are now reviewing their technology strategy.

When asked why their organizations are experiencing inefficiencies, only 50% of respondents reported their technology stack met employee needs while others recognized the need for change.

For example, 88% said having empowered, autonomous teams is critical to an organization's future success and 80% said agile and innovative workers played a big role in helping ensure business continuity and success during disruption.

"The pandemic has revealed that many organizations are battling a critical disconnect when it comes to their technology: the platforms they currently use do not fully empower their workforce to drive innovation and have organizational impact," said Mark Mader, CEO of Smartsheet. "We believe that to effectively compete, businesses must transform to work more dynamically - to simplify, streamline and integrate how work is initiated, managed, and delivered by their people and by their teams."

As organizations look forward, 86% agree the pandemic has changed the way their leadership is thinking about future-proofing the business. Nearly three-quarters (71%) of respondents agree that going forward, they expect their organization's leadership to entrust teams with innovating based on their own specific needs. In addition, over half (54%) feel their organization's innovation will be equally driven by employees and senior leadership opposed to 40% pre-pandemic.

"Organizations without the right technology pre-pandemic not only had to overcome the consequences of technology-based inefficiencies but their workforce also suffered resulting in decreased morale and lower productivity," said Alex Clemente, Managing Director of Harvard Business Review Analytic Services. "This impact on the workforce is driving a change in how leadership is approaching technology in the long-term, by empowering teams to be the catalyst of innovation and remain productive and competitive."

Data volumes and value increasing exponentially

STUDY IDENTIFIES pressures to capitalize on a new era and the opportunity found in data.

Splunk Inc. has published the results of new research that explores how prepared organizations are for the beginning of the Data Age. Two-thirds (67%) of those surveyed expect the sheer quantity of data to grow nearly five times by 2025.

The research shows that leaders see the significant opportunity in this explosion of data and believe data is extremely or very valuable to their organization in terms of: overall success (81%), innovation (75%) and cybersecurity (78%).

The report, built using research conducted by TRUE Global Intelligence and directed by Splunk, surveyed 2,259 global business and IT managers from the U.S., France, China, Australia, U.K., Germany, Japan and the Netherlands. The vast majority of survey respondents (81%) believe data to be very or highly valuable yet the majority (57%) fear that the volume of data is growing faster than their organizations' ability to keep up.

"The Data Age is here. We can now quantify how data is taking center stage in industries around the world. As this new research demonstrates, organizations understand the value of data, but are overwhelmed by the task of adjusting to the many opportunities and threats this new reality presents," said Doug Merritt, President and CEO, Splunk. "There are boundless opportunities for organizations willing to quickly learn and adapt, embrace new technologies and harness the power of data."

The Data Age has been accelerated by emerging technologies powered by, and contributing to, exponential data growth. Chief among these emerging technologies are Edge Computing, 5G networking, Internet of Things (IoT), Artificial intelligence and machine learning (AI/ML), Augmented and virtual reality (AR/VR) and Blockchain. It's these very same technologies that nearly half (49%) of those surveyed expect to use to harness the power of data, but across technologies, on average, just 42% feel they have high levels of understanding of all six.

Data Is valuable, and data anxiety is real

To thrive in this new age, every organization needs a complete view of its data – real-time insight, with the ability to take real-time action. But many organizations feel overwhelmed and unprepared. The new study from Splunk and TRUE Global Intelligence quantifies the emergence of a Data Age as well as the recognition that organizations have some work to do in order to use data effectively and be successful.

- Data is extremely or very valuable to organizations in terms of: overall success (81%), innovation (75%) and cybersecurity (78%).
- And yet, 66% of IT and business managers report that half or more of their organizations' data is dark (untapped, unknown, unused) – a 10% increase over the previous year.
- 57% say the volume of data is growing faster than their organizations' ability to keep up.
- 47% acknowledge their organizations will fall behind when faced with rapid data volume growth.

Some industries are more prepared than others

The study quantifies the emergence of a Data Age and the adoption of emerging technologies across industries, including:

- Across industries, IoT has the most current users (but only 28%). 5G has the fewest and has the shortest implementation timeline at 2.6 years.
- Confidence in understanding of 5G's potential varies: 59% in France, 62% in China and only 24% in Japan.
- For five of the six technologies, financial services leads in terms of current development of use cases. Retail comes second in most cases, though retailers lag notably in adoption of AI.
- 62% of healthcare organizations say that half or more of their data is dark and that they struggle to manage and leverage data.
- The public sector lags commercial organizations in adoption of emerging technologies.
- Manufacturing leaders predict growth in data volume (78%) than in any other industry; 76% expect the value of data to continue to rise.

Some countries are more prepared than others

The study also found that countries seen as technology leaders, like the U.S. and China, are more likely to be optimistic about their ability to harness the opportunities of the Data Age.

- 90% of business leaders from China expect the value of data to grow. They are by far the most optimistic about the impact of emerging technologies, and they are getting ready. 83% of Chinese organizations are prepared, or are preparing, for rapid data growth compared to just 47% across all regions.
- U.S. leaders are the second most confident in their ability to prepare for rapid data growth, with 59% indicating that they are at least somewhat confident.
- In France, 59% of respondents say that no one in their organization is having conversations about the impact of the Data Age. Meanwhile, in Japan 67% say their organization is struggling to stay up to date, compared to the global average of 58%.
- U.K. managers report relatively low current usage of emerging technologies but are optimistic about plans to use them in the future. For example, just 19% of U.K. respondents say they are currently using AI/ML technologies, but 58% say they will use them in the near future.

Tech spending set to boom

CLOUD COMPUTING and remote collaboration have been the main technology beneficiaries during the health crisis, with both remaining priority investment areas for the coming year.

Global analyst firm CCS Insight has revealed the findings of its annual survey of IT investment by senior business leaders. The survey explored spending and adoption plans in a range of areas that have become vital during the pandemic. They include cloud computing, remote work and collaboration, artificial intelligence (AI) and machine learning, security, trust and application development.

The survey polled more than 730 senior executives, predominantly in large organizations in the US and Europe from a range of industries. Respondents held director or above roles, with 60% holding C-level positions, including 20% of the survey in CEO roles.

Highlights include:

Two-thirds expect to increase IT budgets in 2021, despite a recession, with security the top priority

Businesses expect to continue their investments in cloud computing and remote collaboration as they have done during the pandemic. But as the crisis and companies' IT strategies shift to the next phase, security will be the biggest beneficiary in 2021. Cloud security in particular is now top of mind for most decision-makers, and security is also flagged as a priority in collaboration tools, investments in AI, and factors that determine trust in technology suppliers.

Attitudes to remote work have changed dramatically

The survey found that 34% of senior leaders expect more than half their workforce to work mainly from home post-Covid-19. This compares with just 15% prior to the pandemic. The shift to remote working has also meant that collaboration technology – and particularly video-meeting technology – has become mission critical.

The survey found that Microsoft Teams dominates the market, deployed by 46% of respondents' companies.

Cloud migrations are accelerating, and Microsoft Azure is the biggest beneficiary

The shift to remote work, the need to rapidly move operations online to maintain business continuity, and the elasticity of cloud services proving an attractive way to address spikes in demand during Covid-19 have all meant that cloud computing continues to grow rapidly. The proportion of businesses with over half their IT workloads hosted in the cloud is expected to double to 56% within the next year. Although most businesses are embracing a multicloud strategy, according to senior leaders, Microsoft Azure was cited as the most-used and trusted public cloud, ahead of IBM, Google Cloud and Amazon Web Services.

Artificial intelligence is entering a new chapter as businesses gain operational maturity

A year ago, most firms were running trials with machine learning, but during the pandemic, many turned to the technology in areas such as chat bots, contact centre assistance and demand forecasting. Over 80% of survey respondents are now trialling the technology or have put it into production, up from 55% in our 2019 survey. In addition, 58% of those surveyed plan to increase investment.

As more companies become operationally dependent on the technology, they are encountering new challenges associated with the risks of AI. Security is now the biggest challenge organizations face in this area, and more than 80% of respondents said they are concerned about ethical risks stemming from the uses of AI.

Low-code application development is now vital for developers

Software development has become crucial during the pandemic; 46% of organizations now use low-code tools as part of their application development processes. Respondents list Microsoft Power Platform and Google App Maker as the most popular tools in this area.

Insights into C-Level Decision-Making

Nick McQuire, Senior Vice President of Enterprise Research at CCS Insight, said, "Our survey this year of predominantly C-suite executives reveals fascinating insights into many of the most important aspects of technology transformation that will shape enterprise strategies in the coming year.

"Not only have we witnessed huge change in areas such as cloud transformation, remote collaboration, app development and machine learning over the past year, senior leaders expect even more change in 2021 as they push ahead with their digital investments".

He added "An enduring feature of the pandemic has been the elevated importance customers now place on their trust in technology suppliers, particularly cloud providers. In this respect, security and trust are among the top priorities for senior leaders as we move into the next phase of the crisis. Trust and security are clearly important themes that will shape the market".

On the shift to remote working, one of the standout areas of the survey, Angela Ashenden, Principal Analyst Workplace Transformation at CCS Insight, noted, "Clearly the shift to remote working has dramatically influenced businesses' perspectives on the way we work in the long term, and this is affecting the importance they place on tools to enable collaboration between remote workers.

"As offices start to reopen, organizations are now exploring the implications of a hybrid working model in which remote working remains the norm, but some staff return to the office. This will be a major focus area in the coming months".

Employees will return to offices in 12 to 18 months

600 IT leaders across five countries disclose post-COVID-19 priorities in support of a flexible work environment. A new global business survey commissioned by Xerox Holdings Corporation shows an estimated 82% of the workforce in respondents' organizations will have returned to the workplace in 12-18 months' time, on average. In preparation for a return, companies are investing in new resources to support a hybrid remote / in-office workforce, with 56% increasing technology budgets and 34% planning to speed their digital transformation as a result of COVID-19.

The Xerox Future of Work Survey, conducted by the independent research firm Vanson Bourne, polled 600 IT decision makers including senior C-level professionals from the U.S., Canada, the U.K., Germany and France, whose organizations have at least 500 employees. Respondents reported challenges caused by the sudden transition to remote work, with 72% citing they were not fully prepared from a technology perspective.

In addition to technology (29%), the biggest pain points during the required work from home period were communication breakdown across teams/employees (26%) and maintaining focus (25%).

"While there is no doubt the COVID-19 pandemic has changed the way we work, our research found that over time many companies plan to have most employees back in an office environment. This could be for a variety of reasons, including communication, speed of decision-making and talent development," said Steve Bandrowczak, Xerox president and chief operations officer. "At the same time, the sudden shutdown and ongoing hybrid work environment has exposed technology gaps that require new or additional investment in the coming months."

Key survey findings and Xerox takeaways include:

- Businesses plan to return most employees to the office, though expanded remote work policies are here to stay.

Prior to work from home requirements being imposed, 33% of respondents said network/data security and privacy was their biggest concern with a remote workforce; 24% cited employee productivity followed by 16% citing technology infrastructure. These concerns, coupled with the belief held by 95% of respondents that in-person communication is important for personal development and assessing talent, indicate widespread remote work will not replace more traditional workspaces.

However, now that businesses are more comfortable with remote work, attitudes and policies of C-suite leaders and IT decision makers are shifting. Among the countries polled, the U.S. is the most likely to have an increase in confidence in remote working (86%), followed by the U.K. (80%), Germany (80%), Canada (77%), and France (75%). Furthermore, 58% plan to change their work from home policy within the next year, highlighting the need for companies to support a hybrid workforce.

Our takeaway: Employees may not be going back to the office all at once – or even in the same capacity as before – but the need for organizations to support a hybrid workforce is here for the foreseeable future.

- **Sudden stay-at-home orders quickly revealed technology gaps.**

The rapid transition to remote work was difficult for most businesses, with only 28% saying they were fully prepared and 29% citing technology as their biggest pain point. Among the specific countries polled, France was the least likely to be fully prepared for the sudden transition to remote work, while the U.S. was the most likely to be fully prepared. With regards to technology specifically, respondents said their top challenges were remote IT support (35%), inadequate workflow solutions (27%), lack of communications and collaboration tools (22%) and lack of cloud-based solutions (10%). 85% of business leaders also missed the accessibility and ease of use of their office printers, with U.S. respondents missing them the most (93%) followed by Germany (92%) and France (91%).

Our takeaway: To mitigate against future disruptions, such as the rapid transition to remote work resulting from COVID-19, companies will look to invest in new technologies and seek added capability from existing tools to accelerate their processes digital transformation.

- **Technology purchasing priorities are shifting to better support employees.**

As a result of technology gaps uncovered by having a mostly remote workforce, 70% of IT decision makers globally are reevaluating their budget spend, with companies increasing investment in remote technology resources (55%) or a hybrid of remote and in-office resources (40%). The pandemic also has businesses prioritizing investments in cloud-based software (65%), remote IT (63%) support and collaboration software (52%).

Hardware such as laptops and printers were another important consideration, especially for companies based in France, with 22% of respondents citing it as the most important need when it comes to technology, productivity and their overall work experience.

Our Takeaway: COVID-19 is feeding digital transformation plans and companies are placing a renewed focus on meeting employees' needs with both hardware and software.

Gartner identifies five emerging trends that will drive technology innovation

The 30 must-watch technologies on the Gartner Inc. Hype Cycle for Emerging Technologies, 2020 include technologies that enable a composable enterprise, aspire to regain society's trust in technology, and alter the state of your brain.

"EMERGING TECHNOLOGIES are disruptive by nature, but the competitive advantage they provide is not yet well known or proven in the market. Most will take more than five years, and some more than 10 years, to reach the Plateau of Productivity. But some technologies on the Hype Cycle will mature in the near term and technology innovation leaders must understand the opportunities for these technologies, particularly those with transformational or high impact," said Brian Burke, research vice president at Gartner.

For example, health passports and social distancing technologies, both related to the COVID-19 pandemic, are taking the fast track through the Hype Cycle and have high impact. Technologies rarely enter the Hype Cycle at the point where social distancing technologies has entered it, but this technology has received extraordinary attention in the media, mainly because of privacy concerns. Health passports are also unusual as technologies with market penetration of 5-20% are rarely introduced, but this technology, required for access to public spaces and transportation in China (Health Code) and India (Aarogya Setu), is being used by hundreds of millions of people in those countries. Both technologies are expected to reach the plateau of productivity in less than two years."

The Hype Cycle for Emerging Technologies is unique among most Gartner Hype Cycles because it garners insights from more than 1,700 technologies into a succinct set of 30 emerging technologies and trends. This Hype Cycle specifically focuses on the set of technologies that show promise in delivering a high degree of competitive advantage over the next five to 10 years (see Figure 1).

Five emerging technology trends

Digital me: Technology is becoming increasingly integrated with people to create new opportunities for digital representations of ourselves, such as digital passports and social distancing technologies. Digital twins of humans provide models of individuals that

can represent people in both the physical and digital space. The way people interact with the digital world is also moving beyond screens and keyboards to use a combination of interaction modalities (e.g. voice, vision, gesture), and even directly altering our brains. The technologies to watch include social distancing technologies, health passports, digital twin of the person, citizen twin, multiexperience and 2-Way BMI (brain machine interface).

Composite architectures: The composable enterprise is designed to respond to rapidly changing business needs with packaged business capabilities built upon a flexible data fabric. A composite architecture is implemented with solutions composed of packaged business capabilities. Built-in intelligence is decentralized and extends outward to edge devices and the end user.

To become a more agile organization, the following technologies should be tracked: composable enterprise, packaged business capabilities, data fabric, private 5G, embedded artificial intelligence (AI) and low-cost single-board computers at the edge.

Formative AI: This is a set of emerging AI and related technologies that can dynamically change to respond to situational variances. Some of these technologies are used by application developers and UX designers to create new solutions by using AI enabled tools. Other technologies enable the development of AI models that can evolve dynamically to adapt over time. The most advanced can generate entirely novel models that are targeted to solve specific problems.

Enterprises looking to explore the boundaries of AI should consider AI-assisted design, AI augmented development, ontologies and graphs, small data, composite AI, adaptive ML, self-supervised learning, generative AI and generative adversarial networks.

Algorithmic trust: Trust models based on responsible

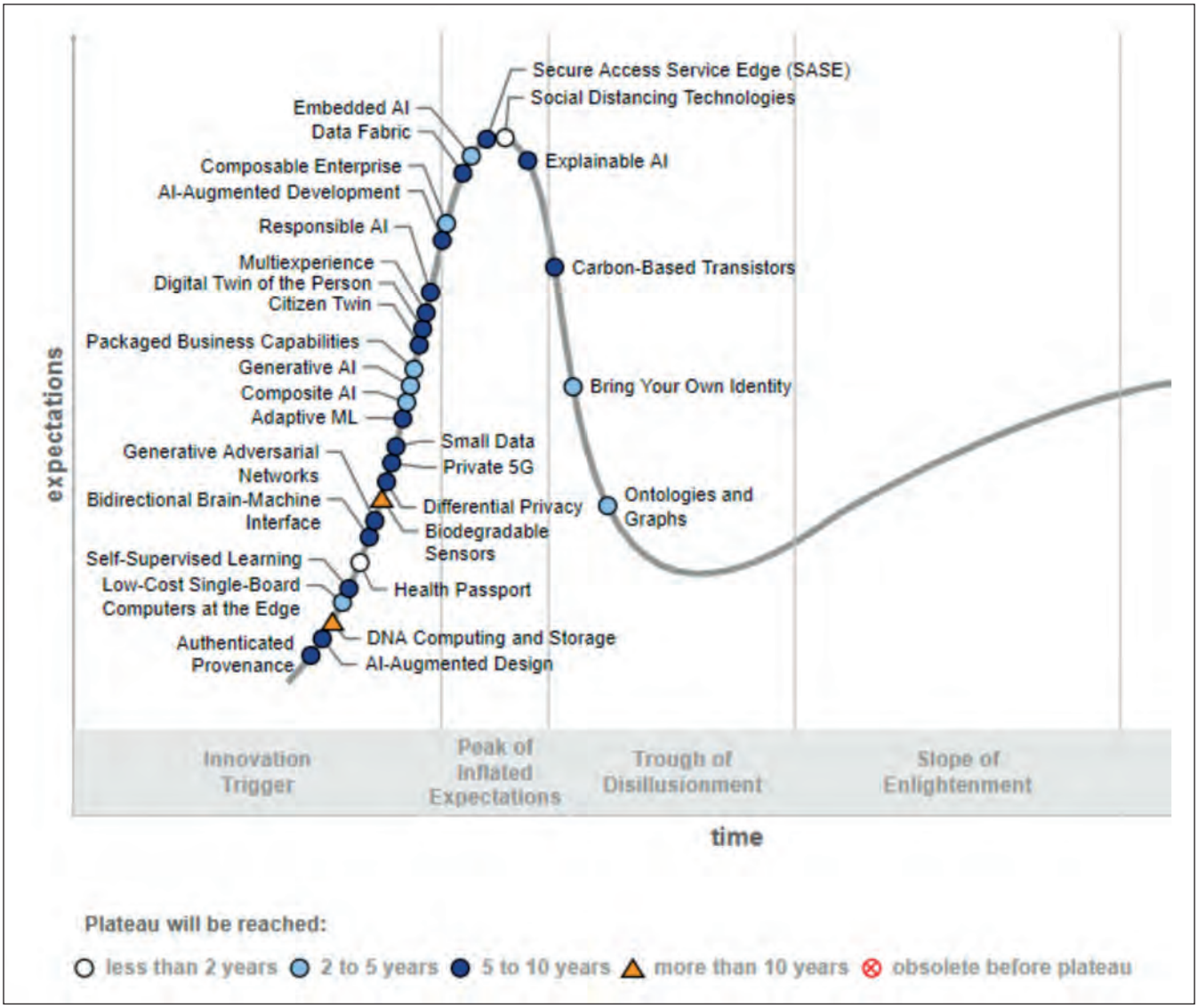


Figure 1. Hype Cycle for Emerging Technologies, 2020. Source: Gartner (August 2020)

authorities are being replaced by algorithmic trust models to ensure privacy and security of data, source of assets and identity of individuals and things. Algorithmic trust helps to ensure that organizations will not be exposed to the risk and costs of losing the trust of their customers, employees and partners. Emerging technologies tied to algorithmic trust include secure access service edge (SASE), differential privacy, authenticated provenance, bring your own identity, responsible AI and explainable AI.

Beyond silicon: For more than four decades, Moore's Law (the number of transistors in a dense integrated circuit (IC) doubles about every two years) has guided the IT industry. As technology approaches the physical limits of silicon, new advanced materials are creating breakthrough opportunities to make technologies faster and smaller.

Critical technologies to be considered include DNA computing, biodegradable sensors and carbon-based transistors.

CEOs will be liable for cyber-physical security incidents

Liability for cyber-physical security incidents will pierce the corporate veil to personal liability for 75% of CEOs by 2024, according to Gartner, Inc.

Due to the nature of cyber-physical systems (CPSs), incidents can quickly lead to physical harm to people, destruction of property or environmental disasters. Gartner analysts predict that incidents will rapidly increase in the coming years due to a lack of security focus and spending currently aligning to these assets. Gartner defines CPSs as systems that are engineered to orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). They underpin all connected IT, operational technology (OT) and Internet of Things (IoT) efforts where security considerations span both the cyber and physical worlds, such as asset-intensive, critical infrastructure and clinical healthcare environments.

"Regulators and governments will react promptly to an increase in serious incidents resulting from failure to secure CPSs, drastically increasing rules and regulations governing them," said Katell Thielemann, research vice president at Gartner. "In the U.S., the FBI, NSA and Cybersecurity and Infrastructure Security Agency (CISA) have already increased the frequency and details provided around threats to critical infrastructure-related systems, most of which are owned by private industry. Soon, CEOs won't be able to plead ignorance or retreat behind insurance policies."

Gartner predicts that the financial impact of CPS attacks resulting in fatal casualties will reach over $50 billion by 2023. Even without taking the actual value of a human life into the equation, the costs for organizations in terms of compensation, litigation, insurance, regulatory fines and reputation loss will be significant.

"Technology leaders need to help CEOs understand the risks that CPSs represent and the need to dedicate focus and budget to securing them," said Ms. Thielemann. "The more connected CPSs are, the higher the likelihood of an incident occurring." With OT, smart buildings, smart cities, connected cars and autonomous vehicles evolving, incidents in the digital world will have a much greater effect in the physical world as risks, threats and vulnerabilities now exist in a bidirectional, cyber-physical spectrum. However, many enterprises are not aware of CPSs already deployed in their organization, either due to legacy systems connected to enterprise networks by teams outside of IT, or because of new business-driven automation and modernization efforts.

"A focus on ORM – or operational resilience management - beyond information-centric cybersecurity is sorely needed," Ms. Thielemann said.

Gartner predicts that the financial impact of CPS attacks resulting in fatal casualties will reach over $50 billion by 2023. Even without taking the actual value of a human life into the equation, the costs for organizations in terms of compensation, litigation, insurance, regulatory fines and reputation loss will be significant

CELEBRATING 10 YEARS OF SUCCESS

The 2020 DCS Awards feature 31 categories across FOUR groups.

THE DCS AWARDS are now firmly established as the data centre industry's premier annual celebration of all that is great and good. End user projects, product innovation and individual excellence are all recognised in an evening that pays more than lip service to the idea of data centre and IT convergence. So, the award categories cover both the facilities and IT aspects of the data centre, recognising the achievements of vendors, their business partners, their staff and their customers.

Getting involved with the DCS Awards couldn't be easier. Take a look at the award categories, and make sure to nominate your company, a customer, or maybe an individual – better still all three (!) – for a chance to be recognised for outstanding achievement when it comes to projects, product innovations and individual contributions within the data centre industry.

Once you've made your nominations, make sure to book a table for the Awards night. You wouldn't want to win an award and not be there to collect it! (And even if you don't win an award on the night, there's a cocktail reception, three course meal and a top comedian to entertain you – we have a track record of booking individuals on their way to the top of the comedy circuit).

To 'We look forward to welcoming you to the Awards night in December.

NOW, GET NOMINATING!

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE

The DCS Awards panel will validate entries and announce the final shortlist to be forwarded for voting by the readership of the Digitalisation World stable of publications in October 2020.

The winners will be announced at a gala evening at the LEONARDO ROYAL ST. PAUL'S HOTEL, London on 10 December 2020.

DCS AWARDS 2020

www.dcsawards.com

Supported by

dca The data centre trade association

Worldwide AI spend to double by 2024

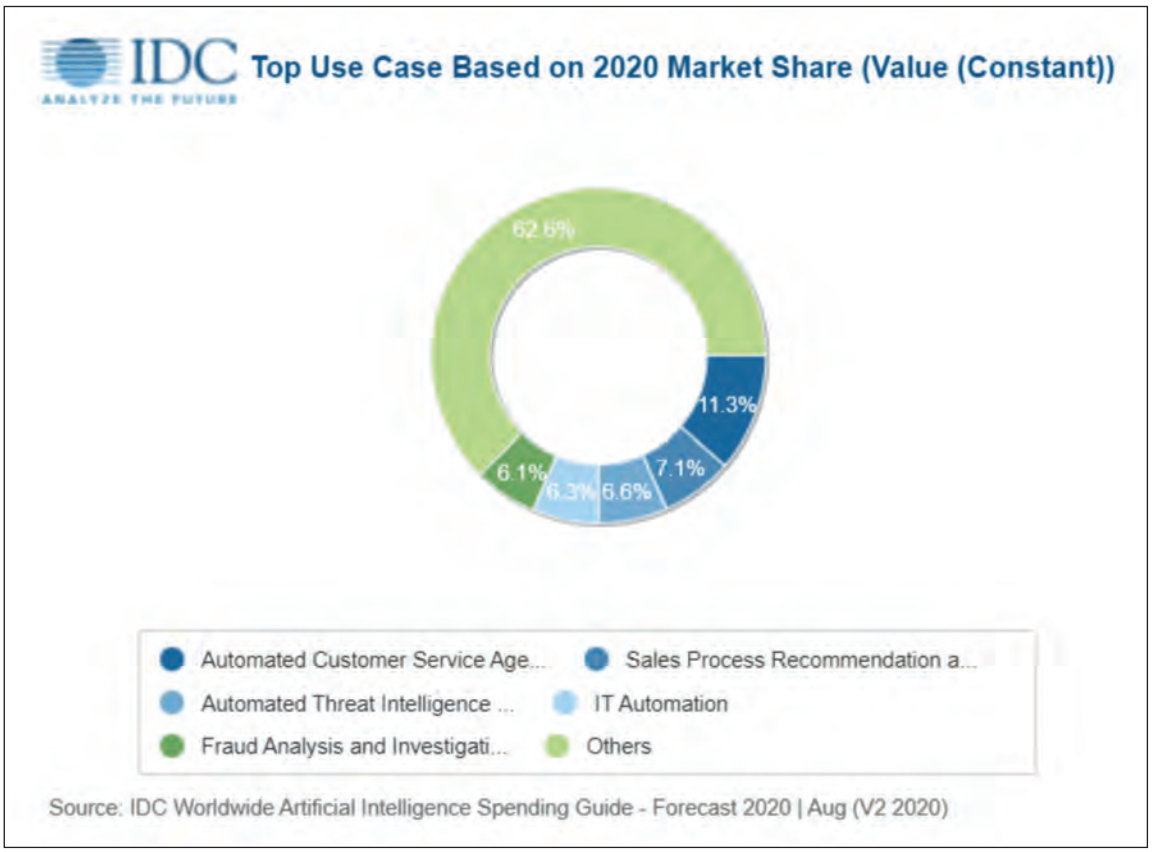
Global spending on artificial intelligence (AI) is forecast to double over the next four years, growing from $50.1 billion in 2020 to more than $110 billion in 2024.

ACCORDING TO the International Data Corporation (IDC) Worldwide Artificial Intelligence Spending Guide, spending on AI systems will accelerate over the next several years as organizations deploy artificial intelligence as part of their digital transformation efforts and to remain competitive in the digital economy. The compound annual growth rate (CAGR) for the 2019-2024 period will be 20.1%.

"Companies will adopt AI — not just because they can, but because they must," said Ritu Jyoti, program vice president, Artificial Intelligence at IDC. "AI is the technology that will help businesses to be agile, innovate, and scale. The companies that become 'AI powered' will have the ability to synthesize information (using AI to convert data into information and then into knowledge), the capacity to learn (using AI to understand relationships between knowledge and apply the learning to business problems), and the capability to deliver insights at scale (using AI to support decisions and automation)."

Two of the leading drivers for AI adoption are delivering a better customer experience and helping employees to get better at their jobs. This is reflected in the leading use cases for AI, which include automated customer service agents, sales process recommendation and automation, automated threat intelligence and prevention, and IT automation. Combined, these four use cases will represent nearly a third of all AI spending this year. Some of the fastest growing use cases are automated human resources, IT automation, and pharmaceutical research and discovery.

The two industries that will spend the most on AI solutions throughout the forecast are Retail and Banking. The Retail industry will largely focus its AI investments on improving the customer experience via chatbots and recommendation engines while Banking will include spending on fraud analysis and investigation and program advisors and recommendation systems. Discrete Manufacturing,



Process Manufacturing, and Healthcare will round out the top 5 industries for AI spending in 2020. The industries that will see the fastest growth in AI spending over the 2020-2024 forecast are Media, Federal/Central Government, and Professional Services.

"COVID-19 caused a slowdown in AI investments across the Transportation industry as well as the Personal and Consumer Services industry, which includes leisure and hospitality businesses. These industries will be cautious with their AI investments in 2020 as their focus will be on cost containment and revenue generation rather than innovation or digital experiences," said Andrea Minonne, senior research analyst, Customer Insights & Analysis. "On the other hand, AI has played a role in helping societies deal with large-scale disruptions caused by quarantines and lockdowns. Some European governments have partnered with AI start-ups to deploy AI solutions to monitor the outcomes of their social distancing rules and assess if the public was complying with rules. Also, hospitals across Europe are using AI to speed up COVID-19 diagnosis and testing, to provide automated remote consultations, and to optimize capacity at hospitals."

"This release of the Artificial Intelligence Spending Guide was adjusted for the impact of COVID-19," said Stacey Soohoo, research manager, Customer Insights & Analysis. "In the short term, the pandemic caused supply chain disruptions and store closures with continued impact expected to linger into 2021 and the outyears. For the most impacted industries, this has caused some delays in AI deployments. Elsewhere, enterprises have seen a silver lining in the current situation: an opportunity to become more resilient and agile in the long run. Artificial intelligence continues to be a key technology in the road to recovery for many enterprises and adopting artificial intelligence will help many to rebuild or enhance future revenue streams and operations."

Software and services will each account for a little more than one third of all AI spending this year with hardware delivering the remainder. The largest share of software spending will go to AI applications ($14.1 billion) while the largest category of services spending will be IT services ($14.5 billion). Servers ($11.2 billion) will dominate hardware spending. Software will see the fastest growth in spending over the forecast period with a five-year CAGR of 22.5%.

On a geographic basis, the United States will deliver more than half of all AI spending throughout the forecast, led by the Retail and Banking industries. Western Europe will be the second largest geographic region, led by Banking, Retail, and Discrete Manufacturing. China will be the third largest region for AI spending with State/Local Government, Banking, and Professional Services as the leading industries. The strongest spending growth over the five-year forecast will be in Japan (32.1% CAGR) and Latin America (25.1% CAGR).

Worldwide Public Cloud Services market totalled $233.4 billion in 2019

THE WORLDWIDE public cloud services market, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), grew 26.0% year over year in 2019 with revenues totaling $233.4 billion, according to the International Data Corporation (IDC) Worldwide Semiannual Public Cloud Services Tracker.

SPENDING CONTINUED to consolidate in 2019 with the combined revenue of the top 5 public cloud service providers (Amazon Web Services, Microsoft, Salesforce.com, Google, and Oracle) capturing more than one third of the worldwide total and growing 35% year over year.

"Cloud is expanding far beyond niche e-commerce and online ad-sponsored searches. It underpins all the digital activities that individuals and enterprises depend upon as we navigate and move beyond the pandemic," said Rick Villars, group vice president, Worldwide Research at IDC. "Enterprises talked about cloud journeys of up to ten years. Now they are looking to complete the shift in less than half that time."

The public cloud services market has more than doubled since 2016. During this same period, the combined spending on IaaS and PaaS has nearly tripled. This highlights the increasing reliance on cloud infrastructure and platforms for application deployment for enterprise IT internal applications as well as SaaS and digital application delivery. IDC expects spending on IaaS and PaaS to continue growing at a higher rate than the overall cloud market over the next several years as resilience, flexibility, and agility guide IT platform decisions.

"Today's economic uncertainty draws fresh attention to the core benefits of IaaS – low financial commitment, flexibility to support business agility, and operational resilience," said Deepak Mohan, research director, Cloud Infrastructure Services. "Cost optimization and business resilience have emerged as top drivers of IT investment decisions and IaaS offerings are designed to enable both. The COVID-19 disruption has accelerated cloud adoption with both traditional enterprise IT organizations and digital service providers increasing use of IaaS for their technology platforms."

"Digitizing processes is being prioritized by enterprises in every industry segment and that is accelerating the demand for new applications as well as repurposing existing applications," said Larry Carvalho, research director, Platform as a Service. "Modern application platforms powered by containers and the serverless approach are providing the necessary tools for developers in meeting these needs. The growth in PaaS revenue reflects the need by enterprises for tools to accelerate and automate the development lifecycle."

"SaaS applications remains the largest segment of public cloud spending with revenues of more than $122 billion in 2019. Although growth has slowed

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

Segment	2019 Revenue	Market Share	2018 Revenue	Market Share	Year-over-Year Growth
IaaS	$49.0	21.0%	$35.4	19.1%	38.4%
PaaS	$35.9	15.4%	$25.8	14.0%	38.8%
SaaS*	$148.5	63.6%	$123.9	66.9%	19.8%
Total	**$233.4**	**100%**	**$185.2**	**100%**	**26.0%**

Source: IDC Worldwide Semiannual Public Cloud Services Tracker, 2H19
* Note: SaaS revenues include both SaaS Applications and SaaS System Infrastructure Software.

somewhat in recent years, the current crisis serves as an accelerator for SaaS adoption across primary and functional markets to address the exponential growth of remote workers," said Frank Della Rosa, research director, SaaS and Cloud Software.

Looking at the segment results, a combined view of IaaS and PaaS spending is relevant because it represents how end customers consume these services when deploying applications on public cloud. IDC has been tracking and publishing this view of the market since 2019. In the combined IaaS and PaaS market, Amazon Web Services and Microsoft captured more than half of global revenues. But there continues to be a healthy long tail, representing over a third of the market. These are typically companies with targeted use case-specific PaaS offerings. The long tail is even more pronounced in SaaS, where nearly three quarters of the spending is captured outside the top 5.

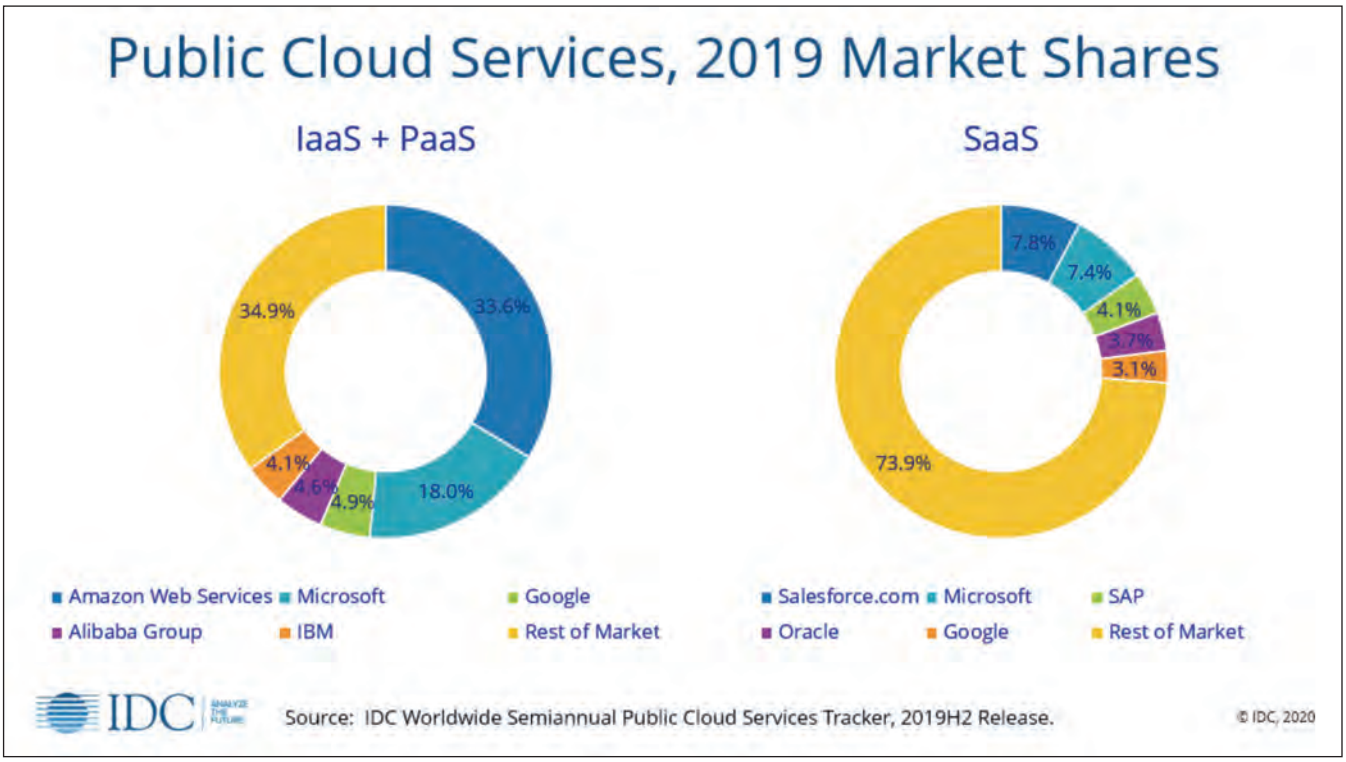
Solid security growth

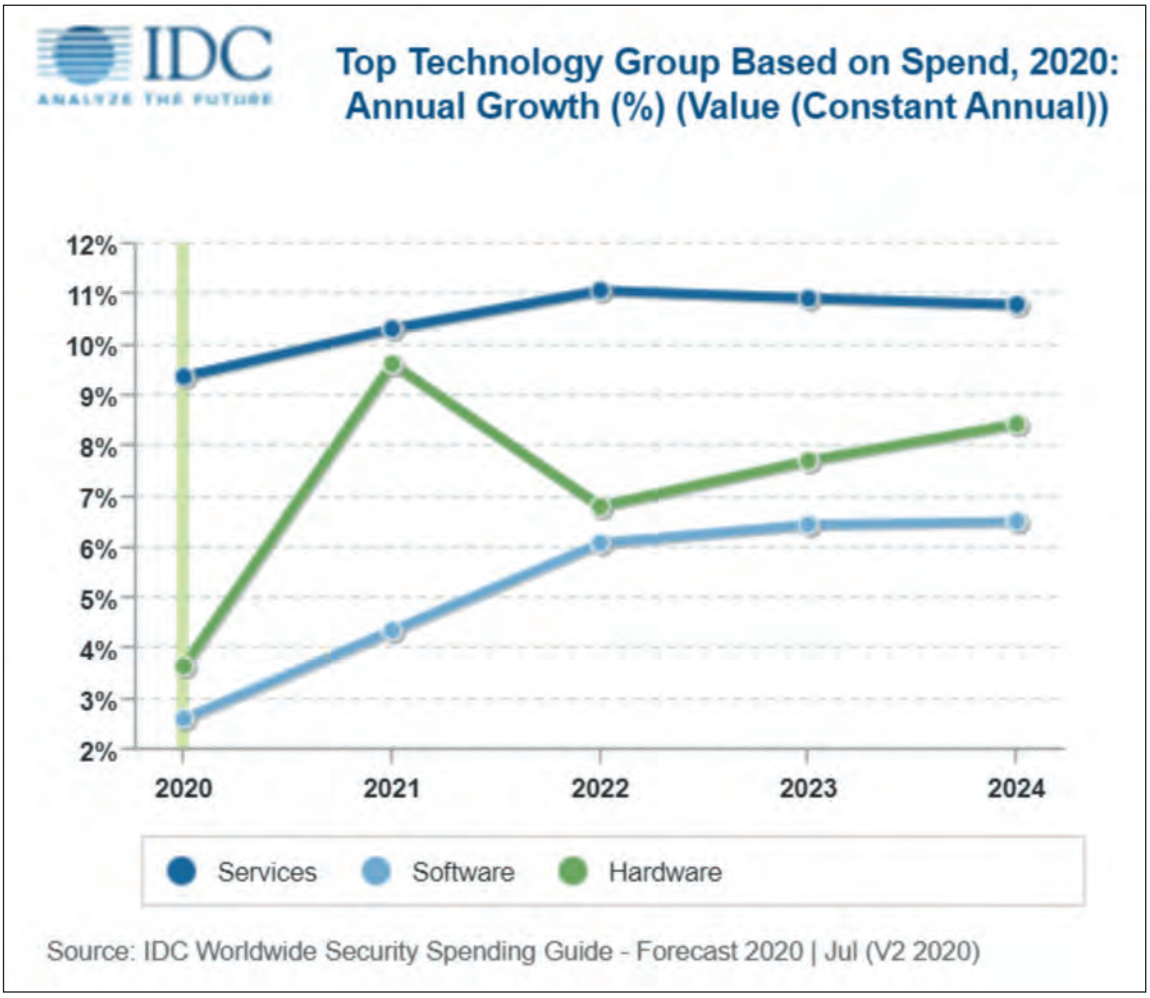
Worldwide spending on security products and services will see solid growth in 2020 as organizations invest in solutions to meet the needs of a much larger remote workforce and a wide range of security threats and requirements. According to a new forecast from the International Data Corporation (IDC) Worldwide Security Spending Guide, worldwide spending on security-related hardware, software, and services will be $125.2 billion in 2020, an increase of 6.0% over 2019. As the global economy recovers from the impact of COVID-19, IDC expects worldwide security spending to reach $174.7 billion in 2024 with a compound annual growth rate (CAGR) of 8.1% over the 2020-2024 forecast period. The new Spending Guide also offers expanded coverage of security IT services with the addition of 13 technology detail markets.

"While IT spending is contracting across most industries and technologies in the wake of the pandemic, security spend remains strong, particularly in industries including State/Local Governments, Telecom, and Federal/Central Governments that have become essential in our new environment. Indeed, these three industries will exhibit double-digit growth in security spending through 2024," said Karen Massey, research manager, Customer Insights & Analysis. "Meanwhile, Banking, Manufacturing, and Professional Services continue to have the largest share of security spending. We even see positive movement in security for industries that are currently struggling, such as Retail and Transportation."

The three industries with the largest security investments (Banking, Discrete Manufacturing, and Federal/Central Governments) will account for roughly 30% of overall spending in 2020 and throughout the forecast. The industries that are seeing the greatest increase in security spending this year are Federal/Central Government (10.0%), State/Local Government (8.9%), and Telecommunications (8.5%). These three industries will also deliver the only double-digit CAGRs over the five-year forecast period, led by State/Local Government with an 11.1% CAGR.

Security services will be the largest and fastest growing segment of the security market accounting for roughly half of all spending throughout the forecast





and a 10.5% five-year CAGR. Managed security services – single-tenant solutions operated by third-party providers and residing on customers' premises (customer premises equipment) – is the largest category of security services spending, followed by integration services and consulting services. Managed security services will also be the fastest growing segment with a five-year CAGR of 13.6%.

"Complexity abounds with security technology deployment and sprawl requiring assessment and design services," said Christina Richmond, program vice president, Security Services. "While COVID-19 has had a negative impact on many ICT technologies, security services have witnessed increased engagements, especially in outsourcing services such as managed security services (MSS) and managed detection and response (MDR). Security services will see strong demand throughout the forecast period."

Software will be the second largest segment of the security market, led by endpoint security and security analytics, intelligence, response, and orchestration software. Hardware spending will be dominated by network security needs, including firewalls, intrusion detection and prevention, unified threat management, and virtual private networks. Both product segments are expected to recover in 2021 with year-over-year growth rates of 9.6% for hardware and 4.4% for software.

Large (500-1000 employees) and very large businesses (more than 1000 employees) will be responsible for two thirds of all security-related spending in 2020 and throughout the forecast. These two segments will also see the strongest spending growth with five-year CAGRs of 9.3% for large businesses and 8.6% for very large businesses. Medium (100-499 employees) and small businesses (10-99 employees) will spend more than $30 billion combined on security solutions this year.

From a geographic perspective, the United States will be the single largest market for security solutions with spending forecast to reach $56.4 billion in 2020. Four industries – discrete manufacturing, federal government, banking, and professional services – will account for more than $20 billion of the U.S. total. China and the United Kingdom are the next largest country markets with security spending expected to reach $7.9 billion and $7.6 billion this year.

Telecommunications and state/local government will be the industries with the largest security spending in China while banking and discrete manufacturing will be the leading industries in the UK.

INNOVISION2020
DATA CENTRE INSIGHTS + PERSPECTIVES

InnoVision: A very special issue of DCS Magazine dedicated to the data centre industry's visionary leaders and technology innovators

To herald the launch of the all-new Data Centre Solutions digital publication, we have produced a very special first issue, entitled InnoVision – providing an overview of the state of the data centre industry right now.

80+ Vendors from across the supply chain have provided their viewpoint on the future and innovation.

How will the data centre industry evolve over the coming months and years, what will be the major drivers and opportunities?

Read today

https://digitalisationworld.com/magazines

IN ASSOCIATION WITH

DATACENTRE SOLUTIONS

DIGITALISATION WORLD

PAM4: a fundamental shift for 400G networking

Four-step Pulse Amplitude Modulation (PAM4) in pluggable fibre optics is expected to be the biggest shift in networking since its introduction to the network in the last decade.

BY RAY HAGEN, GLOBAL PRODUCT LINE MANAGER AT PROLABS.

PAM4 modulation is empowering and driving the transition from 100G to 400G data rates in the data centre. Its capabilities will impact the network by reducing overall 400G upgrade costs, so it is absolutely imperative that any data centre manager or director fully understands its implications when planning for future upgrades.

PAM4 concepts for consideration

Modulation

With earlier generations of 100Gbps (Gigabit per second) or lower data rates, data centre operators did not need to concern themselves as much with modulation. Transceivers simply utilized NRZ (binary non-return to zero) formatting which ensured the interoperability between data rates and interfaces. From a technical standpoint, NRZ transmits 1 bit per waveform (0 or 1). PAM4 waveforms, by contrast, each can carry 2 bits and offer four different levels or steps, carrying 2 bits each - 00, 01, 10 or 11.

Baudrate

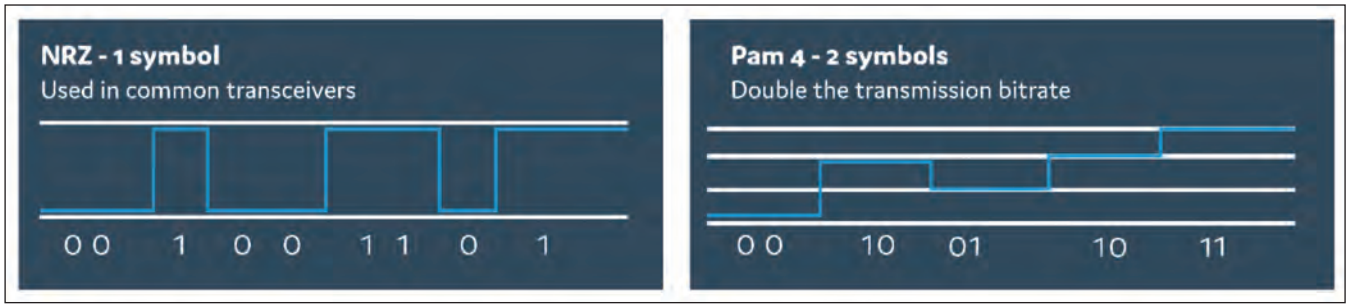
The use of the term baudrate may be a flashback to the dial-up modem era for some, yet it returns to our lexicon with the introduction of PAM4. Baudrate and bitrate were equivalent with NRZ modulated transmissions, but this is not the case with PAM4. NRZ transmissions have the same baudrate and bitrate, as one symbol can carry one bit. For example, 25Gbps bitrate is equivalent to 25GBdps (gigabaud per second) baudrate.

In comparison to this, 400G PAM4 transceivers each hand off eight 50Gbps lanes on the electrical interface to the host network element. Each of these PAM4 lanes carry a line transmission rate of 25GBdpd (25-gigabaud) at 2 bits per symbol to achieve 50Gbps per lane.

Lanes and Gear Boxes

Standard 100G QSFP28 transceivers do not transmit a single lane of 100Gbps, but instead achieve 100Gbps via four lanes of 25Gbps. Housed within the transceiver are four transmitting lasers and four receivers for optical connectivity alongside four lanes of 25Gpbs on the electrical interface.

The QSFP-DD 400G Multi-Source Agreement (MSA) designates eight lanes of 50Gbps PAM4 on the electrical side (400GAUI-8) while on the optical side, they may transmit with eight lasers of 50Gbps PAM4 or four lasers of 100Gbps PAM4. An electrical gearbox converts and re-times data between the eight electrical lanes, preparing it for transmission across four lanes of 100Gbps for 4x100G transceivers. These eight lane optical transceivers do not require a gear box for re-timing. Like baudrate, gearboxes are not new concepts and are being reintroduced for 400G applications. In the most recent designs, the gearbox is embedded into a DSP IC (Digital Signal Processor Integrated Circuit) offering additional functionalities such as equalisation. 400G QSFP-DD LR4, FR4, and LR4 transceivers each employ a gearbox to convert



and re-time between electrical and optical interfaces.

Key considerations for 400G upgrades

400G port breakout connections are used at the core to aggregate connections between multiple network elements, such as servers, storage, and other appliances, with a single top-of-rack or leaf switch port. 40G and 100G breakout connections traditionally used Direct Attached Cables (DAC), Active Optical Cables (AOC), or a parallel transceiver with a Multi-fibre Push On (MPO) interface connected to four small form-factor (SFP) type transceivers, as modulation was not a concern in these previous cycles.

Reduce upgrade expenses by deploying alongside existing 100G network elements

Legacy 100G network elements accept four lanes of 25G NRZ communication at the electrical interface. Standard 400G 4x100G breakout DAC cables split each breakout section into a 2x50G PAM4 electrical signal but do not offer a gearbox function to re-time to the 4x25G NRZ interface accepted by legacy switches. 4x100G AOCs are unfortunately expected to follow a similar path in not offering backward interoperability with legacy 100G NRZ switches.

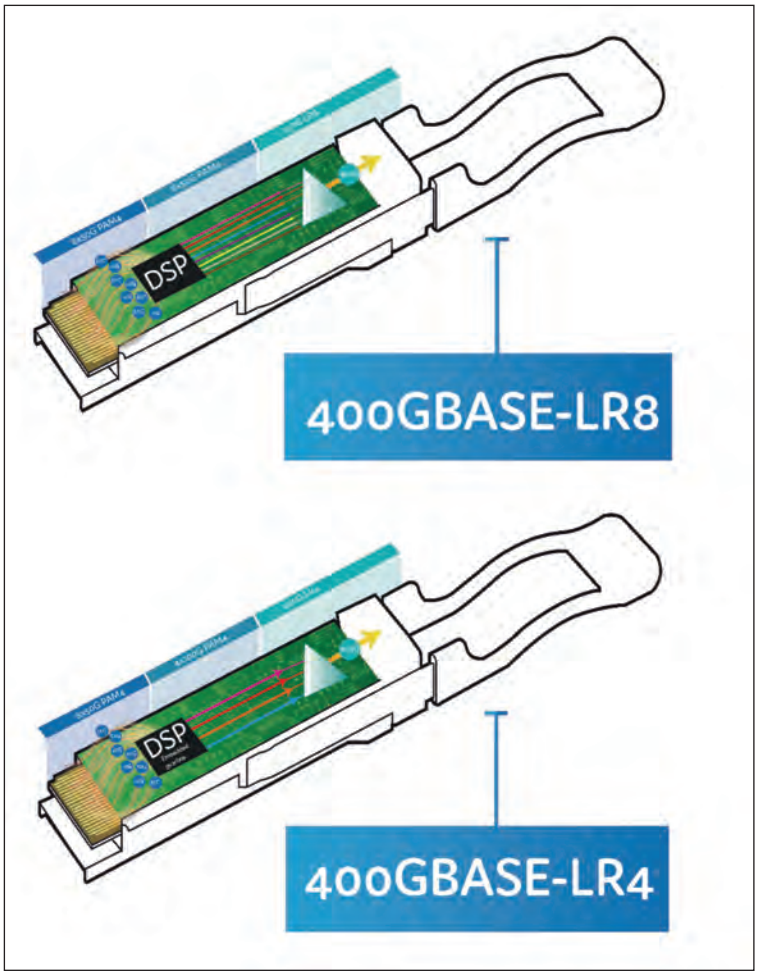
Legacy transceivers are built on four lanes of 25G NRZ formatted signalling on both the optical and electrical side. Common NRZ four lane transceivers SR4, LR4, etc. will not be interoperable with 400G transceivers in a 4x100 application.

Luckily, some transceiver-based breakout solutions offer options for interoperability with legacy gear. In particular, a new class of single lambda (single wavelength) 100G transceivers has been introduced that will support 100G PAM4 at the optical interface and 4x25G NRZ at the electrical interface. These transceivers perform the re-timing between PAM4 and NRZ modulation schemes within the transceiver gearbox.

The QSFP28 DR and FR (also referred to as DR1 and FR1) transceivers are the first transceivers of this kind and are already available. These optics are fully interoperable with not only legacy 100G network gear but also with QSFP-DD DR4 and DR4+ breakout transceivers. The QSFP-DD DR4 and DR4+ are parallel series modules, accepting an MPO-12 connector, with breakouts to LC connectors to interface with the DR or FR transceivers. DR4 to 4xDR connections are up to 500M, DR4+ to 4xFR connections are up to 2km over single-mode fibre.

The network is not ready for PAM4 but there is still a strong need to increase port density

The QSFP-DD specification used by 400G network elements does offer backward compatibility to NRZ technology. Network elements using these additional capabilities of the QSFP-DD MSA offer flexibility for



data centre operators to increase port density in comparison to legacy 100G QSFP28. 200G, 2x100G DAC and transceiver solutions are available for these use cases.

2x100G DAC cables offer a 200G, 8x25G NRZ electrical interface to a network element's QSFP-DD port. The corresponding breakout cable's terminations connect with 100G NRZ port in legacy equipment. These DAC cable applications are only practical for in-rack connections. Copper DAC cables are less complex in design and construction, making them the first products to market for this application, however in line with ever-changing demands breakout AOC cable technologies continue to be developed and are anticipated to be available on the market soon.

200G 2x100G transceivers connect with legacy NRZ transceivers at reaches of up to 10km. These transceivers act as "two transceivers in one housing" complete with two sets of Tx/Rx pairs on the faceplate of each unit.

Multiple 2x100G optical choices are available for these requirements, depending on the reach the application calls for. The short-reach option is to opt for the QSFP28-DD 2x100G SR4 which utilises a MPO-24 connector. The SR4 is capable of supporting

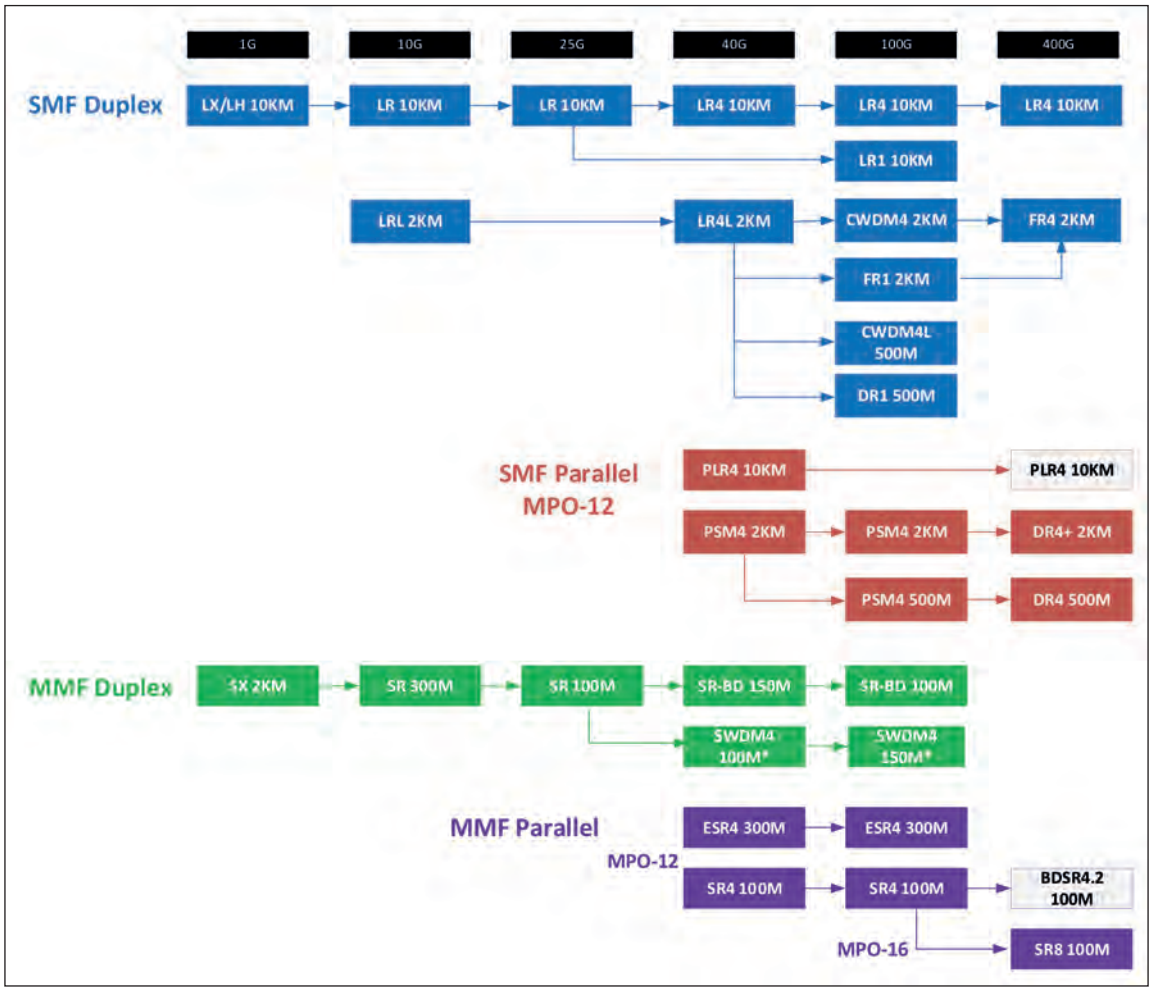


Figure 1. Roadmap of the upgrade paths between your current network and one that serves the needs of tomorrow's consumers

reaches of up to 100m multimode fibre (MMF) while doubling port density over a standard QSFP28 SR4 pluggable optic. For those needing a bit more oomph, the intermediate and long-reach alternatives are the QSFP28-DD 2x100G CWDM4, for a reach of up to 2km or theQSFP28-DD-2x100G LR4 for infrastructure reach requirements of up to 10km single-mode fibre (SMF). The LR4 transceivers leverage the use of a new high-density "CS" connector which encompasses a full Tx/Rx pair within the footprint of a single LC connector. The CS connector enables the two Tx/Rx pairs from a single transceiver.

Understanding and choosing your upgrade path

Without a doubt, multimode fibre has the largest footprint in today's data centres. However, single mode fibre is rapidly growing as a viable option for many data centre connections. The technical requirements for 100G and 400G higher data rates are pushing the capabilities of vertical-cavity surface-emitting lasers (VCSEL) that may limit the reach in comparison to previous technologies.

These practical limitations in the data centre will be raising their head when upgrading over a multimode fibre pair. 40G and 100G transceiver technologies deploy both standard-based and proprietary technologies to transmit or receive on a fibre pair. With a multitude of upgrade options available to network managers and data centre operators, it is of the utmost importance to plan as far in advance as possible. Truly understanding each upgrade path available and choosing the right one for your business can minimise or even avoid complications down the line. Switching plans mid-deployment can have major time and cost implications and should be avoided where foreseeable at all costs.

Preparing for the advancements of future data centres While PAM4's arrival to the market brings forth promising transmission methodologies that achieve the speeds and reaches that 4K video, 5G mobile, and IoT all demand, it also brings forth a host of complexities that must be carefully navigated. Taking the time to thoughtfully map out which upgrade path, and which optics within those paths, makes the most sense for your business can avoid wasted time and capital.

Whether your needs are to reduce operating expenses, increase port density, get prepared for tomorrow's bandwidth or speed needs, or even something in between, PAM4 and QSFP-DD solutions can help you win tomorrow's upgrade battles, today.

Accelerating digital transformation in the cloud

As new technologies evolve into the mainstream, creators and users look to further developments and innovations to leverage capabilities for increased value. This is what's currently happening in the cloud computing space.

BY MARK ANDERSON, SENIOR DIRECTOR OF GLOBAL SOLUTIONS ENABLEMENT EMEA, AT EQUINIX.

EUROPEAN BUSINESSES are increasingly moving their critical IT infrastructure to the cloud, to take advantage of a rapid rise in the use of remote applications, storage and management solutions. As these tools continue to develop, they have become even more critical to accommodate an exponential growth in data volumes to support businesses' needs for more agile IT solutions. The COVID-19 pandemic has only accelerated this trend, as organisations expedited a shift towards cloud-based solutions in order to thrive during companywide remote working policies. Enterprises have become more confident about and reliant on moving their valuable data to the cloud to maintain an agile and commercially relevant IT ecosystem in an increasingly interconnected and digitally empowered marketplace.

A sector in transformation

Given that cloud adoption has moved firmly into the mainstream, these strategies are only expected to

grow – with Gartner forecasting that the global public cloud services market will increase by 17% during this year alone. And the segment will continue to expand over the next few years, with investment expected to reach $354.6 billion by 2022, up from $227.8 billion in 2019.

A key driver of this growth is enterprises interconnecting to multiple cloud providers. Software as a Service (SaaS) represents the largest global market piece, and is set to increase from $99.5 billion in 2019 to a forecasted $151.1 billion by 2022. This is largely due to the scalability of subscription-based software. Gartner predicts that Cloud System Infrastructure Services (IaaS) will follow closely behind, set to reach $74.1 billion within the next two years, representing the highest growth rate year on year at 24%. This increased growth is the result of increased demand for cloud-based applications and workloads which cannot be serviced by traditional data centre setups.

As businesses become increasingly dependent on cloud technology, IT leaders recognise the need to prioritise the relocation of existing digital assets. Equinix's 2019-20 Tech Trends Survey, which explores IT decision-makers insights, revealed that nearly three quarters (71%) of global IT decision-makers will move their IT function to the cloud in the near future, compared to 68% in the UK. While two-thirds (66% globally, 59% in the UK) plan to do so within the next 12 months. This is despite nearly half (49% globally, 43% in the UK) of IT specialists perceiving possible cybersecurity risks around cloud adoption as a potential threat to their business.

Yet as businesses accelerate their own digital transformations, they will require the tools and infrastructure to help them navigate the challenges and opportunities of a post-COVID-19 world. In order to remain competitive, they must be able to connect with partners, customers and supply chains anywhere in the world with low-latency, and be able to access powerful cloud-enabled applications and analytical tools within a scalable environment.

While currently, transitioning IT services to the cloud tends to focus on new solution deployments, as edge computing enters the mainstream, more companies will be looking at multiple deployment paradigms to collect, process and store application data flows that need to be tightly connected to their cloud implementations to expedite their digital transformation. This rapid adoption is fueled by several factors including the ease of use, scalability and the need for improved security that cloud computing offers. As the world is now more dependent on a dispersed workforce, clouds allow businesses to respond more quickly to user requests and monitor analytics more effectively from anywhere in the world.

Finding a solution that fits

As enterprises continue to march towards the cloud, they have several cloud architectures to choose from. Cloud service providers often have different areas of expertise – some companies using a single cloud provider may find that their needs are met in some sectors while they are under-serviced in others. Multicloud solutions, offer businesses the flexibility of picking and choosing the cloud providers that they want to have access to. Enterprises then have the advantage of tailoring their cloud architecture to meet their business requirements. Multicloud architectures can also help bolster cyber security, as a robust multicloud strategy helps reduce the risk of cyber-attacks, given that the cloud services are not housed in a single location.

Hybrid cloud is another option to help enterprises gain a competitive edge – as businesses seek to become more agile, in rearchitecting their clouds to

allow them increased flexibility in moving frequently used workloads to and from public clouds while still keeping archived data in a private cloud. The shift to a hybrid cloud environment can offer more flexibility to meet data regulation and data sovereignty requirements than a 100% migration to the cloud, by providing an optimised combination of private cloud and public cloud and on-premises infrastructures. Both hybrid and multicloud architectures allow companies to easily scale up their digital capabilities as and when required – which is especially helpful when expanding into new markets or territories. This also means that organisations can also scale back at a click of a button. This flexibility will prove even more advantageous as businesses deal with a fluctuating market and increased digital demands over the next 12 months.

Today it is not uncommon for enterprises to participate in one or more digital platforms as an owner, producer, partner or consumer – which makes the case for a hybrid multicloud solution even more compelling. For example, a business may play multiple roles, purchasing from one platform and selling on another. However, it may lack the ability or capacity to tie all of those different environments and players together with direct, secure connectivity for optimal application performance and data protection.

A hybrid multicloud strategy can help solve that challenge by placing on-premises critical applications and information resources in close proximity to cloud workloads.

While many businesses have significant ambitions to embrace more multicloud strategies, adoption remains low. Less than one in five (17% globally, 14% in the UK) of IT decision-makers surveyed for Equinix's 2019-20 Tech Trends Survey said their business was currently deploying across multiple clouds.

A scalable solution

As more organisations move beyond their initial fears of entrusting sensitive data to third parties – to relocate both critical and noncritical data workloads to the cloud – cloud technologies will only continue to grow along with the need for interconnection bandwidth. Equinix's Global Interconnection Index Vol. 3 highlights that interconnection bandwidth in Europe is predicted to increase annually by 51% (CAGR), representing 22% of total global capacity. The report underscores that cloud and IT services will remain one of the largest industry segment users of interconnection bandwidth in the region, expected to reach 418 Tbps by 2022.

Services like Equinix Cloud Exchange Fabric® allow companies to interconnect with multiple cloud providers directly, connect those clouds privately to hybrid infrastructure deployments in co-location and to connect to their other business processing locations and those of their partners and suppliers; dramatically lowering the risks posed by the public internet. By using direct interconnection strategies to optimise cloud migration, enterprises decrease the likelihood of a cyber breach and ensure sensitive data is stored safely. The strategy also increases the performance of backup and recovery processes over private, high-speed, low-latency connections and allows businesses with a global footprint to access workloads from anywhere in the world.

As the cloud services landscape becomes increasingly sophisticated the global shift towards hybrid and multicloud deployments shows no sign of stopping, as more enterprises reap the business rewards of adopting a cloud-based infrastructure to deliver scalable solutions, accessible from dispersed locations. Investment in cloud-based solutions will continue to rise as businesses seek to be more agile, flexible and digitally competitive in an interconnected world.

AIOPS SOLUTIONS ONLINE SUMMIT

ENABLING APPLICATION OPTIMISATION

The importance of proactive performance monitoring and analysis in an increasingly complex IT landscape.

29 October 2020

aiopssolutions.com

The answer to a successful multi-cloud strategy lies in the network

Digital transformation entails many technologies, but cloud adoption sits chiefly among them. As organisations have adjusted to a highly distributed workforce in the wake of COVID-19, the importance of cloud has increased significantly, becoming an integral component of company operations to ensure business continuity.

BY NAV CHANDER, SENIOR DIRECTOR, SERVICE AND CLOUD PROVIDER MARKETING AT SILVER PEAK

EVIDENCING this new reliance on cloud, Gartner projects that the Desktop-as-a-Service (DaaS) sector will experience vast growth in 2020. Fuelled by the remote working situation, worldwide spending is expected to increase by 95 per cent year on year to $1.2bn1, up from $616m in 2019. Given the importance of cloud, many organisations are now adopting multi-cloud strategies to leverage multiple cloud platforms to support an expanding range of Software-as-a-Service (SaaS) and corporate workloads, each with unique performance and service level requirements.

With so much relying on the power of the cloud now, businesses need to know they're achieving a multiplier effect from their cloud investments. Picking

and choosing which provider to use for which service, based on that provider's particular strong suits across the different aspects of the cloud environment, is a natural move to ensuring businesses are getting the most from their money.

For instance, a company may be looking for the Google Cloud Platform's strength in machine learning or Microsoft Azure's seamless integration with Office 365 and Microsoft databases – each platform has its advantages, so why not use each where it is best suited. However, it's not simply a matter of putting various cloud services and applications into a variety of different baskets. Essential to the success in guaranteeing optimisation and return on investment while adopting multi-cloud strategies lies in several variables, but the most important of these is arguably the underlying network infrastructure upon which the cloud is supported.

Cloud demands advance beyond the capacity of legacy infrastructures

As a result of the accelerating adoption of cloud and multi-cloud strategies, enterprises are experiencing additional demands being placed upon their wide area network (WAN) infrastructure. However, many companies still rely on traditional, router-centric WAN approaches that are increasingly becoming outmoded. Indeed, in the face of multi-cloud strategies, even basic SD-WAN solutions struggle to cope.

These WAN solutions were never designed for the cloud era and can force compromises on organisations when it comes to choosing which cloud strategies to employ. Fundamentally, this is because network traffic patterns have shifted dramatically since the inception of cloud. Applications are more demanding upon the network, and security needs are of a greater importance now that everything is open and connected to cloud, increasing the potential attack surface.

Traditional, router-centric networks send all traffic from branch offices on a circuitous route back to the data centre instead of straight to DaaS, SaaS and Infrastructure-as-a-Service (IaaS) applications and instances. The requirement to backhaul is due either to an inflexible architecture and/or security requirements that dictate advanced inspection that conventional routers lack the ability to perform.

This long-winded path, sometimes called the trombone effect, adds significant latency when connecting user to cloud applications and can cause significant impairment to performance and business productivity. Before the pandemic, this may have represented nothing more than an inconvenience, but with remote workforces now highly dependent on the cloud, these issues can cause significant disruption to company operations.

First and foremost, enterprises are seeking a means to assure optimal application availability and reliability, so that even if one WAN transport service experiences an outage, applications will remain available by failing over to the remaining service

To better enable the practice of multi-cloud strategies, it falls upon advanced software-defined WAN (SD-WAN) networking solutions to provide the best in service option as networking infrastructure to support complicated cloud demands. SD-WAN technology enables enterprises to connect users directly to applications by using any underlying transport option available on the network. This might take the form of broadband internet, multiprotocol label switching (MPLS), or even 4G and 5G.

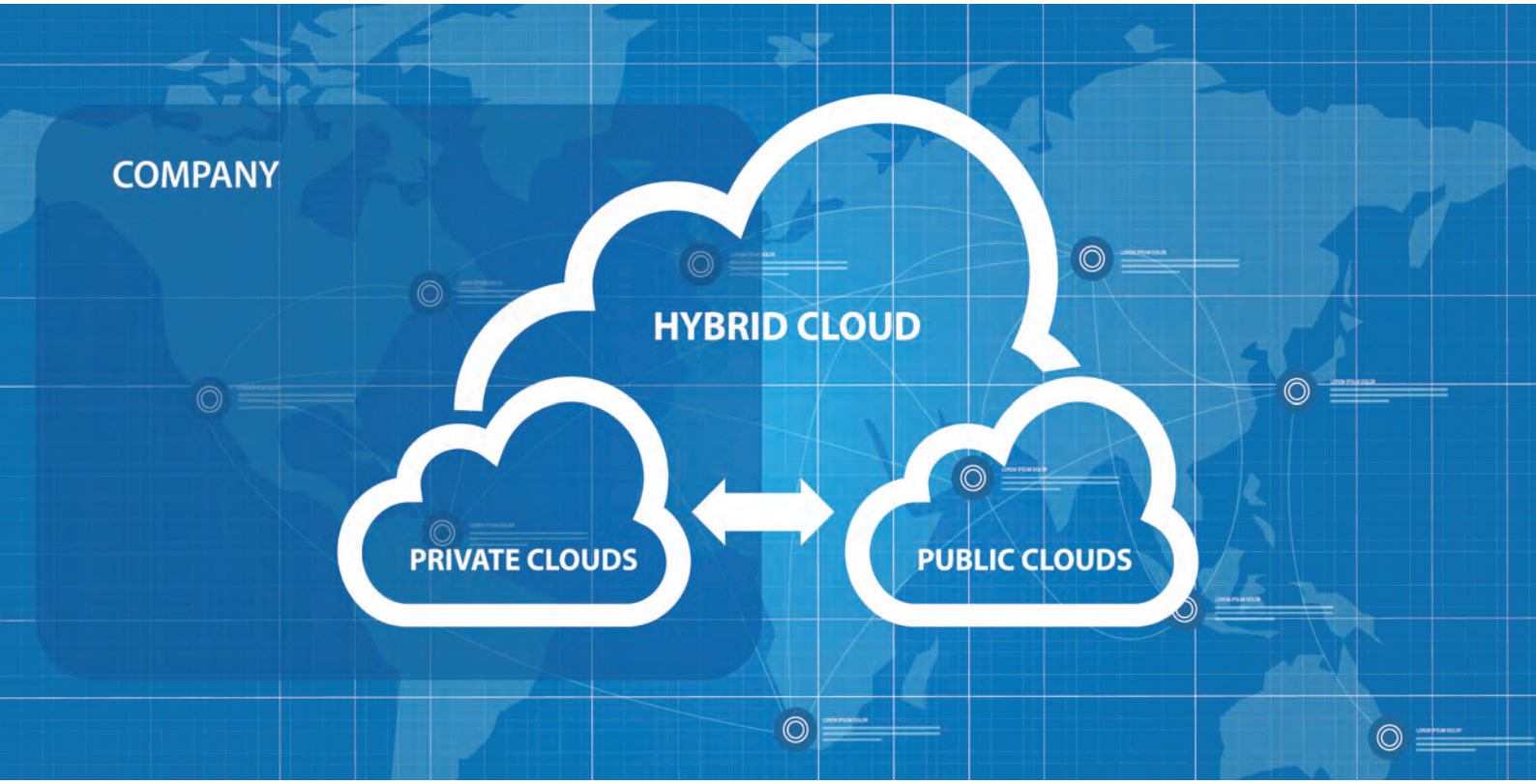
SD-WAN solutions offer an alternative to router-centric infrastructure as it increasingly slides into redundancy; however, not all solutions are best-suited to supporting multi-cloud environments and there are a number of criteria that have to be met to optimise its benefits.

Guaranteeing multi-cloud strategies

When selecting an SD-WAN solution to deliver on the promises of multi-cloud, enterprises must ensure that cloud-hosted applications can perform well over any underlying network, without compromising end user experience. Before examining the SD-WAN requirements in supporting multi-cloud, it is important to identify the key drivers as to why organisations put multi-cloud in place, as there are the ambitions that need to be fulfilled.

First and foremost, enterprises are seeking a means to assure optimal application availability and reliability, so that even if one WAN transport service experiences an outage, applications will remain available by failing over to the remaining service.

Following this insurance in maintaining operations, enterprises are seeking to support regulatory and compliance requirements, thereby allowing



organisations to maintain the integrity of application data in a specific geographic region in accordance with local legal mandates. This is especially important for large enterprises whose operations span worldwide jurisdictions.

Lastly, in adopting multi-cloud strategies, enterprises are looking to reduce IT spend on IT infrastructure CAPEX and to increase agility to on-board and connect enterprise users to new applications. And through automation and centralised management, IT organisations can shift their focus from network maintenance toward the deployment of new cloud applications and services.

The answer to multi-cloud lies in a business-driven SD-WAN

Not all SD-WAN solutions can fulfil the criteria to meet the ambitions that lead enterprises to adopt multi-cloud strategies. The answer to optimised multi-cloud lies in a "business-driven" SD-WAN solution – WAN infrastructure that acts as an enabler to the company, rather than a constraint.

In the context of multi-cloud, this means the WAN must ensure that end users accessing cloud applications always have an excellent, consistent quality of experience whether they are working from a remote office, branch or corporate campus site.
To ensure this, there are three key SD-WAN platform requirements that enable IT to realise their multi-cloud deployment objectives and support their end users' ability to access these multi-cloud applications directly and securely.

First, the SD-WAN platform must automate branch-multi-cloud connectivity to scale applications horizontally across multiple cloud providers with the flexibility to select the best cloud provider for the right application.

Second, the platform must also be able to identify and assure the consistent performance of business applications by applying granular quality of service (QoS) and security policies based on the end user and group profiles prioritised by application.

These two provisions allow for the smooth running of business-critical applications across the multi-cloud upon which company operations depend. Thirdly, to truly guarantee multi-cloud performance, these technological criteria must be met in conjunction with the ability to support applications across the leading public cloud providers.

Looking towards a multi-cloud future

The pandemic has accelerated the adoption of multi-cloud strategies, but this trend was well underway even before the turn of the year. Such technology offers soaring promises of digital transformation and the option to use the best cloud service when and where it is required.

However, as cloud adoption itself increases demand on the network, this is even more so the case for multi-cloud. If companies want to truly make the most of the cloud and all it has to offer, their first target lies in employing a business-driven SD-WAN.

DIGITAL CHANGE MANAGEMENT SUMMIT

25.11 2020

www.dcmsummit.com

How Managed Service Providers and Cloud Service Providers can help SMEs on the road to digital transformation

A unique online event to connect MSPs, VARs and System Integrators with their target market

Hybrid cloud adoption: Getting migration ready

Hybrid cloud is a popular solution among enterprise grade businesses, but it is not a one size fits all solution. The building blocks of this model are complex and potentially costly to manage. This article will examine the core challenges and provide a blueprint to enable decision makers and IT leaders better manage the challenges they will likely face.

BY IAN SHEEN, TECHNICAL LEAD - STRATEGY AND TRANSFORMATION, TELSTRA PURPLE.

The Challenges

Workload destinations and migration

Workloads differ across companies, teams and employees. Taking a holistic view of each critical workloads supported by a hybrid solution is paramount to building a solid network structure. Map out each of the end needs and work backwards from there, to ensure the system works clearly and effectively for all.

Skill and expertise

Securing the right talent will enable organisations to take full advantage of Hybrid Cloud and continually adapt to the innovations taking place within the cloud environment. The pace of innovation within cloud architecture is lightning quick, requiring time, money and an agile mindset to keep up with these new technologies. This is further exacerbated when migrating to Hybrid Cloud, as public and private cloud require different expertise and skills, with prospective employees being in high demand.

Security and compliance

Compliance is not a one-off activity; it needs continuous oversight to ensure industry-specific standards, government policies and internal protocols. The factors are not constant so neither should be the approach to Hybrid Cloud. It's crucial to identify and seek or hire expert advice, to guarantee compliance within the various policies and protocols without impacting the agility and flexibility of a Hybrid Cloud platform.

Network performance

Businesses that have not prepared their networks to handle the migration to Digital and Cloud will likely experience unreliable connections. Cloud solutions are network intensive, so it is vital that businesses plan adequately when preparing for migration. Failure to do so will result in an unstable and inflexible network that is unable to keep up with the cloud solution.

Data fragmentation and governance

Hybrid Cloud utilises multiple cloud networks which in turn disperse data across numerous environments across different regions. In doing so, data is siloed, scattered and copied all over the place, which can lead to an incomplete view and an inability to extract real value from it. This results in data being fragmented, reducing performance and impacting capacity due to inefficient use.

It is important for enterprises to have a robust data strategy that compensates for fragmentation and ensures full visibility of the data, wherever it sits in the organisation. Organisations that are unsure of where their data is or how to access it risk compliance issues, eroding the advantages of Hybrid Cloud.

Hybrid Cloud adoption blueprint

Preparing for migration

Preparation and planning are key to a successful Hybrid Cloud migration strategy. Business leaders should first address the following questions when building their strategy:

- How do I protect my data? How do I connect to the cloud so that my data is safe?
- What are the implications and impact to my processes and users by moving to the cloud?
- Where should my data and each of my applications reside?
- How does my solution scale?
- Which workloads should be serviced by SaaS?

For many organisations, these questions boil down to whether the migration is being completed in-house or being outsourced. For in-house options, businesses must ensure they have the capabilities and skills within their teams, and that they can afford to have those individuals be taken away from their day-to-day activities. If an organisation chooses to outsource, they must be diligent in seeking out experts who understand their business and have access to the right experience. This will ensure providers offer the right solutions and manage the transformation process successfully.

Making the network hybrid ready

Building a robust network to handle the increased workload without sacrificing connectivity is vital. Software-defined networking is well-suited for this, and offers the requisite foundation for a network hosting hybrid cloud solutions. Software-defined networking offers enterprise-grade connectivity through an on-demand model that is as agile as the cloud. The building blocks offered by this method can be combined and deployed virtually to deliver robust, high-capacity connectivity to cloud and data centre locations globally. The 'pay as you use' commercial model enables great flexibility and a virtual eco-system that can respond to changing needs, daily or hourly if required.

Improving governance, performance and security
Visibility of cloud usage and application performance across the business is vital to reducing risk, while still powering agility and innovation. IT teams can provide the right IaaS to achieve this, if they are supported by the right architecture and services, as well as flexible and secure networking. This will ease monthly planning and security management, whilst assisting in the analysis of cost trends.

For outsourcing models, a fully managed service can take care of governance and compliance, including essential security activities. This approach reduces the burden of day-to-day management whilst boosting assured performance and service availability through monitoring and maintenance. The best managed solutions will have strong automation elements to simplify common tasks and ensure compliance scales as easily and quickly as the cloud does.

Understanding your applications and service flows
Business functions often comprise multiple applications and flows. A key element of any future cloud strategy is understanding the interdependencies between them, as these will become more complex in the hybrid world. Components that used to reside in a common control plain within a private enterprise can be straddled across multiple tiers in a hybrid architecture. Communication flows can become more complex, so an enterprise is best served by understanding the big picture before introducing the new layers of control that a Hybrid model dictates.

Maximising your data agility

Data powers innovation, businesses and decision makers, marking it as highly valuable intellectual property for organisations. However, issues arise when storage limits are reached and when moving data from one location (or provider) to another. These are complex tasks that increase the chances of data leaks if not managed and provisioned for appropriately. Visibility is key to ensure access and security of our data across multiple cloud environments. By locating centralised data storage near major cloud services and linking them with high-speed connections, businesses will benefit from high performance and low latency while keeping their data in secured facilities. Additionally, it provides increased flexibility by letting enterprises migrate data between different storage levels without impacting performance.

Final word

Hybrid Cloud continues to be a popular choice among enterprises, with its ability to offer high performance, flexibility and agility in a constantly evolving environment. As a result, user expectations, business requirements and data regulation will only become more complex, which in turn will lead to more challenges and pitfalls when approaching hybrid solutions.

In summary, there is no one-size-fits-all model of cloud for businesses. There are nuances and restrictions that affect everyone differently. However, there are strong and adaptable models that can be quickly and efficiently adapted to fit individual needs – but it is vital to fully understand what those needs are and where they sit within the business. Set realistic targets and deadlines and invest in the right technology and solutions. Business and ways of working are no longer rigid; the technology use, just like the strategy one employs, must be flexible, agile and scalable. It is vital organisations plan to ensure they have the right skills, expertise and architectures in place to avoid potential challenges and get the most out of their cloud deployment.

Negotiating the continued investment in digital transformation

Even before COVID-19, digital transformation was one of the top priorities for every organisation.

BY ASH FINNEGAN, DIGITAL TRANSFORMATION OFFICER, CONGA.

AS AN INITIATIVE, it is very much about establishing a pro-data ecosystem and better protecting one's assets. With the appropriate tools and systems in place, it can provide absolute clarity for businesses as everyday operations are effectively streamlined and each department has access to the information they need at any given time.

Now, as the catalyst of great change, the coronavirus is the most unplanned reason digital transformation is accelerating for many organisations – with the primary concern being how to transform digitally, and how to do it fast. However, these are short-term solutions that have likely been forced out of necessity and will lack the foresight of a well-planned and carefully implemented transformation programme. In fact, Conga research shows only 50 percent of initiatives are reported to be somewhat successful[1]. Long term strategies that reconsider the current business process, prioritise data and produce real actionable insight are key.

However, given the current economic volatility – where change is not a choice, the outcome is still unknown and there is no set timeline for our return to normality – and the UK officially entering a recession, many boards and IT departments will be tightening their purse strings and reluctant to make any serious, long-term investments at this time. However, it is the responsibility of senior leaders to convince their teams and the board otherwise. As organisations navigate the current pandemic, it is imperative that businesses continue to streamline processes and reconsider their current systems or methods of working. Digital

transformation is not only a step to guaranteeing a business's survival but enabling it to continue to thrive after this crisis. These strategies are more vital than ever – what organisations do now will impact how well they perform later. Whilst the continued investment in these technologies may seem daunting, business leaders must create an insight-driven digital transformation programme to future-proof their organisation for all outcomes.

'Selling' the strategy to the board – the importance of investing in DX

The best way to sell these investments to the board is to highlight the return on investment (ROI). While digital transformation initiatives may come at an initial cost, they can dramatically increase revenue and operational efficiency. For example, streamlining contract processes enable companies to speed up the contract creation time, which not only means the workforce has more time to concentrate on generating more leads, but it also means deals will be sealed faster. In fact, companies have the ability to reduce content creation or renewal time from weeks to days. There is also the cost to the business of not being digital – especially in times like these where the large majority of employees are working remotely. Digital transformation technologies enable the business to continue operating to the same standard as it was prior to the pandemic. For example, employees can continue to negotiate contracts without having to leave home and capture a record of all negotiations and redlines automatically in its system of record. Once contracts have been fully negotiated and are ready for signature, electronic signature technology means there's no need to rely on signing in person or mailing paper documents.

In addition, business leaders should be aware of the risk element of not continuing with their digital transformation initiatives, such as the cost of human error to the business, or even the cost of lack of visibility when it comes to storing data, handling contracts or even renewals. Indeed, with legal teams operating remotely, they might not have full visibility or access to all contracts, which exposes the business to great risk and possible compliance issues. Ensuring all are onboard – gaining support from IT management

It will also be difficult for IT management to convince workers to adopt the new technologies – especially since they have been working remotely for some time. While companies will have invested a lot in digital transformation technologies, without properly training their workforces, their employees will likely develop bad habits in their remote working environment, and the investment could end up being futile. Organisations must ensure that they run regular remote training sessions, troubleshooting and answering any questions that their workforce might have about the technology. Only through complete transparency and by instilling positive behaviour can leaders ensure all teams are onboard from the start of the programme.

Likewise, IT management teams need to consider the benefits of an adept transformation programme – streamlining the business process ensures efficiency and removes bottlenecks, lowers the chances of error and potentially, costly fines. With the move to more flexible working, security, privacy and compliance are high on the agenda, effective data management is critical. It is vital that businesses ensure their data is protected with the appropriate cloud services and protection in place. Whether it is incorrectly processing data, or failing to block virus or malware behaviour, these security issues could jeopardise the integrity of an organisation. Only through an effective data-led strategy, can leaders account for all outcomes.

A successful strategy: creating actionable insight

Every major player knows the future is data and, given the pandemic, organisations have quickly realised the importance of properly structuring data and insights – it is an assured way of improving the overall performance of their business. Whilst the majority of businesses (97 percent) already have a digital transformation strategy in place, it is imperative that companies continue with their transformation efforts, that is, continuing to evolve and adapt their strategy[2]. Now more than ever, it is important for organisations to review their business and simplify the process. The best solution is the one that streamlines business operations and provides total transparency across all areas of the organisation. In short, a successful digital transformation project starts with a clear strategy and ends with the successful adoption of technology which enables businesses to accelerate and thrive.

For any business pursuing a new digital transformation project, it is important to think of it not as a 'COVID-19 digital transformation plan,' but as a long term strategy plan that stabilises and safeguards the business for the future. This will require embracing technology that ensures workforces are able to operate more efficiently, from anywhere, at any time. Such a crisis has highlighted the reality of failing fast, but the need to innovate faster. It is important that businesses continue with their transformation efforts, but ultimately, reconsider their current systems or methods of working. Senior leaders must take charge and promote a data-led initiative with the full support of the board and their wider workforce.

Reference

1. https://conga.com/state-of-digital-document-transformation?utm_medium=press-release&utm_source=business-wire&utm_campaign=research&utm_content=state-of-ddx

2. https://conga.com/state-of-digital-document-transformation?utm_medium=press-release&utm_source=business-wire&utm_campaign=research&utm_content=state-of-ddx

Why apps must WOW users

Mobile apps are an essential part of our daily lives - be it for news, weather, health, fitness, travel, directions – you name it from the moment we wake up to the moment we go to bed, apps form part of our everyday routine and we rely heavily on them. But this really highlights the challenge that businesses face in developing compelling and engaging apps that users want to interact with.

BY GERRY TOMBS, CEO, CLEARVISION.

FUNDAMENTALLY, for an app to succeed, it must act as an extension of the user, augmenting their lives, solving their problems in new ways, and delivering such a seamlessly brilliant experience that they turn to it repeatedly until it becomes valued as an essential part of their lives.

This kind of user engagement is commercial gold and is what companies are seeking as they compete to gain customer loyalty and streamline business processes. So why is experience so critical in today's market and how can businesses deliver enterprise grade apps that have the experience users are looking for?

Millennials and Generation Z

By 2025, millennials will make up 75 percent of the active working population, with Gen Z hot on their heels[1]. These true digital natives have matured in an always-on, instant access mobile culture. Not for them queuing at the post office or the bank, or indeed, queuing anywhere. Whether in a role as consumers, or as employees, they demand that apps live up to their high expectations before they become long-term members of their digital application ecosystems.

They build that ecosystem based on companies that offer the service that fits in with their omnichannel lives, enabling them to multitask life-changing decisions such as getting a mortgage with the mundanity of grocery shopping. And if one brand can handle both, even better!

Customers and employees are looking for brilliant experiences and loyalty is quickly transferred to the app that can deliver "wow" moments. This makes creating slick, smart, and creative apps mission-critical to businesses that want

to compete for digital mindshare and break into the trusted application ecosystem of the user.

An app that fails to meet the user's expectations is just that: a failure. Organisations risk wasting valuable investment and development time if they can't get into the experience mindset that creates apps that truly are an extension of the user.

Getting into the mindset of your users

So, how do you get into that mindset?
A really good example is something that Zurich UK did, using the technology of our low-code partner, Mendix. Zurich wanted to investigate new ways to promote life insurance adoption across the UK market, and recognised that people were put off from buying life cover because they thought it was unaffordable and perhaps a luxury. To challenge that view, Zurich developed a selfie app. They came up with the novel idea of FaceQuote, a frictionless, first-to-market application that provides prospective life insurance customers by soliciting a selfie, estimating the user's age, and calculating a monthly premium based on this estimated age.

The FaceQuote App consists of only two pages, providing a simple, nearly instantaneous idea of what life insurance would cost a typical customer. The user's selfie is sent by FaceQuote to an image processing intelligence that provides an educated guess of the user's age with just one click. The estimated age then drives an estimate of a life insurance premium for the user.

I give this example because it is the very definition of a brilliant digital experience, in this case made possible by low-code – it's an app that works perfectly for the end user and helps the organisation meet an important business goal.

Apps that work anytime, anywhere, any environment
Although we develop apps in solid network environments with full connectivity, the real world just isn't like that. An app that is truly appreciated by a user will get spun up in any situation, and it needs to deliver value no matter how bad the connection or even when there's no connection at all. Here at Clearvision we understand that if we can't provide users with a fully functional app at any time or at least a clever and fun way to interact with the app while offline or when experiencing network limitations, we aren't delivering well. And that's why I think that more than ever, user experience experts and mobile developers must be aware of how important offline synchronisation and network management are in achieving the best technical solution without compromising a great user experience.

Put simply, the experience needs to deliver, even when the network doesn't. That's why testing in all kinds of less-than-ideal scenarios and prioritising mobile design and functionality at every stage are key.

The FaceQuote App consists of only two pages, providing a simple, nearly instantaneous idea of what life insurance would cost a typical customer. The user's selfie is sent by FaceQuote to an image processing intelligence that provides an educated guess of the user's age with just one click. The estimated age then drives an estimate of a life insurance premium for the user

It's the only way the app will win its way into the user ecosystem.

Where thinkers become makers

When we're talking about app development, the usual tale is of speed: rushing headlong to get apps out the door under pressure from business units or competitors. However, when trying to deliver a brilliant experience, it is well worth regularly taking the time to step back and check that you're still heading in the right direction. That's the beauty of low code – it actually frees up time to make sure that the app is delivering on criteria such as usability, creativity, and those "wow" moments. Because technical debt is lower with low code, there's no fear of change; on the contrary, continuous change is positive and prolongs the lifespan of that app. We keep adding value to the app instead of retiring it, so those previous investments are never lost.

In today's world, user experience is a key battlefield for businesses trying to win hearts and minds. Earning a place in the user's app ecosystem is the ultimate prize, so the pressure is on to deliver experiences so brilliant that they unquestionably enhance the user's life. Understanding user stories and how they can be changed, delivering a seamless mobile experience and taking time to create an intuitive, innovative product are all cornerstones of delivering brilliant digital experiences that permit the app to become "part of us.".

Is Kubernetes the kale diet of the enterprise world?

When kale first became synonymous with healthy eating, consumers rushed to buy kilos of it. However, without other ingredients or the right recipe what ends up on the plate can be pretty underwhelming, and in some cases plain inedible.

BY BAS LEMMENS, VP AND GENERAL MANAGER VMWARE TANZU.

IT'S NO COINCIDENCE then, that a bag of kale is the first thing to pop into my head when I think about Kubernetes – a recent craze within the tech industry: Container technology was once the domain of developers. Now, IT operations are taking control, and Kubernetes is out in front.

According to VMware's The State of Kubernetes 2020 report, although it's early days for enterprise adoption – more than half of respondents (57%) operate fewer than 10 Kubernetes clusters, and 60% run less than half of containerised workloads on Kubernetes – momentum is increasing. Spending on containers is up too, with one in four enterprises now allocating more than $250,000 a year on these technologies.

Let's talk more about Kale

As the adoption of Kubernetes moves beyond the experimental phase, it's imperative for IT teams to be fully aware of the value added by adoption, before investing millions in container technologies. This can be likened to the hype surrounding superfoods – such as kale. Kubernetes is often seen as a 'fix all problems' product with massive potential. Similar to super foods though, such as kale, it's about how you use it that really counts.

It's important for IT teams not to rush into buying kilos of Kubernetes – assuming naively it's the only solution for achieving agility, positive customer experience and innovation. Defining business outcomes before investing time, energy and money is the best approach to maximise investments.

A secret formula

It requires more than just Kubernetes to achieve business outcomes. Hype surrounds the technology and term Kubernetes. A lot of false expectations exist too. Some companies may have heard on the IT grapevine that Google, AWS, Netflix, and Microsoft bet on Docker as a container format and Kubernetes as the orchestration engine – that the technology can scale and provide infrastructure at the same level as the big players. Simultaneously they may not be aware that the whole business model of such companies focuses on making infrastructure fluid and immediately available. Regular customers have a very different business model, with solutions based on

trusted platforms by trusted partners that have solved virtualisation in the past, and those partners now have solutions to achieve the same outcomes with containerisation.

Of course, Kubernetes technology also has its benefits. Businesses can become more efficient in their use of IT and achieve better results, faster, from development life cycles. They'll produce better software because via more automation and standardisation. Organisation can then use software to explore new business opportunities, experiment with the best ways to profit from ideas, and evolve accordingly. In contrast, a 'non-K competitor' will have a harder time evolving software quickly, and the software supply chain will become a bottleneck for helpful ideas they have.

The right recipe for Kubernetes

Kubernetes is still a maturing technology which needs a degree of handholding to ensure successful deployment. It's useful to build efficient platforms, because it can be extended, and gives good abstractions to interact with containers, scheduling them in an efficient way. But if you think you can simply install it and be productive, you'll find yourself on a rocky road. You have to train and enable teams. Everything is different in Kubernetes, starting from the declarative definition of how you want your systems to be run, to the way you enable logging and routing on pods.

To make things easier, organisations may want to look at certain tools and existing systems that reduce complexity overall, rather than jump on every bandwagon that, in an architectural context, only adds complexity to an already complex world.

Once large organisations switch over to a cloud native platform, developers can get more productive and create more sustainable streams of software updates. This means that these organisations can start to explore new features and approaches to solving business problems with software, every week. While a week's worth of code might seem small, it adds up over time to major changes. Best of all, because organisations are testing features out with real-world feedback, changes are validated with data: software is only getting better.

Cloud native platforms like Tanzu Application Service and Tanzu Kubernetes Grid help out here because they put in place self-service options for development teams and standardise how infrastructure is created and managed. This not only removes a tremendous amount of time-consuming manual work, but also leads to better production resilience and security, because developers can follow a set path and it's harder to deviate from best practice.

The ultimate beneficiaries of Kubernetes

Developers get the most tangible benefits from Kubernetes. According to VMware's aforementioned Kubernetes 2020 report, the top two benefits are improved resource utilisation (56%), and shortened software development cycles (53%). Instead of waiting weeks or months for the simple infrastructure needed, let alone complex clouds to run applications in, developers can now get those environments quickly and through self-service.

Operations equally benefit. Less time is spent on mundane tasks, and production is stable and reliable. Once business teams know how to take advantage of a weekly release cycle to test new features, they benefit as well by getting a fast time-to-market, and a tool to evolve the business with validated data.

There are many traditional ways to design and run software. This variability adds extra expense, time, and risk to the software process – as years of over-budget, over-schedule, and under-featured software shows. Adopting Kubernetes technology may well be the right way forward for your company – just like incorporating kale into your diet may be better for your health.

Kubernetes puts in place one way to design and run software, removing waste for you to focus on the actual software, eradicating the hassle of managing it whilst worrying about ever-extending timelines.

Is UiPath's hyperautomation just hype without the automation?

As the business world attempts to keep pace with the exponential march of technology, and in general continues to fall well behind, there are nonetheless several interesting market signals indicating that things are about to change.

BY DAVID POOLE, CEO OF EMERGENCE PARTNERS.

UI PATH'S latest seeding round, announced recently, is a serious signal of intent, with CEO Daniel Dines pledging to "bring automation to one billion citizen developers." The robotic process automation (RPA) market is taking the digital world by storm, with at least one unicorn and a growing number of products, services and addons developing in a rapidly growing sector. Large corporations are queuing up to buy these tools, and there are already thousands of consultants designing and implementing process improvements - and yet, there remains huge frustration and strangled potential. Even today, after six years of mainstream exposure, Gartner estimates that 95% of the buyers of RPA systems have only implemented up to five bots. Thus far, the hyperautomation story has arguably consisted of plenty of hype, without the automation to match.

A similar pattern is emerging in the low-code/no-code (LCNC) market. LCNC means that apps that used to take months or even years to build can now be configured, tested, adjusted, connected and launched in as little as a few days, by citizen developers who possess an acute knowledge of the business. This has been touted as the next big thing for years, with multiple very large companies from Microsoft to Salesforce to PegaSystems - plus a whole bunch of the good, the bad and the ugly other providers - all developing products. But once again, take up has been slow. As recently as 2018, Forrester found that only 23% of 3,228 developers surveyed worldwide were using low-code. Nonetheless, Gartner predicts that low-code application development will be responsible for more than 65% of application development activity by 2024.

RPA and LCNC have a few things in common which make their potential for disrupting the whole software and technology sector huge:
1. They are both generic tools that can be used in almost any kind of business, from any sector, and can enable rapid and transformational change.
2. They are both democratising the enterprise-grade creation of new business systems, moving away from the traditional development models that have for decades been the domain of the IT department.

These technologies will be integral to the full realisation of hyperautomation, which tops Gartner's list of 10 strategic technology trends for 2020. Hyperautomation promises to seamlessly combine multiple technologies and human intelligence into an interoperable system of automation - but as demonstrated by the long gestation periods of RPA and LCNC, this will be far from an overnight sensation. Hyperautomation is following the path of exponential technologies

Daniel Dines at UiPath predicts that soon, more or less every worker will have a bot on their desk. Despite the frustrating start, this looks to be a distinct possibility. UiPath's strategy - intuitive user interfaces and democratised automation tools to unleash the potential of people – is absolutely on the right track to deliver on hyperautomation ambitions.
RPA and generic automation tools in general are exhibiting the behaviour of exponential technologies. Much like solar power, digital photography, exponential technologies, they suffer in the near term from the effects of what is known as Amara's Law. This states that: "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."

As these technologies emerge, they tend to disappoint for some time, and initially fail to deliver on their potential while the markets work out the best way to extract their value, innovate new products, imagine new pricing models, refine use case implementation approaches, and build ecosystems. These slow beginnings are something of a rite of passage before the full force of scaled-up exponential growth

can be felt. As I wrote recently in Data Economy, organisations must think long-term and not be afraid to undergo periods of underwhelming results during this experimental phase of the business lifecycle. The results in the long-term are astonishing; in one such example, solar power has grown 48x over the last 11 years in the US after a slow start.

Adopters must value the strategic over the incremental
As the RPA market finally begins to reach maturation, there are lessons we can learn from its stunted growth over the past decade - particularly since low-code/no-code is in the earlier stages of a similar journey.

According to KPMG, nine out of ten enterprise adopters of RPA failed to get past piecemeal projects and pilots to achieve proper scale. Traditional operating models have been focused on incremental improvements; on cost reduction over value creation. This is an approach that will have businesses hunting ever after for short-term fixes to drive out further costs, while kicking the can down the road when it comes to designing an intelligent strategic journey that really benefits customers and employees.

The slow take up and low penetration of the business systems and transformation market is perhaps not surprising, given that there are certain elements of the adoption process that set buyers up for failure before they have even signed the dotted line. Here there are a couple of key red flags to be vigilant about:

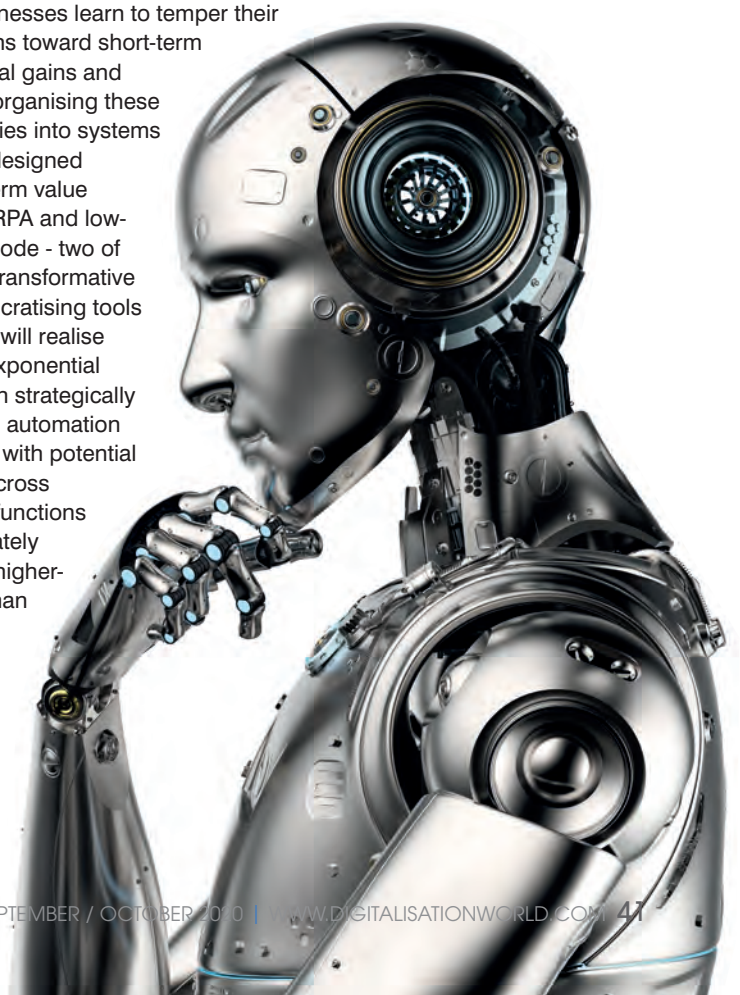
- Old school software sellers rebadged with RPA digital business cards and licensing models as old as the hills, and a lack of interest in anything other than shifting licenses - as many as possible, as quickly as possible. Many of the software companies themselves are rather too traditional and have not evolved their own business models sufficiently.
- A general lack of strategic thinking in the software buying process. Partly prompted by the offers of cheap or special deals from vendors, and in their eagerness to achieve huge returns on investment, there remains a lack of long-term direction, and so adopters tend to suffer from the 'random acts of automation' syndrome. Vendors typically view strategic thinking as little more than a delay in license sales, so are not really motivated to offer substantial guidance – although I would surmise this would be much better for their own long-term growth.

This is where a level of specialist guidance is often required. Businesses need to look to the future of profound transformation - the kind of transformation that uses technology to deliver and enable step changes in value creation. The journey to democratised automation in the enterprise will make the world a better place to live and work, but many organisations lack the frameworks to ensure that the benefits of hyperautomation are realised in a controlled manner. Adopters need to develop the strategies for integrated hyperautomation initiatives that drive an equable, symbiotic relationship between human creativity and the power of machines - and this vision does not spring forth naturally from the current buying process.

Accelerating the exponential

It is exhilarating to imagine the positive potential of equipping all the humans in an organisation with the endurance and superpowers that automation can provide. But without a clear strategic direction and intent across the entire business, and without the control environment to ensure standards are maintained, enterprises could be destined to go into self-destruct mode. Horses for Sources' Digital OneOffice is an excellent example of a framework that unifies front, middle, and back office processes, with end-to-end strategic automation that smashes through traditionally rigid organisational structures. Systems like this need to be designed for teams across an organisation to collectively analyse, design, automate, measure, monitor and reassess. The human impact of getting this change process right is monumental: conventional management and organisational structures will need to be changed, performance measurement and reward processes re-written, recruitment policies and standards reimagined.

We are well on our way towards a highly augmented human workforce, and I applaud pioneers such as UiPath that are hauling the market in this direction. But this high promise will only be delivered upon once businesses learn to temper their temptations toward short-term incremental gains and focus on organising these technologies into systems carefully designed for long-term value creation. RPA and low-code/no-code - two of the most transformative and democratising tools we have - will realise their full exponential potential in strategically Integrated automation initiatives, with potential to scale across business functions and ultimately augment higher-value human workers.



Self-sovereign identity

How blockchain is putting people in control of their data.

BY JOHN O'CONNOR, AFRICAN OPERATIONS DIRECTOR AT IOHK.

ALTHOUGH TECHNOLOGY has been an essential tool for connecting and monitoring the ever-changing pandemic, a larger variety of apps and services means that more people are aware of the risks they are taking with their data. From concerns over Covid 'track-and-trace' apps to huge data farming companies like Facebook and Google, to the more recent questions raised over the true intentions behind TikTok, consumers are becoming increasingly aware of, and concerned about, where their data is going.

The rise of surveillance capitalism has been a growing concern in recent years, as personal data becomes more and more commoditized. In response, people are demanding more control over their data, who has it and how it gets used. As a result, we are seeing the 'self-sovereign identity' movement gain increasing traction. Self-sovereign means that people control their own data and are able to create and control their own credentials and digital identities without third-party technology providers or governments.

The movement seeks to end the corporate harvesting of data, and wants to instead create a new consumer-led 'data marketplace' that empowers people to selectively trade personal data for financial rewards.

While data privacy has long been a concern, we haven't had the technology in place to tackle it until now. As blockchain technology has matured, solving this issue is finally becoming a real possibility. Blockchain protocols securely store data, putting people back in control of their information

The large-scale harvesting and trading of data isn't going to lose its value anytime soon, but it can be placed back in the hands of the people.

While data privacy has long been a concern, we haven't had the technology in place to tackle it until now. As blockchain technology has matured, solving this issue is finally becoming a real possibility. Blockchain protocols securely store data, putting people back in control of their information. Not only this, but third-generation blockchain protocols can allow people to create digital identities. For instance, imagine being in a bar. When you show your ID to the bartender, you're showing them more than just your age; they also see your date of birth, full name, and potentially even your home address. Self-sovereign identity means giving people control over their data, so they can only show the data they need to.

This is done through cryptographic techniques, such as zero-knowledge proofs (ZKPs), which make blockchains ultra-private, allowing information to be verified without revealing it to anyone but the recipient and allowing users to prove the information without giving away more than necessary. Such techniques can give people access services that require validation through data, but without sharing an excess of personal information, including age-restricted services or insurance.

Tracking your data

Concerns over personal data exploitation have been thrown into sharp relief during Covid-19. Technology is one of the best tools that we have to help combat the spread of the pandemic. Track-and-trace apps have the potential to help prevent further outbreaks, but questions continue to arise about the data that these apps require. These apps require a fair amount of personal information, particularly your address or geographical location. Although the severity of the tracing varies from country to country, it is often unclear what happens to user data after it has been surrendered, so there's no way of knowing who has seen it or has possession of it.

By employing blockchain technology in these track-and-trace apps, governments can address these data security concerns. Blockchain-enabled apps allow users to store personal data on their devices and only share the information that they want to share. Not only that, but this data is restricted to the owner and the person it is being shared with, preventing third parties from accessing it. This could make track-and-trace apps more secure, ensuring that we don't miss out on technology that can combat the pandemic without compromising our private data.

Securing your information Smart identities also hold great potential for students and graduates. Following recent hacks on a number of universities, data security is front of mind for students and their universities. Using blockchain, students will be able to verify their qualifications instantly. Degree certificates as well as medical records other forms of ID can be kept in a smart wallet on the student's device, and specific information can be shared on request, such as when applying for a job. IOHK is already piloting a project in Georgia to provide a way for students to access their qualifications securely. We've found from this pilot, Atala, that students not only want their qualifications to be secure, but also to be to be sufficiently portable so that HR workers and recruiters can seamlessly recognise and work with these blockchain-enabled records.

These solutions are not only for universities. In the same way that students can keep their qualifications in their own smart wallet, on their mobile device, service-providers, such as insurance companies, can also reduce corporate data privacy risks by transitioning to serverless apps where personal data is stored on consumer devices - rather than one centralised location removing third-parties from the equation. Surveillance capitalism and data commoditization are fast becoming commonplace, but with self-sovereign identity solutions, consumers and businesses alike are finally able to take back control of their data.

The foundations of blockchain have always been in privacy and giving people control, and now the technology has evolved it can put these principles into practice, allowing users to control their own data, only sharing what they want to with a select number of second-parties, in projects like Atala. At a time when personal data is more valuable than ever, blockchain is allowing users to keep their details safe.

Monitoring from home

Three things to still watch out for in your IT network.

BY MARTIN HODGSON – HEAD OF UK & IRELAND, PAESSLER AG.

IT'S A TALL ORDER to keep remote teams well connected and working seamlessly when employees are scattered outside the office. IT is the nucleus of modern business, so remote IT management is critical in ensuring data is shared freely yet securely among colleagues for efficient collaboration.

One of the main challenges for IT teams has been that not only are their users logging in remotely, but so are they. With the lockdown having lasted for months now, IT teams have been far away from the physical IT equipment that runs their business. Some businesses may now choose to open their doors for staff, however for those who are maintaining remote working measures how do IT teams ensure that everything is running as it should until they are given the green light to get back into the workplace? How can they be alerted when a critical service is slow or even worse down?

The answer to all these questions is the same as when everyone is working in the office: network monitoring. Here are three things you can do (and need to do!) to keep a close eye on your technology infrastructure.

1. Optimise bandwidth to avoid bottlenecks

Without a doubt bandwidth will remain key to how efficiently staff are able to work whilst not in the office. This is all based on how fast and effectively users can access and use services and applications. Video conferencing or sharing files on cloud services like Microsoft 365 are some of the main factors that have been incremental in teams working remotely. And with staff relying on remaining connected, low bandwidth needs to be avoided at all costs. In addition, teams may be split between those returning to the office and those who choose to remain at home so IT teams need to ensure that all team members can get the same efficient connection regardless of location. In short, bandwidth is probably still the most crucial element to monitor.

Bandwidth is a tricky problem because there are now so many variables that could affect a user's connection to services – and many of these variables are outside of an IT team's control. First, there's the user's wireless network at home, which might have countless devices connected to it right now. Also, in the same way that things are changing globally on a daily basis, employees may have also experienced changes to their connectivity solutions – something that IT teams will also have to bear in mind.

Then there's the user's connection to the Internet itself. This is almost impossible to monitor, of course, because you can't exactly install a network monitoring solutions in each employee's home without contravening privacy laws. Rather, this needs to be handled on an exception basis: Keep a close eye on what staff are having issues with. If someone complains that they're having problems with some or other services, start by asking them to run an Internet speed test. This will indicate whether the issue is with their connection to the Internet, or somewhere else. To control and limit the amount of incoming issues from staff, it's vital to continue to actively monitor what is going in the organisation's network. By monitoring potential problem spots in the network, it makes it easier to spot traffic congestion – before users raise the alarm.

2. Secure data and control access through the VPN

Virtual Private Networks have most likely been considered a saving grace by many workforces. However, it also means that there will still be dozens or even hundreds of remote workers connecting at any time. And of course, this means it's vital to ensure the VPN is functional.

The key aspects to consider with VPNs are the traffic in and out of the VPN, and the number of connections. Slow traffic might indicate a potential problem and knowing the number of currently connected users can help with troubleshooting and diagnosis. To be able to do so, businesses can use Simple Network Management Protocol (SNMP) for VPN monitoring. If the VPN environment is based on Cisco ASA or SonicWall devices, the system should incorporate a number of default sensors that use SNMP to monitor the VPN traffic, users, and connections of those solutions. If there is an alternative VPN option, then user-defined SNMP sensors can be used. Manufacturers such as Juniper and Fortigate provide MIB files that can feed into the monitoring system, allowing the monitoring of the corresponding VPNs.

3. Forge the digital workplace of the future with teleconferencing

There's no doubt that the glue that has been holding virtual teams together is online video meetings. Teleconferencing tools, like Microsoft Teams, Zoom, and others, are the only way that teams can continue working as...well, teams. So of course, these need to be up and running.

Fortunately, some monitoring systems have now implemented out-of-the-box solutions to monitor teleconferencing. These solutions can monitor applications like Zoom, checking live streaming status, web client status, web portal status, chat and meetings status. They show the operational states of the services and according error messages if something malfunctions; this new sensor type will help you keep tabs on the availability of Zoom so you can immediately react if there is an issue, which is especially important if your company relies on remote work via Zoom.

Bandwidth is a tricky problem because there are now so many variables that could affect a user's connection to services – and many of these variables are outside of an IT team's control

However, if no direct monitoring solution is available, there are also indirect options that can be made use of. Most services offer either an API or a Website for users to check on the availability of the service. For example, Zoom offers this service status, along with details of an API to query the status. It's crucial to keep tabs on this since having a live feed of status data can allow the IT admins to immediately react if there's an issue on Zoom or similar platforms.

Of course, there are also countless other things to keep track on; the above are just some of the more important ones when a large proportion of staff is working remotely. Having a system in place that allows IT teams to stay on top of the daily functions of the workforce will reduce the chances of unexpected issues as we progress through the current climate.

The silver lining in Covid-19's challenge to our work culture

The problems presented by this pandemic have undoubtedly made this an historic period for our generation, and while there are plenty of negatives to go around, the potential for positivity should not be overlooked.

BY HARGO KALRA, BUSINESS INTELLIGENCE MANAGER AT CONTACTENGINE.

A RECENT STUDY in Nature from May 2020 states global CO2 emissions are down "17% in early April 2020 compared with the mean 2019 levels" due to the lockdown, with nearly 50% of this coming from "changes in surface transport".

The true and long-term economic impact of Covid-19 (coronavirus) is currently unclear, though forecasts appear bleak. For example, an April 2020 University of Oxford report states "the economic fallout from this pandemic is likely to cripple even the most resilient of markets, threatening national and global growth". However, given that we are already down the rabbit-hole, would this not be the ideal moment to challenge the status quo? Within this article, I briefly explore some of the concurrent benefits for employees, companies, as well as the bees and trees arising from Covid-19 that I recently wrote about in this whitepaper.

The daily commute - a relic to be discarded

Near universally, each one of us in the workforce has faced the challenges associated with commuting to our place of work. Per the U.S. Census Bureau, commute times in the United States reached a record high in 2018. Similarly, in the UK, average annual commute times have risen by 21 hours from a decade ago. Numerous studies globally detail the negative impact of commute time on productivity. For instance, Ma and Ye (2019), find a positive relationship between commute time and absenteeism. Apart from the

positive impact on the environment due to fewer cars on the roads, the company thus potentially benefits from an economic standpoint by allowing work from home or at least flexible work arrangements.

By working from home and thus reducing the time of the commute (referring here specifically to non-active commutes), employees may be fresher and less stressed throughout the working day, thus leading to happier states of mind, which translates into higher productivity.

Business flights – rocketing out of relevance
Business travel accounts for a large proportion of companies' carbon footprint, particularly in the consulting sector. For instance, PricewaterhouseCoopers estimates nearly 80% of its carbon footprint in 2019 related to business travel.

Again the lockdown has provided a necessary shift of thinking for these employers to start using teleconferencing and digital methods of communication leading to a sharp fall in global aviation emissions. Overall, including both leisure and business travel, "aeroplane emissions fell by almost 1/3rd" in March 2020, with experts predicting that it could take nearly three years for the industry as a whole to recover from this setback.

If one can achieve similar, or even more productive, results by utilizing the glut of teleconferencing technology now thriving (one only has to look at Zoom's stock price over the last six months), then its morally and fiscally irresponsible to fly for these meetings in person. Put in the simplest of terms, taking into consideration that roughly 28-36K deaths per year in the UK due to "long-term air traffic pollution", more than 1/3rd of which is related to commuting for work, even a marginal improvement here leads to lives being saved.

The flipside

Making the change in our daily way of work-life to more flexible working arrangements, i.e. the ability to work-from-home, will inevitably have butterfly effects, with certain experts predicting these activities may offset some of the gains made in healing the environment. More research is required to definitively state that this change in the working culture will result in reduced greenhouse gas emissions given the variability in energy sources by different regions around the globe.

Detractors suggest that if employees have increased time to themselves, as well as the ability to work remotely, this may lead to increased leisure travel and thus negate the reduction in business travel. However, this seems a myopic view of the overall benefits, as research assessing the environmental impact of teleworking suggests that there is a high likelihood that the overall impact will be positive. According to this study, the largest impact comes from "reducing commuter travel and displacing office-related energy consumption".

Much like the industrial revolution, the digital revolution will have its say in defining our work lives. It is conceded that not all industries can change to work-from-home culture; manufacturing being the prime example here (though 3D printing and advanced robotics may have a thing to say about that).

It might even be simplistic to think that those who could switch to flexible working arrangements, could do so on a full workweek basis.

We would be conceited, however, in ignoring the opportunity afforded in this moment of crisis to at least do what is within our remit to help the environment recover to a sustainable level because it is only in our interest (and the interest of future generations) to do so.

The simultaneous and symbiotic benefits to employee, company, and the environment just represent the cherries on top of this particular cake.

Again the lockdown has provided a necessary shift of thinking for these employers to start using teleconferencing and digital methods of communication leading to a sharp fall in global aviation emissions. Overall, including both leisure and business travel, "aeroplane emissions fell by almost 1/3rd" in March 2020, with experts predicting that it could take nearly three years for the industry as a whole to recover from this setback

How a strong company culture can drive digital transformation

Now, more than ever before, organisations are relying on a driven and engaged workforce – that is safe, happy, self-motivated, and built for collaboration, and productivity as well as the business's bottom line.

BY KIRSTY CARTER, CHIEF OF STAFF FOR TECHNOLOGY SOLUTIONS AND SERVICES PROVIDER, SOLUTIONIZE GLOBAL.

AFTER ALL, how can anyone expect a dysfunctional, toxic culture to translate into a productive homeworking scenario that's committed to pushing revenue into the black? Or provide a welcoming environment and seamless onboarding process – especially when it must take place remotely – for a new starter to remain loyal and eager to succeed? Staggeringly, breathHR's 'The Culture Economy' 2018 report highlights how poor company culture costs £23.6bn per year – with 34% of people quitting their jobs because of a dire workplace atmosphere.

The figures continue to back up how a motivated team can drive commercial success. For example, research by financial economists showed companies that were listed as being among 'the best places to work' delivered nearly 20% higher returns to shareholders. Why? Because their teams were given the support to remain mentally-strong, the correct tools to be productive and the motivation to be trusted to do their jobs well – much to the benefit of the end user. There are plenty more statistics which evidence how placing a huge emphasis on employee wellness and maintaining a healthy and happy workforce are powerful elements that every enterprise should strive towards. In addition, how installing the right kind of tech can enable employees to bolster business growth, embrace agility and set the benchmark for competitors to follow.

But how does digital transformation truly fit into all this?

Innovation, inspiration and reinvention

Encompassing new, fast – and frequently changing – technology to solve problems, this revolution has completely shifted how organisations are now managed.

Looking back to how firms may have operated decades ago, it's likely that tech and IT teams would've worked in silo away from other departments, never directly communicating with the end user – leaving that to the customer-facing roles.

However, technological transformation has empowered modern-day processes. It's enabled teams to converse with all members of the company and beyond, regardless of the office space they occupy. Now, the customer is very much able to get answers to their questions straight from the innovators themselves.

Not only that, remote working possibilities have empowered workforces, enabling people to work from anywhere – in any time zone. And the digital revolution continues to challenge business leaders to embrace a forward-thinking mindset – and possess a level of trust in their employees to do a good job even when they're not in the same room.

But transformation isn't just one act, it's a continuation of developments highlighting exactly how agile companies really are when it comes to truly modernising their approaches – and realigning change management processes to stay ahead of the game and maintain an inspiring place for people to work.

Adopting a forward-thinking mindset

And without all this – namely the innovation and aspiration in which technology presents – company culture would suffer greatly. Enterprises that are crippled by a toxic environment become slow to react to the ever-evolving technological landscape because there is a distinct lack of care from employees – and

their products and services would ultimately get left behind.

Digital transformation affects an entire team that's built up from a wide range of personalities and characteristics – all of whom play a pivotal role in the company's success. However, if those individuals didn't have the right technology in place that is a driving force in bringing them together – and inspiring, upskilling and developing trust – an organisation will struggle to remain relevant.

Agility in the marketplace has never been more pertinent and it's those firms that are able to utilise machines to their benefit as a productivity enabler – whether in an office space or working remotely – means they will complete projects more swiftly, and be able to pivot to market needs. Taking labour-intensive jobs out of a time-strapped employees' day – and plugging in automated systems to man the mundane work – allows individuals to truly shine and concentrate on their priorities. And with that comes a happy team member who instils pride and passion into the company's culture, leading to enhanced productivity and positive end user experiences.

For a motivated workforce to continue, the balance between empowering employees and undergoing digital transformation must work side-by-side, and that means obtaining staff 'buy-in' from the get-go, and when any kind of change occurs.

Giving workers the opportunity to enhance their skillsets via savvy machinery can create loyalty, trust and assurance that they'll do the best possible job – and therefore develop a dynamic team that always places the end user and business growth at the forefront of their minds.

For a motivated workforce to continue, the balance between empowering employees and undergoing digital transformation must work side-by-side, and that means obtaining staff 'buy-in' from the get-go, and when any kind of change occurs

Security lies in visibility

The analysis of the online attack surface in 2020.

BY FABIAN LIBEAU, VP EMEA AT RISKIQ.

AS BUSINESSES have had to navigate the disruption caused by the ongoing pandemic, the sweeping digital transformation of enterprises has been dramatically accelerated in 2020. Although this transformation was inevitable and trend-setters may be rewarded for their innovation, it is also imbued with risk. Indeed, 2020 has shown that as digitalisation moves assets beyond the confines of the company firewall, threat actors are well-positioned to exploit the changing landscape.

The ever-expanding online attack surface

To understand the threats that companies are currently facing, it is important to identify the vectors through which they can be targeted beyond the corporate firewall – this is called their Internet Attack Surface. Expansion beyond the corporate firewall takes the form of businesses undergoing a rapid migration to cloud and the near-total adoption of public-facing assets for customer engagement, such as web, mobile and social platforms. This expansion has only been further driven by the necessity of standing up remote access services for all employees as COVID-19 has imperilled physical interaction across the globe.

While essential to business operations, these digital initiatives thrust company assets into the murky labyrinth of the modern Internet. In this vast network of connections, boundaries can be ill-defined and this offers cybercriminals cover through which to compromise consumers and mount forays into the corporate network. Underlining the nature of the threat is the Verizon Data Breach Report1, which highlighted how external-facing web applications, into which network security tools lack visibility, comprised the vector-type most exploited in hacking-related breaches.

Visualising the online attack surface

To visualise the online attack surface, it helps to picture the Internet as a boundless tapestry that is ever-expanding in all directions every day. This tapestry is comprised of a multitude of entities – websites, IP addresses, components, frameworks and code – and

these threads are often spun together to create the internet that is known and interacted with today.

Companies have little choice as to whether their presence is woven into this tapestry – they simply must exist in the online world if they are to compete. However, even a simple website connects company assets to the vast structure of the web. Therefore, companies have no choice but to reside in a burgeoning digital metropolis, haphazardly regulated, and inhabited by both the legitimate and the ill-intentioned. Indeed, threat actors are happy to exploit their connections to legitimate assets to victimise both companies and their customers.

Given the size of the internet, the scope of the attack surface is almost unfathomable. Critical to having visibility into the online attack surface is using technology that is able to extract internet data and map the billions of relationships between internet-exposed infrastructure worldwide. This visibility enables businesses to assess their online attack surface and judge the digital risk. For example, over a two week period, RiskIQ's Internet reconnaissance infrastructure detected the appearance of 2,959,498 new domains and 772,786,941 new hosts, which equates to a daily rate of 211,392 and 55,199,067 respectively2. Each of these new domains and hosts represents a potential target for threat actors. Conversely, threat actors set up their new attack infrastructure while hiding in this background noise.

Vulnerabilities in a modern website

A modern website is the foundation upon which companies exist and compete in the online world. These are made up of many different components – the underlying operating system, frameworks, third-party applications, plugins, trackers, and so on. Each component works to form a part of the website to deliver a user experience that people now expect. This reduces time-to-market and optimises user interactions. However, given that many of the building blocks used are so ubiquitous, malicious actors who successfully craft an exploit against one of these building blocks can re-use the same exploit across an abundance of websites. If organisations are not vigilant in applying vendor issued patches in a timely manner, it is only a matter of time before they'll become a victim of this type of exploit.

One example of this are exploits targeting content management systems (CMS). The use of CMSs are favoured by many developers as they allow for the creation of modern, dynamic websites while reducing the time needed for new content and updates. However, this also means that if an exploit is developed by threat actors against a popular CMS, many organisations can be victimised – and the impact widespread. Showing how widespread the use of CMS's are, over a 2 week period RiskIQ's crawlers identified 13,222 WordPress plugins and 4,780 total CMS instances in the Alexa top 10,000 most visited websites. Known vulnerabilities in commonly used components are reported as common vulnerabilities and exposures (CVEs). CVEs are rated according to severity by the common vulnerability scoring system (CVSS), which categorises their danger on a scale of 1-10. According to the scoring system, 7-8.9 represents high vulnerabilities, whereas 9-10 represents critical vulnerabilities. Looking again at the Alexa top 10,000 domains, RiskIQ found 2,840 domains that were running at least one potentially vulnerable web component, while 8,121 potentially vulnerable web components in total were uncovered. A portion of these vulnerable assets will have patches and mitigating controls to ensure against attack, but many will not.

Hackers or security teams: who has better visibility?

The numbers highlight the far-reaching nature of an Internet attack surface. However, if security teams had full visibility over this attack surface, the exposures could be assessed and prioritised, with remediation resources focused on addressing the most critical ones. Unfortunately, enterprises are finding that, often, threat actors have a keener understanding of the online attack surface than their security teams. This is the result of two salient dynamics that can complicate and obscure a company's online profile – shadow IT and mergers and acquisitions (M&As). In the current public health climate, with most office workers signing on remotely, the critical issue of 2020 is shadow IT. Shadow IT is the deployment of new applications and systems at a department or line of business level that bypass the central IT and security teams. Often justified by the need to move at the speed of business, it has grown exponentially in recent years with the adoption of cloud-based applications and services.

The challenge is that beyond the purview of security teams, over time, these unmanaged assets represent a significant vulnerability in an organisation's attack surface. If these assets are not patched or tested, their operating systems, frameworks, and third-party applications can quickly age and become vulnerable to even crude hacking tools.

Visibility is key to security

When it comes to defending an organisation's Internet Attack Surface, visibility is crucial. In simple terms, you can't protect what you don't know about and you can't proactively defend against targeted attacks if you have no visibility of the attacker and the infrastructure they're setting up to target you or your customers. The public Internet has become the new security battleground and never has the 2500 year old quote by Chinese General Sun Tzu been more relevant: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Why you should self-isolate, but your IT infrastructure should not

One of the many distressing fallouts from the pandemic is the significant increase of COVID-19 related threats, as financially motivated cybercriminals prey on people's fear and thirst for information, making them easy targets.

BY ZEKI TUREDI, CTO EMEA, CROWDSTRIKE.

FOR BUSINESSES, this means defending against a much higher rate of attacks as cybercriminals try to breach enterprise networks by any means necessary. In fact, CrowdStrike has observed a 330 percent increase in malicious files using COVID-19 themes since the pandemic first struck in March, and cyber criminals show no signs of slowing down their brazen behaviour. Even more worrying, we've seen a change in tactics where ransomware actors are increasingly moving to extortion where they are stealing sensitive files and threatening to release them if they are not paid.

While lockdown restrictions are still largely in place, many employers have adopted informal stay-at-home instructions, leaving many of us unable to return to the office and enterprise networks largely distributed and more vulnerable. With many businesses already buckling under the pressure of the global pandemic, a large scale attack could bring hault business operations entirely and bring it to its knees.

CrowdStrike's 2020 Global Threat Report revealed that Big Game Hunting (BGH), the shift towards harnessing ransomware attacks with high payouts,

characterised by low volume, high-return victim targeting, is increasingly on the rise. The number one issue when dealing with ransomware and BGH is that conventional signature-based endpoint protection has proven itself to be woefully inadequate, even with additional measures such as whitelisting, Indicators of Compromise (IOCs) or machine learning. This is due to the nature of BGH which it harnesses not just sophisticated ransomware but also the expertise and persistence of a hands on keyboard attack. CrowdStrike tracked that the volume of hands-on-keyboard intrusions reached 112 percent of the levels of 2019 in the first half of 2020 alone. 82 per cent of this activity has been attributed to eCrime and this shift is set to continue — especially as we settle into the future of home working.

In the battle against the rising level of highly sophisticated ransomware threats, organisations need to adopt an integrated multi-pronged approach. Here I've outlined some methods of prevention and detection that organisations should look to add to their strategy to help prevent and detect against an increasingly complex and rapidly evolving threat landscape.

IOAs, the enemy of ransomware

One essential method to deploy when trying to defend against ransomware are Indicators of Attack (IOAs). Unlike IOCs used by legacy endpoint detection solutions, IOAs focus on detecting and preventing the intent of what an attacker is trying to accomplish, regardless of the malware or exploit used in an attack. When using IOAs, security teams can detect red flags that an attack may be in progress within the network, and halt the adversary in their tracks before they can accomplish their objectives. Using this method is extremely effective against fileless attacks and hands on keyboard attack methods, which are starting to be used by more attackers in place of traditional malware.

In addition, IOAs provide a reliable way to prevent ransomware from deleting backups, encrypting systems and moving laterally across your network. This gives users the ability to restore encrypted files, even if file encryption began before the ransomware was stopped.

Three is the magic number

Due to the increasingly sophisticated nature of ransomware attacks, organisations must ensure they

Corporate networks need constant surveillance and built-in EDR can act as a 'CCTV camera' which helps security teams monitor everything that takes place across all endpoints. This second layer of defence can help security teams monitor actions such as running an application, connecting to a network, visiting a website or writing a file. By leveraging built-in EDR capabilities, security teams can gain a more holistic view of their organisations' network with the fidelity necessary to identify IOAs

have a robust and holistic cyber strategy in place to defend their network. This requires a combination of solutions to create a layered and integrated three-pronged approach that combines next-generation antivirus (NGAV) with endpoint detection and response (EDR) and managed hunting.

As the first layer of defence, businesses should adopt a NGAV solution. These solutions typically provide the most proven and advanced prevention capabilities to defend against known and unknown malware, and even attacks that do not use malware. Next-gen antivirus solutions which leverage AI-powered machine learning can also allow organisations to rapidly analyse IOAs to help identify a ransomware attack and slam the breaks before the bad actors can complete their mission and inflict damage.

Corporate networks need constant surveillance and built-in EDR can act as a 'CCTV camera' which helps security teams monitor everything that takes place across all endpoints. This second layer of defence can help security teams monitor actions such as running an application, connecting to a network, visiting a website or writing a file. By leveraging built-in EDR capabilities, security teams can gain a more holistic view of their organisations' network with the fidelity necessary to identify IOAs.

Beyond this, organisations need to ensure they factor in a human element into their strategy, as technology can only go so far in defending against attacks. Ransomware delivery tactics have become far more superior than traditional 'spray and pray' techniques, where bad actors try to flood corporate inboxes in the hope someone might open the malicious file, which are continuing to decline in popularity.

The rise of "living off the land" (LOTL) techniques, which involves the bad actor painstakingly preparing the environment, deleting backups and clearing logs well before ransomware binaries are deployed, are increasingly on the rise. Criminal techniques continue to grow in sophistication, so a rigorous people process and technology is key to mitigating risk.

Organisations should seek to couple their technology with a human-powered effort which combines threat intelligence resources with advanced security technology to proactively protect systems and information. This is where threat hunting – the practice of proactively searching for cyber threats that are lurking undetected in a network – comes into play. Without threat hunters, security teams can easily miss a crucial opportunity to thwart ransomware operators before they have the opportunity to begin encrypting files. Threat hunters are highly trained experts who use the information gathered by the NGAV and the EDR solutions plus threat intelligence information on the tactics, techniques, and procedures of adversaries. They use this intel to investigate security data and discover any hidden attacks that may not be flagged by automated elements of defences. It's the holistic nature of these elements working together that provides the ultimate power behind this three-pronged approach.

Don't forget about good hygiene!

As our networks evolve and move from physical systems to the cloud or from desktops to virtual environments, we need to make sure we have visibility into these changes. Hygiene plays a key and crucial role in making sure we are able to identify security gaps quickly but more importantly, make the life of an attacker as difficult as possible. Having the tools to quickly identify new and serious vulnerabilities or account miss-use is now even more important, with our ever growing disparate and hybrid workforce.

Stay secure for the new normal

With the rise in COVID-19 motivated attacks and rapid adoption of distributed working styles, it's crucial that organisations and their security teams ensure their cyber defence strategies are in tip-top shape. By using AI-powered next-gen solutions in combination with threat hunters, security teams can breathe a sigh of relief as they know the network is secure and teams are still able to be productive. COVID-19 has brought up many challenges for businesses but security should not be one of them if the correct solutions are in place.

CELEBRATING 11 YEARS OF SUCCESS

Announcing the 11th edition of the premier IT awards: The Storage, Digitalisation + Cloud Awards 2020.

In what has been, and continues to be, extraordinary times for the business world, it seems doubly important to recognise the projects, innovations and individuals which have made such a huge difference during 2020. Almost overnight, employees switched from office working to working from home, and the new, or next, normal, means that, into the future, what might be called a 'hybrid work' model looks set to evolve, with flexible working very much the order of the day. What was already becoming a trend as part of many organisations' digital transformation programmes, has been accelerated.

The SDC Awards 2020 will celebrate the achievements of end users and the IT community as they have innovated like never before to ensure business continuity in these challenging times. This year more than any other, please do make sure that you enter our SDC Awards. There's no limit to the number of entries, all of which are free of charge, and we'll be promoting all the short-listed entries via Digitalisation World's multi-media platform over the coming months, ahead of the awards ceremony. We really do want to celebrate and recognise the many amazing achievements which have come about in response to the coronavirus.

WHY ENTER?

MAXIMISE VISIBILITY
Free PR opportunities with 5 months of marketing utilising the Digitalisation World portfolio.

POSITIONING
Position your product or service as an innovator in your field.

INCREASED CREDIBILITY
An award win, shortlisting or nomination acts as a 3rd party endorsement.

NETWORKING
Over 300 industry leaders attend the gala awards evening.

COMPETITIVE ADVANTAGE
Gain an advantage on your competitors.

NOMINATION IS FREE OF CHARGE AND VOTING IS DONE BY THE READERSHIP OF THE DIGITALISATION WORLD STABLE OF PUBLICATIONS.

SDC AWARDS 2020

www.sdcawards.com

How to implement effective data lifecycle management

Digital transformation is taking hold. Leading to organisations producing more data than ever before and at an increasingly fast volume.

BY PHILIP BRIDGE, PRESIDENT, ONTRACK.

NO MATTER WHAT data a company produces, managing it through its entire lifecycle is vital to ensure security and compliance. Whilst the default reaction is to keep data "just in case", the simple truth is that most corporate data outlives its use very quickly. Once data is no longer deemed valuable, it becomes a liability, one that could expose an organisation to extreme risks.

Whether it's customer, employee or corporate data, the more data an organisation manages, the more risk it carries. The last few years have seen a substantial increase in cyber-attacks, with the main purpose to steal corporate data and set a ransom for its "safe" return. In fact, the a report by McAfee states that in the first quarter of 2019, ransomware attacks grew by 118%.

Organisations should consider not only the risks of data exposure but also the cost of protecting the data in the first place. The more data you have on servers, backup tapes, and mobile devices, the more investment you need to make to ensure it's secure. Cybersecurity needs to be a top priority for businesses of any size to protect itself against the ever-evolving threat network. According to ISACA's State of Enterprise Risk Management 2020 study, 53% of respondents stated that they had seen increased risk to their organisation over the last 12 months. Additionally, 29% claimed cybersecurity is the most critical risk category facing enterprises today, and 33% believe that information/cybersecurity risk will be the most crucial category of risk facing their organisation in the next 18-24 months.

An organisation should not only be wary of the cost of cybersecurity and the potential risk of data breaches. There are also less measurable elements an organisation should consider. These include the cost of procuring and maintaining data storage and backup equipment; the cost of preserving personnel processes and software to manage data storage, backup and archiving; and the time and resources of workers who have to sift through unnecessary data to find relevant information.

To effectively mitigate the risk of data exposure and avoid the costs of storing and handling unnecessary information, an organisation should implement an end-to-end process for managing its information from creation to disposal. A data lifecycle management programme can benefit an organisation by reducing risk, improving service and saving on costs. Typically, the data lifecycle includes six phases:

- **Create –** Data creation occurs throughout organisations. It can take place on-premise either in your data centre or on employees' devices or externally in the cloud. Protecting your data during this phase will include access controls such as passwords, threat scanning for viruses, and data classification that will specify the data type, its location, how it should be protected, and who has access to it.
- **Store –** Once data has been created, it is typically stored on a computer hard drive or in a datacentre. Storage also involves near-term backups that must also remain protected. Storage protections include access control around who can read and overwrite the data, device control such as data encryption,

backups to protect from data loss, plus security measures to protect the backups themselves.

- **Use –** During the 'use' phase, data is accessed, viewed or processed. Protections during data usage include access control, encryption, data rights management for copyrighted information and data loss prevention, which involves software and business rules to prevent unauthorised access to sensitive information.
- **Share –** Data is often shared amongst internal employees and to corporate partners outside of the organisation. Data sharing can occur through the network, via removable media, or across the internet via transfer sites or email. Data sharing safeguards involve access control, encryption, network security (firewalls/intrusion detection) and data loss prevention. When organisations are dealing with third-party vendors, they should have clear measures in place for data removal and verification after services have ceased.
- **Archive –** For short-term data protection, all data must be backed-up regularly, either onsite or offsite. When an organisation needs to retain data for the long term, it can be archived to tape or disk media and placed in remote, secure locations.
- **Destroy –** When an organisation's data reaches the end of its life, it must be permanently erased. Determining which data is erased, how it's erased and how that erasure is verified depends on several factors, such as content type, usage needs and regulatory requirements.

Without a data lifecycle strategy in place, an organisation is leaving itself exposed to serious security risks and costs. Today, the cost of ineffectively safeguarding data comes with too high a price. Data breaches, damaged reputation, lost customers, downtime, and large fines are all potential risks for an organisation that doesn't effectively manage its data's lifecycle.

Those organisations that take the time to invest the necessary efforts and resources in data lifecycle management can minimise the risks and costs of their business-critical data at all stages. Make sure you are not one of them. **https://www.ontrack.com/en-gb/**

Data lies at the heart of a business

DW talks with Jonathan Bowl, AVP for UK&I and Nordics at Commvault, focusing on recent additions to the company's technology portfolio and discussing wider industry issues, including containers, on-prem v cloud and the changes they are seeing as part of the 'new normal'.

DW: *Commvault's FutureReady event took place recently. Can you tell us how it went – presumably it was a virtual gathering rather than a physical get together?*

JB: The majority of events have gone virtual this year thanks to the on-going pandemic. Although we missed getting together in-person with all of our friends, partners and customers at our annual CommvaultGO, we knew we had to go virtual this year. FutureReady was the first time we'd looked at doing a virtual event, but it was a great success! We had analysts and journalists attend from all across the globe – joining from the US, Europe, India, Singapore and Japan. The event aimed to give attendees a first look at Commvault's breaking news, and meant they could engage with Commvault executives and network. It proved that events can still be engaging and fulfilling even done remotely – just because it's virtual doesn't mean it's any less fun!

DW: *The company made a significant amount of news announcements at the FutureReady. Can you give us the high-level view of these, which seem to focus on intelligent data management?*

Yes, there were three major releases announced during our FutureReady Day. Our most exciting and anticipated being the HyperScale X launch – our new scale-out appliance for the Commvault intelligent data management platform.

We also announced our new product portfolio, and our updates to Hedvig Distributed Storage, which includes new enhancements for Kubernetes running in hybrid and multi-cloud environments. Our expanded product portfolio is helping customers use their data to cope in these challenging times, as data management is crucial for maintaining a semblance of normal in today's business world.

DW: *In more detail, can you talk us through the HyperScale X launch?*

JB: HyperScale X is the latest generation of Commvault's fully integrated scale-out data management solution, and is also the first product in our portfolio to integrate technology from the recent Hedvig acquisition. To put it simply, HyperScale X combined with the Hedvig technology boosts resiliency, backup and recovery performance, and agility when customers need it most. It provides scalability, security, and resiliency to accelerate an organisation's digital transformation journey as they move to hybrid cloud, container, and virtualised environments. And, because the architecture is flexible, customers can get up and running quickly, and grow as their needs demand – which is becoming more essential in the current climate.

DW: *And the Backup + Recovery piece?*

JB: Our new standalone backup and recovery product ensures data availability for all workloads – including containers, cloud-native, and virtual – across cloud and on-premises environments. So, it delivers simple, and reliable, data protection through a single extensible platform.

DW: *Which differs from the Disaster Recovery announcement?*

JB: Yes, the Commvault Disaster Recovery is a comprehensive disaster recovery product, which enables customers to ensure business continuity and verify recoverability across cloud and on-prem environments. It provides simple, automated disaster recovery orchestration, flexible replication, and verified recovery readiness.

DW: *And where does the Complete Data Protection solution fit in?*

JB: The Complete Data Protection solution is the marriage of Commvault Backup & Recovery and Commvault Disaster Recovery. It brings our industry-leading functionality into a single data protection solution, to ensure data availability and business continuity for all workloads across cloud and on-prem environments.

DW: *Governance and compliance issues are also covered?*

JB: Commvault now offers both Commvault® Data Governance and Commvault® eDiscovery & Compliance, which were previously bundled together as Commvault Activate. Both solutions give customers greater visibility into their data, identify opportunities for storage efficiencies and manage risk. We have now made it easier for organisations to purchase these solutions in alignment with how they consume other Commvault offerings with a simplified pricing model.

DW: *Along with containers and Kubernetes in particular?*

JB: There have been new enhancements in the Hedvig Distributed Storage Platform for Kubernetes running in hybrid and multi-cloud environments.

Kubernetes has fast become the standard container infrastructure platform for application modernisation, so it's now even more important for businesses to ensure the storage infrastructure supporting containerised workloads has an integrated solution for Kubernetes deployments. This infrastructure must integrate across all types of Kubernetes deployments (cloud-managed or self-managed) and deliver seamless migration, data protection, availability, and disaster recovery for the entirety of these containerised environments. Seamless migration features are key for a DevOps audience, whether their Kubernetes deployments are managed outside the organisation or in-house

Commvault's new native API Kubernetes enhancements in the Hedvig Distributed Storage Platform provide customers the flexibility to develop and run modern applications in any Kubernetes environment with the ability to seamlessly protect, migrate, recover, and use their data. Customers have the flexibility to develop and run new modern applications with encryption and third-party KMIP support for data security in any Kubernetes environment. It also offers the ability to seamlessly protect, migrate, and use the data stored in Hedvig to speed the DevOps process and remove any cloud-managed or self-managed Kubernetes service barriers.

DW: *Finally(!), there was some news around the subscription pricing?*

JB: We've seen that customers are increasingly looking to shift toward OPEX-based and cloud-like pricing, and so require the flexibility and efficiency that a subscription pricing model enables. We're proud to be leading this transition, with more than 40% of our software and product revenue coming from subscription licensing. Our recent announcements further enable Commvault's products and ecosystems to lead with subscription pricing models, enabling simplified choice for customers. We're dedicated to continuing to support customer requirements for a perpetual pricing model.

DW: *Moving on to some wider industry issues, please an you talk a little bit about the momentum behind containers right now and what Commvault is seeing?*

JB: Containers are becoming a key technology that is being used in the development of all new applications. We are seeing that, as part of digital transformation initiatives, enterprise organisations

have made the strategic decision to build all new digital based apps around cloud and containers and phase out older applications – they see this as the way in which they can be agile and quickly respond to changing customer and market demands. We have seen a number of customers across many verticals and sizes have the need for protecting and managing data for container based applications. For example, one customer has been developing production applications on containers for over two years, and we have been working closely with them to get support for OpenShift and Kubernetes.

Initially, organisations tried containers but found that managing and scaling them were problematic and resource intensive. But today, container technology has matured with several container management / operating platforms available that take this pain away – as a result, interest and actual production application development is now actively pursued in companies of all sizes, especially enterprises. Companies such as Netflix and Amazon utilise containers to be able to provide the scalability and service levels that customers expect.

Now, the new issue to overcome is managing and protecting data associated with these new container based applications – hence the surge in interest and requirements for container support from data management products. The flexibility that containers provide has opened up a new challenge around data management, as applications can be simply scaled up and down, easily relocated and moved. It's harder to keep track of the data produced or used by the applications to ensure that it is available, protected, secured and managed. This is where Commvault comes in – we are developing our capabilities here to assist customers and address these issues.

DW: *How would you characterise the on-premises vs cloud and managed services debate when it comes to how end-users are looking to source storage and data management solutions?*

JB: There's been a lot of talk about cloud, on-premises, off-premises and hyperscalers, and I think there's a certain notion that in reality, an application has different characteristics and requirements. I don't think anyone is going to go wholesale – IT manufacturing needs data to be close to it. The reality is that organisations will be using a combination of different types of cloud platforms depending on the apps, characteristics and data they're using. It's not really a case of one or the other; it's a case of brokering applications and deciding which will go in the cloud, and which will go on-premises. The importance is having flexibility. Over the past 6-9 months, Covid has helped to accelerate the decision-making. Large enterprises will likely have a multi-cloud environment, but there will also be examples of wholesale organisations utilising the cloud that will have wanted to bring things back in-house. The pandemic has been a catalyst for off-premises, but there will always be a need for hybrid. Flexibility is the most important thing to move workloads.

DW: *Before we finish, we can't ignore the current, slightly surreal business environment. What changes have you seen in terms of how end-users are consuming your solutions during the pandemic?*

JB: We have seen a huge focus on end-point protection, and the protection of devices. People have been working with mission-critical data for a while, but now we are working with it literally on the dining table, which gives more opportunities for it to be damaged. The need to ensure the device of end-users is protected and secure is important. The FBI has said that cybercrime reports have quadrupled during the pandemic, thanks to remote working. There's a huge focus now on ransomware detection and ensuring systems working in this way are architected. This is because of the notion that data is valuable, and so there's an even bigger desire to make sure that this asset is held securely.

DW: *And is it possible to begin to work out how this will play out in the longer term, bearing in mind that digital transformation was on many organisations' radars in any case?*

JB: The current situation has given rise to the acceleration of digital transformation. Businesses want to adapt and stay alive, and so how they use the data they have to engage with customers continues to be the foreground of how organisations have spun themselves around in order to provide new services. What's really been highlighted in this pandemic is that data lies at the heart of a business, and is in fact the real value. Transformable businesses use their insights to build new models and processes in order to help them compete and prepare. Using data to derive insights is becoming increasingly important for organisations to transform and evolve and stay current.

Angel
BUSINESS COMMUNICATIONS

WEBINARS

Specialists with 30 year+ pedigree and in-depth knowledge in these overlapping sectors:

Expertise: Moderators, Markets, 30 Years + Pedigree
Reach: Specialist vertical databases
Branding: Message delivery to high level influencers via various in house established magazines, web sites, events and social media

Semiconductor (Silicon/Compound)
Publications include: Compound Semiconductor, Silicon Semiconductor, CS China, SiS China

Power Electronics
Publications include: Power Electronics World

Future Mobility
Publications include: TaaS Technology, TaaS News

Data Centres
Publications include: DCS Europe, DCS UK, SNS International

SmartSolar UK & Ireland
Publications include: Solar and Power Management, Solar UK and Ireland

Sensors
Publications include: Sensor Solutions Magazine, Sensor Solutions International

Digitalisation
Publications include: Digitalisation World, Information Security Solutions, Managed Services

Photonics
Publications include: PIC Magazine, PIC Conference

Expert Moderators

Dedicated technical and time-served experts/editors

MARK ANDREWS
Mark Andrews is technical editor of Silicon Semiconductor, PIC Magazine, Solar+Power Management, and Power Electronics World. His experience focuses on RF and photonic solutions for infrastructure, mobile device, aerospace, aviation and defence industries

PHIL ALSOP
Journalist and editor in the business to business publishing sector for more than 30 years currently focusing on intelligent automation, DevOps, Big Data and analytics, alongside the IT staples of computing, networks and storage

JACKIE CANNON
Director of Solar/IC Publishing, with over 15 years experience of Solar, Silicon and Power Electronics, Jackie can help moderate your webinar, field questions and make the overal experience very professional

DR RICHARD STEVENSON
Dr Richard Stevenson is a seasoned science and technology journalist with valuable experience in industry and academia. For almost a decade, he has been the editor of Compound Semiconductor magazine, as well as the programme manager for the CS International Conference

For more information contact:

Jackie Cannon **T:** 01923 690205 **E:** jackie@angelwebinar.co.uk **W:** www.angelwebinar.co.uk
6 Bow Court, Burnsall Road, Coventry, CV5 6SP. UK
T: +44(0)2476 718 970 **E:** info@angelbc.com **W:** www.angelbc.com

Eight steps to accelerating the digital transformation of professional services

The pandemic has revealed gaps in digital capability, especially when it comes to remote working and dynamic collaboration. Alan McMillen, CEO at Repstor, offers an 8-step action plan for consolidating content management to support more flexible working models.

THE URGENCY around digital transformation has intensified as a result of the COVID-19 lockdown. Professional services firms have a seen an unprecedented challenge to their ability to work digitally. Almost all professional services organisations have accepted that ways of working, and indeed entire operating models, will never be the same again. Many businesses are considering replacing bespoke content management systems with a simplified cloud-based platform strategy that enables employees to work from home easily and allows the business to source talent from a global marketplace. There are eight steps on the path to a consolidated collaboration platform:

1: Assess how current content access and collaboration limitations are holding your people back

Review current pain points and trace them back to their source. Firms that continue to rely on their own physical servers and on-premise data centres to store and manage everything, for instance, are likely to have experienced the biggest issues gaining access to the latest files and client information during lockdown.

2: Remember one of the biggest takeaways of COVID: that even big firms can effect change quickly when they need to

We saw this first-hand during the lockdown. Large professional services firms - which ordinarily might take nine months to conduct risk assessments, vet vendors and consider options from every angle before choosing and implementing a solution– were suddenly strikingly agile. When necessity called for it, they were able to make and enact decisions within days – even with due diligence.

Many had started down the road to deploying Microsoft 365 and were planning or had started Microsoft Teams pilots on a small scale, but the need to get something in place to meet demand turned these pilots into full roll outs, with tens of thousands and in some cases more than 100,000 users deployed in weeks.

3. Whatever the plan, make it in the cloud

In 2020, it makes no sense to persist with proprietary storage area networks (SANs), physical servers and on-premise backup scenarios, when the latest and best IT capabilities are all readily available in the cloud - and managed around the clock by dedicated experts.

4. Allow for data migration

Any platform migration needs planning, so many firms favour a hybrid approach – where they embrace a new platform for new activities, but continue to leverage existing systems for a time.

However, many firms are turning to a 'big bang' approach to platform consolidation and replacing legacy technology that has held them back during lockdown. This is now seen as a 'must do', to ensure they can operate efficiently – rather than sinking investment into trying to make multiple on-premise systems available and able to work together for remote workers.

For many, the platform that makes most sense is Microsoft 365 including Teams.
It's not just about the data. End users must be able to access and work with their content productively. Ensuring the content is effectively consolidated, organised and associated with projects and available to the right users is all key to delivering on productivity and quality that will provide additional ROI.

5. Give thought to change management

Although a hybrid/gradual approach to migration allows professionals to adapt to the change, harnessing a familiar platform like Microsoft 365 minimises the need for formal change management and new staff training. Because everything is channelled seamlessly through already-familiar interfaces like Outlook and Teams, knowledge workers don't have to change the way they behave to have more intuitive access to the content and connections they need.

6. Let go of the past

Professional services firms have found that it is possible to halve the costs of specialist content management systems by consolidating project activity and related documents and correspondence on a mainstream platform already used extensively from department to department, sector to sector, around the world. So the case for leaving costly legacy investments in the past is strong.

7. Prioritise the mobile experience

For too long, professionals using specialist document management applications have lacked a decent mobile experience, hampering their ability to work flexibly from anywhere. Post-lockdown, secure remote and mobile access to core business applications and content has become a core expectation. Look for a solution that supports offline access to content, too, so professionals aren't interrupted in their work if they lose their internet connection.

8. Look ahead

Digital transformation isn't just about what firms want to achieve now. It's also important to consider future potential, especially as technology is advancing all the time. Beyond the cost and resilience benefits of consolidating document management and client engagement management in the cloud, firms might also look to automate more processes.

The Power Automate functionality in Microsoft 365, for example, is extremely powerful for streamlining and automating workflow. Firms can start by tying applications together so that data can flow more fluidly between them without manual intervention.

The future is uncertain, but one thing is for sure. Professional services firms can take real strides now towards a fully flexible digital future.

enel x

Energy management solutions that deliver commercial and environmental rewards

Global resources, local market knowledge and specialist technological expertise make Enel X the trusted energy management partner for data centres and large scale enterprises all over the world.

Join us as we pave the way for a cleaner, more dynamic future.

enelxuk@enel.com | www.enelx.co.uk