Software World
Database & Network Journal

THE SOFTWARE WORLD SERIES

Software World

An International Journal Of Programs & Packages

MAY
VOLUME 51
NUMBER 3 2020

PUBLISHED SIX TIMES PER YEAR

THE SOFTWARE WORLD SERIES

Software World

FIFTY YEARS

An International Journal Of Programs and Packages

Vol.51 No.3 May 2020

Editor: Steven Patterson

Linkedin
www.uk.linkedin.com

Published by:
A.P.Publications Ltd
58 Ryecroft Way,
Luton, Beds. LU2 7TU.
UK

Tel: 01582 722219

Website:
www.softwareworldpublication.com

Editors E-mail:
smpluton@ntlworld.com

Subscription Rates:

1 Year/2020
U.K. £135.00
Less Agency Discount £122.00

Overseas £161.00
Less Agency Discount £145.00

Single Copies:

£24.00 (U.K)
£29.00 Overseas

ISSN 0038-0652

Software World and Database & Network Journal are published in the Peoples Republic of China by the Shanghai World Publishing Corporation.

SOFTWARE WORLD INTELLIGENCE

We apologise for the delay in the arrival of some issues, and hope normal service will be resumed as soon as possible.

OPINION

Using Data and Analytics to Continue Business as Usual during Coronavirus.

Andrew Morgan, Head of Data Engineering at 6point6.

While the coronavirus pandemic is having a devastating impact on lives and wreaking havoc on the global economy, business leaders need to be aware of how to move quickly in order to protect their businesses. Responding at speed to this difficult situation allows companies to continue to operate as smoothly as possible, and in doing so, the jobs of their employees can be safeguarded. Data and analytics are usually a key driving force at the forefront of innovation, but in these times, they are even more imperative to navigate this most challenging of business environments.

Monitoring the teams' pulse

Operational success begins at home. A situation in which employees communicate entirely via computers and mobile phones presents new challenges. Millions of employee interactions that used to happen face-to-face every day are now taking place remotely. Now that communication and output are universally digital, organisations can use this interaction data to gain a new, comprehensive understanding of how their teams are coping and where support is needed.

> **Many business models work on a basis of estimating a team's effort, putting a valuation on this, quoting accordingly, and then carrying out the task.**

For example, many business models work on a basis of estimating a team's effort, putting a valuation on this, quoting accordingly, and then carrying out the task. Now that the work is all carried out online, analytics can be used to more accurately measure the previously hidden time spent dedicated to a specific operation. Using this new data can enable a more accurate costing process. In a time of greater uncertainty, the firms that are better at quoting, estimating, and keeping their promises of timeliness will surely impress customers that they are well managed, even in times of crisis.

These measurements can also be pooled to gauge the health and happiness of your colleagues. The platforms that now host people's entire working day provide insight and analytics that can be blended with analytics such as NLP (natural language processing) to provide meaningful insights into how employees are responding to any given situation These functions can help business leaders understand the internal mood of the company. By understanding employee welfare, management can move accordingly to keep their teams happy and thereby, the continued efficient operation of the business.

This does not mean an intrusion on privacy; such analytics retain employee anonymity. Certain programs, for example, search for keywords and emoji in employee messages, and the algorithms report in real-time on the sentiment being experienced across the team.

Responding to disruption

A significant supply chain risk is building up in business' networks. While data pipelines are running relatively smoothly, the current climate is placing considerable demand on resources such as bandwidth and storage. We have already seen examples of leading platforms taking the initiative and moving to mediate these strains, like Netflix reducing their resolution globally in anticipation of a streaming boom.

Meanwhile, coronavirus is disrupting operations around the world, affecting the movement of goods, the provision of services and labour, and forcing many companies to throttle down or even close in some instances, threatening jobs and livelihoods.

While shock to the supply chain is never good, all patterns and behaviour effects will be exhibited in data. Companies must look at ways they can use graph-based analytics in order to give a clear picture of their supply chain, spot issues, and plan work arounds rapidly.

Now is the time to ensure analytics and data are being used to provide a complete understanding of the supply-chain in detail. You will need to know anything from production capacities, to your supplier's suppliers, and the resilience of those businesses to changing economic conditions, as well as the alternatives available if any of these options are disrupted by the pandemic. Meanwhile, tracking purchasing power and competitor pricing, and indeed the other numerous global economic factors influencing demand for a business' goods and services, is all vital data.

By understanding supply chain trauma in detail, you can build models that help them navigate problematic scenarios. You can use valuable and up-to-date data to form contingencies and alter existing systems in order to both monitor, minimise the impact on business, and clearly communicate unavoidable impacts early to your own customers.There are numerous data products, data marketplaces, specialised data analytics solutions and companies providing expert consultation, available to provide insights and help integrate solutions into your business - and now is the time to invest in them.

Embracing external data

The ability to ingest data rapidly is key, especially in a world where there is an abundance of such data now flowing through data pipelines. External data has become a vital component to consider for business decision-makers.

> ***By absorbing from external sources effectively, you can bring this data into your own models, and adjust those models accordingly.***

Coronavirus, as a black swan event, will have invalidated many of the algorithms businesses typically use to make operational forecasts and other strategic decisions. Such AI tools are trained on previous data using year-on-year patterns, making it difficult for these algorithms to predict the effects of an unknown. In order to remain agile and pivot in response to the current crisis - and indeed future crises - businesses must alter their data practices to consume external data sets. By absorbing from external sources effectively, you can bring this data into your own models, and adjust those models accordingly. The pharmaceutical industry already observes this process of factoring in external data to inform its budgeting and forecasting. It uses epidemiological and demographic studies to inform its understanding of disease prevalence and impact. It then makes decisions around medicinal production and distribution based on those findings and its own models.

This is where data-sharing will be key. Academics are sharing both data and data science methods effectively, with initiatives launched for the sharing and collecting of Covid-19 data. Businesses must use all external data they can access to feed into their models and forecasting, to gain a more accurate picture of their supply chain and the impacts the business will suffer.

Collaboration could also be useful. In the same way that banks share data to create a person's credit score, retailers, for example, can work together to share data and better understand critical supply chains during the coronavirus. The coronavirus pandemic, while primarily being a human tragedy, is also having an increasing impact on the global economy. Yet business leaders can use data and analytics to ensure their companies continue to function smoothly in the evolving situation.

www.6point6.co.uk

●

Iskratel and Telekom Slovenije test their 5G Campus Network.

Iskratel and Telekom Slovenije are analysing the first tests of the 5G network they have built together to enable the smart factory in Kranj, Slovenia.

The joint solution has enabled the development of new business models and the testing of a smart 5G infrastructure. It connects a number of state-of-the-art virtual networks for individual business verticals, including smart factories. This is a key sector enabled by 5G, which will offer manufacturers and operators with significantly greater control and automation.

Kristijan Melinc, Sales Director of BU Core at Iskratel, said: "I am very proud we have deployed a 5G network in our own business environment. We leveraged our expertise in core networks and together with our partners shaped a complete solution that will allow us to address demands for campus networks in various industries. We were able to learn much more about the intricacies of 5G applications from our real-world installation rather than from theory or lab-style test projects."

Telekom Slovenije's Member of the Management Board, responsible for technology, Matjaž Beričič, MSc, said: "5G is an evolutionary upgrade of 4G. It enables the development of new and innovative mobile ICT solutions across industry verticals. Reliable, fast, and responsive wireless data transfer between devices will enable the industry to stay flexible and competitive. 4G / 5G technology enables advanced multimedia services, the development of the Internet of Things (IoT) services and the digitisation of business verticals - while providing reliability and cybersecurity from the outset. We plan the public mobile network in such a way that within one smart physical infrastructure we will enable state-of-the-art virtualised networks for different verticals - in different ways - as fully virtualised or as a hybrid public-private, so called "campus" network. With Iskratel, we have established a reference case in which we will be able to test different capabilities, implementations and new ideas for new opportunities on specific use cases."

In addition to both partners evaluating technical performance, the Institute for Non-Ionizing Radiation (INIR), an independent and accredited national organisation, also performed measurements of electromagnetic radiation of the 5G base station in Iskratel's production facilities. Measurements were performed at maximum base station traffic, with four test terminals that simultaneously performed a data rate test at the time of the measurements.

The results of the measurements show that the radiation exposure at all measuring points is far below the warning values set by the Regulation on the protection of workers from the risks related to exposure to electromagnetic radiation and the values set by Council Recommendations.

OPINION

Stark Digital Divide in Internet Speed Amid COVID-19, But ISPs Are Making a Difference.

Fastly Inc.

Fastly, Inc., a global edge cloud platform, have announced a February to April 2020 analysis of internet performance within median income brackets in the U.S. The first in a series of data analyses on the digital divide — the unequal distribution of internet access across socioeconomic and geographic lines — these findings uncover a clear stratification of download speeds, indicating households with lower incomes experienced lower download speeds compared to households with higher incomes. In the weeks since the onset of the COVID-19 pandemic, more and more people around the world are relying on the web for work and education from home, bringing the internet's inequities into sharper focus. A beacon of hope lies in recent internet service provider (ISP) decisions to upgrade internet speeds for lower income communities, which analysis shows has led to noticeable improvements in internet performance. Notably, Fastly's data only represents those who have some sort of residential internet connection, and does not include a group at the very heart of the digital divide issue — those without internet at all.

Findings show 22.3% of connections in lower income brackets still do not have acceptable internet performance during COVID-19.

"We hypothesized that internet performance would vary by income, but we were surprised to see such a stark stratification," said Fastly's Chief Architect and Founder, Artur Bergman. "Because of Fastly's visibility into telecommunications and ISP activity, as well as end user experience, we can connect threads that help to define the tangibility of the digital divide for many communities in the U.S. This becomes especially insightful as more and more people transition to a more web-reliant world in light of COVID-19. We observed relief for those segments of the population arise as a result of decisions from ISPs like Comcast and Cox Communications. Both implemented upgraded internet speeds in mid-March, which led to recognizable improvements in download speed for lower-income communities."

As Web-Reliance Increases, Low Income Communities Could Struggle With Connectivity

To understand the impact of the digital divide on low-income families during the COVID-19 pandemic, Fastly compared the median download speed between February 26 and April 21 for five brackets of annual average income. Download speed is a measure of the bandwidth that a user's connection to our server achieves, which is typically lower than the connection speed users signed up for with their internet providers. The analysis shows ZIP Codes with median incomes in the highest brackets are seeing the highest download speeds, compared to ZIP Codes with the lowest median incomes, which are seeing the lowest download speeds. This reflects that, among other inequities, people in higher income neighborhoods have both access to higher bandwidth connectivity and the means to use it.

*This is the FCC-recommended range for students and telecommuting, and the number of users is proxied by the percentage of connections. Date range evaluated is February 26 to April 21.

While an increase in download speed is seen within this date range in users of all income groups, users in the lowest income group saw the largest increase. This bracket had its median download speed increase from 13.7 Mbps to 17 Mbps, a 25 percent increase in download speed over a period of two months. Fastly analysis also shows that on February 26, 26.3 percent of the connections in the lower income bracket did not meet the minimum download speed recommended by the FCC for both telecommuting and online learning (five Megabits per second). However, from mid-March to mid-April, Fastly observed the biggest improvement in number of users without the minimum required download speeds in that same bracket, dropping from 26.3 percent to 22.3 percent.

ISPs Are Making a Difference

On March 14, Comcast announced it would increase the speed of its Internet Essentials service (a package that is offered to all qualified low-income households for less than $10 a month) from 15 Mbps to 25 Mbps. Prior to the announcement, the median user in the lowest income bracket saw download speeds at 27.2 percent lower than the median user in the highest income bracket. Post-announcement, the download speed gap between a median user in the lowest compared to the highest income bracket reduced from 27.2 percent to 13 percent.

Also on March 14, Cox Communications announced a similar decision, upgrading its residential internet packages to 50 Mbps for 60 days. Prior to the announcement, the lowest income median user saw download speeds at 13.9 percent lower than the median user in the highest income bracket. Post-announcement, the download speed gap between a median user in the lowest compared to the highest income bracket reduced from 13.9 percent to 1.8 percent.

Likely as a result of these ISP decisions, Fastly observed the median download speed of all connections in the U.S. has increased from 17.9 Mbps on February 26, to 19 Mbps on April 21, a 6 percent increase over a period of two months.

Check out the Fastly blog that explores an in-depth view of this data and other findings, and stay tuned for more analysis over the coming weeks.

Methodology and Sources

To cross-analyze income data to observed internet speed data, Fastly used public data from the IRS that allowed it to find the average Adjusted Gross Income per return filed with the IRS per ZIP Code for 2017. Fastly then classified ZIP codes into five categories based on the following thresholds: lowest = less than $30,000; low = $30,000-$49,999; medium = $50,000- $99,999; high = $100,000-$199,999; highest = $200,000 or more.

To calculate download speeds, Fastly used the TCP delivery rate (from tcp_info) measured at its servers, and filtered it as follows. Connections from large organizations that were clearly not residential connections were discarded. Only large connections (more than 100KB transferred) were considered, as well as the top and bottom five percentiles of delivery rate samples to discard outliers coming from estimation errors, night time usage, and from any non-residential connections left in the dataset. Fastly classified the resulting connections into the five income groups based on the ZIP code they originated from.

The speeds shown are aggregated across TCP connections (user connections) to Fastly servers. This means the download speeds shown represent what each user is seeing, which could be different than the bandwidth of an internet connection to a house. As a simple example, a single user over a 5Mbps internet connection and two users simultaneously using the internet over a shared 10Mbps connection might all be recorded as seeing a 5Mbps download speed. Fastly's analysis of the methodology used is that the bandwidth numbers in reality might be higher than what is reported. In other words, Fastly erred on the side of caution in practice being better than what is seen in these numbers.

www.fastly.com

●

Easyjet Phishing Attack; the Signs That Consumers Must Watch Out for.

Earlier this month, it was revealed a highly sophisticated cyber-attack compromised the data of nine million EasyJet customers.

While details are still emerging, EasyJet admitted its decision to go public (which it first came aware of in January 2020), was to warn customers, whose email addresses had been stolen, to be wary of phishing attacks. In light of this Chris Burden, Chief Commercial Officer, at UK-based, managed service provider, Memset, has offered advice to consumers of how to spot potential fraudulent emails.

"Social engineering comes in many forms and phishing attacks are one of the most common. The end objective is to induce targeted individuals to reveal confidential information, such as passwords or bank details. The fraudster attempts to access usernames, passwords, financial information come from disguised communications from what looks like a trusted person; the aim is to have a victim open a link that exposes a device and thus the sensitive information stored on it.

"For the EasyJet attack, it comes at a time when consumers are heavily reliant on digital communications. Unsurprising online purchases, product views and new email sign-ups have increased significantly since the start of the pandemic. Organisations will have strict guidelines and advice in place on how to spot potential phishing emails, but for consumers, they might not be aware of what to look out for. It's not unreasonable to think many would act on an email instruction without second thought, leading to that person becoming compromised.

"For those, concerned there are definite tell-tale signs to look out for.

"Firstly, always be wary of emails from an unknown person asking for sensitive or personal information. Your bank for example, will never ask for your personal information over email or phone. Equally, never share your passwords ever.

"A big giveaway with phishing emails is often the spelling and punctuation – does the tone and language look familiar of the person you 'know' is sending you the email? Additionally, check the spelling of the person's email address, or whether their email address has been shortened. At a quick glance it might appear right, but on closer inspection you can see errors – this is usually one of the biggest giveaways of a phishing attack.

"If you are directed to an alternative site, make sure of that site's legitimacy. Many slightly change a link name to ensure trust, but on closer inspection does not match previous domains used. And finally, if something looks suspicious, simply don't open it and delete it.

www.memset.com

●

OPINION

Preparing and Supporting Your Cloud for the COVID-19 Remote Workforce.

Brian Ussher, President & Co-founder, iland.

As a result of the COVID-19 pandemic, we are witnessing an unprecedented increase in home working, which requires remote access for tools and communications to conduct our daily jobs. This disruption is putting IT infrastructures at risk, while validating much of the industry's investment in business continuity, resilience, scalability, accessibility, data protection and security.

With a global at-home workforce now entirely in place, what can IT professionals and CIOs do to ensure their private and public clouds can keep up and remain safe? And what steps and tests should they take to support a protracted change in the way we work? According to a recent Gartner survey, more than 74 percent of CFOs and business finance leaders expect at least five percent of their workforce will never return to their usual office workspace — becoming permanent work-from-home employees after the pandemic ends.

> ***Even in the face of a global pandemic, we continue to promote a culture that requires easy and instant access to our tools.***

Even in the face of a global pandemic, we continue to promote a culture that requires easy and instant access to our tools, information and each other over cloud collaboration tools like Slack, Google Drive, Office 365, Microsoft Teams, as well as in-house applications.

This demand on IT requires private, public and hybrid clouds to have the agility, scalability and security to support entire workforces no matter where they are. IT leaders who have planned for this worst-case scenario are ready to scale at a moment's notice. Likewise, they've already considered the impact on licensing, vulnerability and added traffic from employees working at home over personal devices and unsecured networks.

IT professionals who support an at-home workforce need to understand the difference between employees "running" applications and "accessing" applications. When technology is set up and configured correctly, it should be easy to access. That's the whole idea of SaaS and cloud. The challenge is, how do you administer it? How do you run it?

Organisations that maintain private clouds onsite, which might not be accessible during stay-at-home orders, need a plan to make repairs physically — like swapping hard drives, replacing switches or cables — when their employees are home.

Likewise, whether at home or work, the end-user experience should be the same. If all apps and tools are optimal in an office environment, how do you make those adjustments ahead of time, so remote employees still have the same access and capabilities as if they're working in the office? And how do you maintain your security and IT compliance obligations?

Where and how to start?

The easiest advice might be to avoid trying to boil the ocean all at once. If your applications and data aren't on the cloud already, it's possible to mobilise secure VPNs and encrypt applications for mobile devices. If you're on the cloud already, you're several steps ahead of others. But you still need to work with your cloud service provider to review your workloads, applications, and data requirements.

At the same time you're focusing on accessibility, remember to address your vulnerabilities. Right now, cybercriminals are stepping up their attacks to take advantage of remote employees. Phishing attacks are at an all-time high on small and large businesses, as well as public resources like hospitals and healthcare providers.

Now's the time to reinforce your organisation's IT security and compliance guidelines, many of which include the relevance of when employees travel or occasionally work from home. This includes a refresher on password policies and how to identify and report phishing attempts. Help employees with securing their home networks, and all the other policies and guidelines they would typically follow at work to protect your company and customer data. This might also be an excellent time to train employees on document and data retention best practices.

COVID-19 will create additional security threats as attackers attempt to take advantage of employees spending more time online while at home and working in unfamiliar circumstances. Some of the biggest threats associated with the pandemic include phishing emails, spear phishing attachments, cybercriminals masquerading fake VPNs, remote meeting software and mobile apps.

Above all, you must have the same level of resilience and redundancy plans in place for home working as you do for onsite, even if you are 100 percent in the cloud. It is important to recognise that the same problems that happen on a day-to-day basis when you're in the office can also occur when the office is vacant.

Prepare for the new normal

Going forward, all businesses should plan for an eventuality like COVID-19 happening again. This means understanding data security, business continuity, resilience, scalability, accessibility and so much more. For example, you may not need extra capacity and compute power now; but you need to know that within minutes you can get to that number. And, as I mentioned earlier, a lot of organisations have internal-only networks to manage power supply, fans, cooling and switches. What if you can't get into the building?

Futureproof and understand the boundaries between personal and company devices and assets. Understand what you need to put into place to protect your business and your employees.

And finally, companies that are leveraging cloud services need to communicate frequently with their providers to address future needs and concerns. Make sure you know what they can do ahead of time to keep your remote workforce operating. Hopefully, these circumstances will be short-term, and life will return to some normality soon, but my advice is to always plan for every eventuality and what may now be the new normal.

www.iland.com

●

Global Cloud IT Infrastructure Spending will Touch $70bn This Year.

Cloud computing has surged in recent years, changing the way people communicate, manage data and do business. Billions of private and business users take advantage of the on-demand technology.

However, with coronavirus lockdown rules in place and millions of people spending more time indoors and online, the global demand for cloud services has soared over the last few months. This growing need for cloud solutions has led to increased spending on hardware and software components needed to support the computing requirements.

Global cloud IT infrastructure spending is expected to grow 3.6% year-on-year, reaching $69.2bn in 2020, according to data gathered by LearnBonds.

Cloud Infrastructure Spending Has Tripled Since 2013
Today, billions of people use personal cloud storage to manage and store private data. However, its ability to provide access to computing power that would otherwise be extremely expensive has seen cloud computing technology spread widely in the business sector, also.

The examples of cloud computing use can be found practically everywhere, from social networking, messaging apps, and streaming services to business processes, office tools, chatbots, or lending platforms.

In 2013, the global spending on cloud IT infrastructure, including hardware, abstracted resources, storage, and network resources, amounted to $22.3bn, revealed Statista data and the International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker. Over the next four years, this amount grew to $47.4bn. The trend has continued to grow strongly so that global cloud IT infrastructure spending has tripled since 2013.

IDC`s report revealed that public cloud infrastructure spending is expected to drive the global market growth this year.

Research director of Infrastructure Systems, Platforms, and Technologies at IDC, Kuba Stolarski said: “As enterprise IT budgets tighten through the year, the public cloud will see an increase in demand for services.

This increase will come in part from the surge of work-from-home employees using online collaboration tools, but also from workload migration to the public cloud as enterprises seek ways to save money for the current year. Once the coast is clear of the coronavirus, we expect some of this new cloud service demand to remain sticky going forward."

IDC's five-year forecast predicts cloud IT infrastructure spending will reach $100.1 bn by 2024, growing by a compound annual rate of growth of 8.4%.

Almost 80% of Businesses to Adopt Cloud Technology in 2020.
The growing need for cloud solutions recently has led to a surge in the vendor revenue from cloud IT infrastructure. In 2019, they made a $63.97bn profit from selling these IT products and solutions, 30% more compared to 2017 figures. The 2019 data also showed that ODM Direct held 32% of the market. Dell Technologies and HPE follow with 16% and 11.7% market share, respectively.

According to a global CIO survey, public cloud adoption was the key draw for many companies in 2020, with 79% of polled groups planning to make heavy to moderate adoption of cloud technology. AI/machine learning ranked as the second-most wanted technology, with 72% of firms planning to use it in 2020.

Statistics show that 70% of businesses plan to adopt private cloud solutions this year, followed by 63% of companies who prefer multi-cloud solutions.
www.learnbonds.com

Report: The Universal Language of IT.

SolarWinds Inc.

SolarWinds have recently released the findings of SolarWinds IT Trends Report 2020: The Universal Language of IT. This year's annual report studies how the breakdown of traditional IT siloes has affected technology professionals across on-premises, cloud, and hybrid environments. While the survey data was gathered before the COVID-19 (or Coronavirus) pandemic elevated technology professionals as essential workers, the findings are underscored by this challenging period of remote work and increased burdens on the IT environments keeping global organisations operating at full capacity. The study reveals a new reality for tech pros where roles have converged yet budgets remain focused less on emerging technologies and more on infrastructure, hybrid IT, expanding their charter from operations to optimisation.

As cloud computing continues to grow, tech pros say they are increasingly prioritising areas like hybrid infrastructure management.

The "universal language of IT" encapsulates the evolving role of technology in business, and the tech pros' responsibility for ensuring overall uptime, availability, and performance as well as greater partnership with leadership to drive business success. As cloud computing continues to grow, tech pros say they are increasingly prioritising areas like hybrid infrastructure management, application performance management (APM), and security management to optimise delivery for the organisations they serve. With the convergence of IT roles in response to the interconnected nature of modern IT environments—and now the need to support a new or larger remote workforce—tech pros are also setting their sights on non-technical and interpersonal skills to ensure teamwork and communication with business leaders increases their fluency in the universal language of IT. Skills development is needed across both technical and non-technical areas to remain successful in today's environments.

"For years we've been talking about hybrid IT and what it means for tech pros; in our seventh year of the IT Trends Report, we see the effects of hybrid IT in breaking down traditional siloes and bringing core competencies across on-premises and cloud environments together," said Joe Kim, executive vice president and global chief technology officer, SolarWinds. "Especially now, when organisations worldwide are facing new challenges and uncertainty, we must take this reality seriously, focusing on skills development and readiness in key areas like security, cloud infrastructure, and application monitoring. While IT continues to be a main driver of business importance, tech pros have an opportunity to help reassure the business and focus on effectively communicating performance now and into the future."

"More than ever before, technology professionals must work alongside business leaders to meet organisational goals while also investing time and energy into cultivating the necessary skills to drive business success," added Kim. "At SolarWinds, we focus on enabling the tech pro with easy to use, affordable products, but we also understand our customers often need more from our partnership. That's why we also make meaningful investments in providing a wide range of training resources—many of which have been virtual since their inception—and an online user community where they can connect with their peers. We have many ways we do this: our Customer Success Center, MSP Institute, SolarWinds Academy, our THWACK® community of over 150,000 registered members and yearly virtual learning event, THWACKcamp™, our bi-annual customer event SolarWinds Empower MSP, and educational digital programming like SolarWinds Lab™ and TechPod™. Each of these avenues serves to help make life easier for tech pros so they can drive even more success for the businesses they support."

2020 Key Findings

SolarWinds IT Trends Report 2020: The Universal Language of IT explores priority areas tech pros manage in a world were roles have converged, and how this reality is affecting skillsets across IT departments and in non-technical areas. Key findings show:

Tech pros are focusing less on emerging technology like artificial intelligence (AI) and edge, and more on hybrid IT and security.

- The top three technologies influencing organisations' staffing needs (by weighted rank) are:
  - o Cloud computing (i.e., SaaS, IaaS, PaaS) (48%)
  - o Security and compliance (57%)
  - o Hybrid IT (39%)
- Only a collective 16% name emerging technologies—like AI, edge, microservices, and containers—as the biggest influence on staffing needs.

• This makes sense when you consider organisations aren't allocating their budget to emerging technologies—particularly as this year's budgets are reevaluated in the face of economic challenges. Nearly three-fourths (71%) indicate their organisations' tech budgets allocate less than 25% of their spending to emerging technologies.

Today's hybrid IT reality has created a universal language of IT where tech pro roles and siloes converge, and complexities are exacerbated by flat to shrinking budgets and a lack of qualified personnel.

• With the convergence of technologies and responsibilities, the top three ways tech pro roles have changed over the past three to five years are:

o Increased work week hours (42%)

o Increased responsibilities outside the firewall (33%)

o Need to retrain existing staff (32%)

• At the same time, tech pros are experiencing barriers to successfully supporting their organisations, including:

o Lack of budget/resources (41%)

o Unclear or shifting priorities (17%)

o Currently offered IT management/solutions lack features/functionality to meet my needs (15%)

• What's more, over one-third (39%) of respondents believe tech pros entering the workforce today don't have the necessary skills to manage modern, distributed IT environments.

Many personnel and skills issues relate to growing areas like APM and security and compliance.

• Sixty percent of tech pros/teams/IT departments are spending more time managing apps and services rather than infrastructure and hardware. This represents a monumental shift in the strategic importance of applications to the modern business.

• This growth in the influence of cloud applications on IT and managed services will continue to rise: according to Gartner, by 2022, as many as 60% of organisations will use an external service provider's cloud managed service offering, doubling the 2018 figure. Gartner also predicts the ongoing effect on skills: by 2020, 75% of enterprises will experience visible business disruptions due to infrastructure and operations (I&O) skills gaps, which is an increase from less than 20% in 2016.

• When organisations adopt cloud and/or SaaS technologies, 57% use network traffic analysis/network app analysis, 57% use user experience monitoring, and 44% use log analysis as their top three approaches.

• When it comes to APM tools, 42% use a mix of native tools (provided by the cloud service provider) and third-party tools. Nineteen percent use only native tools and 13% use only third-party tools.

o More complexity equals more APM: enterprise businesses are more likely to use log analytics tracing and network traffic analysis/network app analysis.

• For 66% of tech pros, at least 10% of their daily responsibilities include IT security management. At the same time, the top three areas of security skills management tech pro organisations are prioritising for development include (by weighted rank):

o Network security (43%)

o Security information and event management (SIEM) (30%)

o Backup and recovery (28%)

• Similar to the way the universal language of IT has affected IT departments, compliance policies have resulted in 35% of tech pros adding additional IT staff.

• Compliance policies with the greatest effect on IT departments include:

o GDPR (92%)

o PCI DSS (32%)

o SOX (14%)

Tech pros need to develop nontechnical skills to operate within the universal language of IT reality where cross-functional and business-level communication is necessary.

• The nontechnical skills tech pros feel are most critical to successfully manage today's modern IT environments include:

o Project management (61%)

o Interpersonal communication (57%)

o People management (54%)

• These results are echoed by CIO's annual State of the CIO Survey, which revealed the top skills needed for digital transformation were strategy building (40%), project management (32%), and business relationship management (25%). These critical interpersonal skills become more important as tech pros increasingly communicate and collaborate across previously siloed IT functions.

• According to the LinkedIn® 2020 Emerging Jobs Report, the demand for soft skills like communication, collaboration, and creativity will continue to rise across the SaaS industry.

• Despite the budget and skills issues tech pros report, 89% of surveyed tech pros say they're comfortable communicating with business leadership when requesting technology purchases, investing time/budget into team trainings, and the like.

To explore and interact with all of the 2020 findings, visit the SolarWinds IT Trends Index, a dynamic web experience presenting the study's findings by region and additional insights into the data, plus charts, graphs, and socially shareable elements.

Additional Resources
• SolarWinds IT Trends Report 2020: The Universal Language of IT
• SolarWinds IT Trends Index

www.solarwinds.com

●

OPINION

Seven Security Mistakes Organisations Make When Adopting Cloud.

Roy White, Senior Cloud Consultant at Cloudreach.

The COVID-19 pandemic is forcing businesses to tackle a variety of sudden technical and organisational challenges. Some may need to scale up remote working capability, others may need to address demand spikes on critical applications. Some may even need to pivot their entire business.

The use of public Cloud may well provide the capability to rapidly address these challenges, to help extend the current operational environment in a hybrid model or create an entirely new footprint within the Cloud. While there certainly are benefits to accelerating the move to the Cloud at this critical point, there are also many risks to be aware of.

An understanding of Cloud best practices, especially regarding security and governance, should be at the forefront of any changes.

For example, many organisations now use publicly available libraries on GitHub to develop applications faster.

The following are common mistakes organisations make when adopting Cloud:

Mistake #1: They approach security the same way they do for on-premises data centers
An on-premises environment is typically owned 100% by an organisations' internal security team and protected by firewalls and perimeter-based solutions like IDS/IPS to form a trusted network. In a Cloud environment, there is no concept of assuming data will have a moat around it. CSPs know this and they purposely build their solutions with security in mind from the foundation with a defense-in-depth model delivered by security being applied across multiple layers. When moving to a public Cloud, IT leaders should take time to review their entire IT architecture and carefully determine what workloads could most benefit from a move to the Cloud.

Mistake #2: They don't view security as a shared responsibility
When organisations move to the Cloud, they often assume the CSP will handle all aspects of security. But moving to a Cloud doesn't absolve your organisation of security responsibilities, and accountability will always reside with the organisation. Security in the Cloud is a shared responsibility, and all parties must play their part. To keep data secure, an organisation must have the right capabilities in place to effectively manage risks. Capabilities are formed of people, processes and eventually tools. Cloud Governance policies and security processes need to be in place to provide an organisation with the guardrails it needs to operate effectively without putting the system at risk. Finally, tools should help support all of the above - providing detailed analytics on usage to prevent data risk and compliance violations, drive enforcement and quarantine if a violation occurs, and provide real-time threat intelligence.

Mistake #3: They don't secure and restrict access to the Cloud platform
Access control is a vital component of Cloud security. Only the relevant people should have access to the Cloud platform itself and should have only the level of rights needed to carry out their role. To maintain proper security, an enterprise should adopt a privileged access protocol. In other words, identify all possible forms of access that are required for system and data and ensure that the controls applied meet the system requirements from open access to public website type data to authenticated access for internal users applications to highly controlled privileged access accounts which may have access to the heart of your data and applications. Then, put processes in place to mitigate exposure and ensure only the right users can access Cloud data and applications including managing the full account cycle from creation to deletion of no longer needed accounts

Mistake #4: They don't focus on the security of the entire supply chain
Threats from external supply sources come in many forms. For example, many organisations now use publicly available libraries on GitHub to develop applications faster. But, using code of unknown provenance, if not fully understood and verified, can lead to insecure applications. While this issue isn't restricted to organisations that use Cloud, it is a growing challenge among enterprises. It's not always easy to verify the security of the code you use, but doing so can ensure you don't open your company up to security problems. Make sure whatever tools you utilise from an outside source – whether it's code, hardware, software or something else – doesn't introduce new security issues.

Mistake #5: They don't work as a team
Today's heightened threat environment requires everyone to take responsibility for security. Rather than work in a

silo, an enterprise security team should collaborate with their CSP to develop an enterprise-wide security strategy. The support and external knowledge a CSP offers can help the enterprise keep abreast of the latest threats and help it address potential resource, skill or time shortages.

This shared responsibility model must also be applied within the organisation itself. Leadership teams should work with developer teams and other internal IT personnel to share security knowledge and responsibilities. This is especially important as more organisations utilise hybrid Cloud models. A single security team is not enough to protect a combination of public Cloud, private Cloud, and on-premises IT environments.

Mistake #6 They don't have the right skills
As we have established throughout this post, security in the Cloud requires a very different approach to security running on a physical network. A different approach demands a different set of skills. Your traditional security team would be isolated, working on policies, configurations, and protocols separate from the rest of the IT team. When you are in the Cloud you need your security professionals to be able to deploy and manage Cloud-native solutions with an understanding of the distribution and elasticity of Cloud architectures. They also need to be integrated with your Development and Operations teams (DevSecOps) ensuring security is built into applications and infrastructure. This requires a technical skill set and awareness beyond just that of network security strategies and traditional security tools.

Mistake #7 They don't balance speed with risk mitigation
This is particularly relevant in the current climate in response to COVID-19 where organisations are rapidly upscaling or adopting new tools and working practices. While this rapid change may be necessary, be wary that there will also be a lot more opportunist, bad-actors, trying to capitalise on business trying to overcome their current challenges.

At this time it is important to remind colleagues of security best practices and risk management. Crisis events are prime time for Social Engineering ploys like Phishing emails that play off people's fear and desire for more information.
The goal is to achieve the right balance of acting fast while not exposing your business to unnecessary risk.

www.cloudreach.com

●

Majority of Application Development Teams Rely More On SaaS Services vs. Building In-House.
Auth0 recently released a 2020 State of Application Assembly survey, revealing that a majority of development teams are turning to best-in-class SaaS services and the adaptability of APIs for building unique features and functionalities into the many apps they are responsible for each year.

Surveying 426 global technical professionals across a variety of roles (developers, engineers, CTOs, directors of engineering, software architects) and company sizes, Auth0 determined that 51% of respondents are responsible for building two to five apps per year, and more than a quarter (28%) build 6-10+ apps per year, with three-quarters of these apps being used for external audiences. There are currently more than 4.1 million apps available on leading app stores (Statista), indicating the staggering amount of development these builders are responsible for.

The survey explored application builder behavior around several services and key findings included:

For applications that required payment, 74% of respondents outsourced, with Stripe being the dominant tool of choice.

For applications that required messaging, 71% outsourced this solution, with Twilio being the highly preferred tool.

The third service explored was authentication, cited as a requirement in 83% of applications built. However, the numbers for outsourcing authentication were lower than the other two services, with respondents outsourcing 58% of the time.

With a substantial percentage of companies still building authentication tools in-house – and because authentication is present in the majority of apps – there's a large potential opportunity for application building teams to streamline their processes and improve efficiency by using a third-party IDaaS tool.

The accelerated timelines that come with app launches are driving teams away from in-house development and towards microservices – app 'building blocks' – that provide features and functionality that would be nearly impossible to build and maintain themselves. Relying on third-party services that are adaptable to their specific needs, significantly frees the team's resources to focus on core innovation and speed-to-market.

"These results confirm a trend of application development teams increasingly relying on first- and third-party APIs and external SaaS services when assembling apps, to simultaneously decrease time-to-market and increase completeness and security," said Martin Gontovnikas, VP at Auth0. "Whether it's payments, messaging, or authentication, this survey shows that teams are turning more to a 'must-have SaaS stack' to expedite development and enable them to focus on their core product."

By 2022, 90% of all apps will feature microservices architectures that improve the ability to design, debug, update, and leverage third-party code. Combined with agile/DevOps approaches and methodologies, enterprises can dramatically accelerate their ability to push out digital innovation – at 50-100x (or more) the frequency of traditional approaches (IDC).
www.auth0.com

●

Why One Iaas Provider Is Not the Same as Another - 10 Aspects to Consider When Moving to the Cloud.

Justin Augat, Vice President Product Marketing, Iland

Saying "yes" to a cloud strategy is the easy part. Eliminating on-premise infrastructure and management overheads in favour of greater agility, efficiency, security, connectivity, cost-savings and more makes a great business case. However, once the strategy is signed off, the hard work begins: how to choose a cloud provider to deliver IaaS that is "just right" for your business? That's when the huge array of different providers and options can start to obscure your vision and make supplier due diligence a problem.

Comparing quotes and services from competing providers without a strong understanding of your business objectives and success parameters can quickly result in decision paralysis or, if you rush the process, the risk that you may end up overpaying for unused resources or compromising on performance as a result of budget constraints. And that is the opposite of what the cloud should be about. Your "just right" cloud provider should deliver a service that fits your objectives like a glove and offers the right level of performance at the right level of investment. Below are ten key aspects to consider when conducting due diligence and selecting the provider that's right for your business.

Finally, check that the data centre location provides adequate distance between primary data and backup data in case you need to activate disaster recovery.

1. Global access and availability: laws, latency and location

When your data leaves your on-premise data centre, there are likely to be limitations on where it can go. If your data needs to be physically held by law in a specific geography, you need to confirm with providers that they can accommodate this. And, once you know where the data is, you need to verify that this location won't create latency or bandwidth issues that will negatively affect performance. Finally, check that the data centre location provides adequate distance between primary data and backup data in case you need to activate disaster recovery.

2. Cloud management:

Once you have your cloud you need to manage it, but how straightforward will this be? You'll want to know how easy the management interface is to use. If it is API/CLI-driven, do you need to allocate internal resources to manage it? Will training be required and will the provider deliver this? What level of control and visibility is possible from the management interface into billing, performance and security?

3. Application performance:

Analyse your applications and determine where the balance between performance and budget lies for each. Mission-critical apps that need high performance and zero latency require more resources and therefore expenditure, whereas a lower priority app used less frequently does not need the same level of guaranteed availability. This analysis is critical to hitting the custom-fit "just right" sweet spot and avoiding costly over-provisioning or performance-destroying under-resourcing. Think about how your business might scale in future rather than about your requirements just now. Ask the provider how they'll help you find the balance between performance and cost. If you have applications licensed on the basis of core CPU count, can the provider offer server blades with fewer CPU cores to match the license core count, to avoid paying for redundant resources?

4. Security and compliance:

Cloud today is generally accepted as offering robust security and compliance, but as the environment matures and regulations intensify, customer requirements become more nuanced, meaning the standard security provision may not be sufficient. You want a provider that is as expert – if not more so – on the regulations and restrictions that your business must comply with as you are. Data sovereignty, industry-specific regulations and general data protection issues are complex and you should be seeking a provider that can offer a consultative service so you can evolve together to ensure long-term security and compliance.

5. Data Back-up and Disaster Recovery:

Not all cloud providers include data backup in their basic cloud service, instead bolting it on for an extra cost. That can come as an unwelcome surprise when you think you're getting the whole package. Make sure you understand what backup capabilities the provider offers – both full and incremental – and whether they are safely located. The same goes for disaster recovery and this is a key part of supplier due diligence. Do they have a second data centre for disaster recovery and is it far enough away from the primary site to be unaffected by a physical interruption there.

6. Connectivity and networking:

When assessing connectivity and networking impacts, it's important to understand what skills you have in-house and whether there are any deficits that will cause your team difficulties. You also need to understand business requirements and what the cloud service provider's capabilities are. For example, many organizations have advanced network topologies that require the usage of specific carriers, virtual or physical equipment, co-location and software defined network options.

7. Strategy and planning:

Central to meeting your business objectives is the question of whether your applications are suited to the cloud IaaS you are planning to adopt. This comes with a raft of sub-questions, such as what CPU, memory, storage, bandwidth will they need, and can they be suitably backed up to achieve the required RPO/RTO objectives? It can be useful to seek providers' support to cover all these angles for all your applications and develop a strategy, otherwise you will need to allocate internal resource or a third party consultant to get all this information and interpret it into a migration strategy.

> ***Many organizations have advanced network topologies that require the usage of specific carriers, virtual or physical equipment, co-location and software defined network options.***

8. Onboarding and deployment

When it comes to pushing the button on your cloud deployment, will you be doing it yourself, or being supported by your provider? Different providers offer varying levels of support, from DIY to a full concierge onboarding and migration service, at different prices. It's vital you know where you are on that scale and how much or little in-house resource will be needed. Your choice might depend on how much appetite there is for the inherent risks of migration, such as application downtime. If appetite is low, you're going to want a provider who can guarantee that data is moved on time, with minimal risk.

9. Support:

Think about the level of support you need. How much internal resource do you have, and how much might you need to draw on your provider? Again, all providers are not the same. Most offer a basic support package, but anything beyond that comes at an extra cost. As the world moves to increasingly diverse working hours due to the effects of the COVID-19 pandemic, 24/7 support is going to become more critical and you want to have visibility into that before you make the leap.

10. Pricing/Billing

Cost visibility is one of the oft-touted benefits of the cloud, so it's frustrating that pricing and billing can often be so obscure and variable. During the due diligence process ask to see a sample billing statement broken down by line item. Make sure you delve into the pricing variables in the service, whether it is all-inclusive or what extra charges you might incur.

Ultimately, moving to the cloud is all about removing the overhead and limitations of on-premise infrastructure. All the factors discussed above might seem like a huge amount to consider but, when you look at the strategic benefits and value that a cloud strategy will deliver to the business, spending time to get your cloud "just right" is well worthwhile. It soon becomes clear that all IaaS providers are not the same. Taking time now to conduct robust due diligence of providers and drill into exactly what they can offer reduces the chance that the business will make a decision that causes problems in the long term.

www.iland.com

●

The University of Texas System Tackles GASB 87 Compliance with Planon.

Planon, a leading global provider of integrated software solutions to enhance real estate and facility management processes, announced that The University of Texas System has selected Planon's Lease Accounting solution to adhere to the GASB 87 lease accounting standard for public organisations in the United States.

The software solution will support the UT System, which is one of the largest systems of higher education in the nation with 14 institutions, student enrolment of almost 240,000 and an annual operating budget of $21.1 billion.

The UT System was in search of a common platform with the ability to calculate the amounts required by the new accounting standards and to integrate with its ERP. The UT System examined several vendors and solutions for GASB 87 (GASB 87 is legislation for public organisations and universities in the United States, related to the standards for ASC 842 and IFRS16) to find a dependable long-term partner.

In 2019, new lease accounting standards were introduced, altering the way that leases are recognised, measured and reported. The main change is that lease payments are no longer recognised as expenses, but assets and corresponding liabilities are calculated and reported on the balance sheet (except for low-value assets or lease terms of 12 months or less) using the single accounting model. GASB 87 has removed the distinction between finance and operating leases for lessees.

'The UT System is committed to maximising efficiencies at its eight academic universities and six health institutions,' said Fred Guelen, President of North American Operations at Planon. 'Planon is proud to support the UT System with our GASB 87 Lease Accounting solution.'

www.planonsoftware.com

IP DEVELOPMENTS

New Geolocation Feature in IP Address Market.

Heficed.

Heficed have introduced the new IP Search feature, accessed via the IP Address Market, which will allow to search and filter IP Addresses based on their location. This is particularly relevant for VPN services, Telcos, hosting providers, ISPs and other industries, whose service quality heavily depends on access to accurate and timely data. By enabling to pinpoint IPs with a city-level accuracy, the new feature will enable us to better control website traffic, affirm user access to location-sensitive content, better implement cybersecurity measures and optimize the overall end-user experience.

Each IP Address is associated with a specific location, upon which the user is granted or denied permission to access certain Internet content. Hosting providers and ISPs leverage this data to control website traffic by seeking out scammers and blocking malicious IP addresses. In addition, they can control people that reach the site by making it accessible to a limited number of countries, for example, due to regulatory compliance (GDPR). Geolocation is also an imperative part of businesses, offering access to region-specific content, such as Netflix, which displays tailor-made show selection based on the user's whereabouts.

Data-driven personalization has become a significant factor in determining the success of a business, and it can be delivered by leveraging accurate IP location data. Seeking to offer more flexibility during the IP selection process, Heficed integrated its IP Marketplace with a few IP geolocation databases, enabling to conveniently search among the subnets and filter them by location. Moreover, integrating its product with third party databases presents the means to ensure data accuracy and prevent compromised IP addresses from entering the IP Marketplace.

"There are a lot of intricacies that need to be factored in when building an IP infrastructure. Locality plays an imperative role here, as a more deliberately chosen location can ensure higher connectivity and better reach," said Vincentas Grinius, CEO of Heficed. "The new feature will allow IPSs and hosting providers to make more informed decisions, as well as significantly cut down time spent on the IP selection process."

Enabling previously locked up IPs to reenter the market alleviates some of the pressure on the network, which leads to a better experience for the end-user.

The concept of leasing IP addresses is unique in the IT industry, however, it benefits a range of parties involved in the network infrastructure. IP Address Market makes network resources accessible to a wider range of companies, which previously may have been lacking funds to acquire the necessary IPs. Furthermore, it acts as a facilitator for all business entities that want to monetize their unused IPv4 address pools and obtain an additional stream of revenue. Currently, the market is under a strain due to IPv4 shortage and continuously skyrocketing usage, influenced by the COVID-19 crisis. Enabling previously locked up IPs to reenter the market alleviates some of the pressure on the network, which leads to a better experience for the end-user.

Heficed is a strong advocate for sustainable internet and its governance, as the company places a lot of emphasis on validating the accuracy and consistency of employed data. Previously Heficed introduced IP Abuse Management, seeking to identify malicious cyber threats and terminate them before any data breach could occur. The feature is included in the service package by default, to ensure better protection of its clients' IP resources and an overall more secure infrastructure.

In the near future, Heficed is planning to introduce several new features to the IP Address Market, one of them being Take Away IPs, which will enable clients to use the leased IP addresses on third party networks. Regular IP health checks are also on the list of upcoming updates, as they will help prevent addresses, associated with any malicious activity, from entering the Marketplace; IP resource holders will receive timely reports with a detailed overview of verified IPs. Finally, the company is working towards implementing the Bring Your Own IPs (BYOIP) functionality, enabling clients to use and monetize their personal IPv4 resources within the infrastructure provided by Heficed. The end goal is to have these processes completely automated, eliminating the need for manual supervision to maintain their operability

www.heficed.com

●

The Data Centre of the Future.

Three emerging technologies that are changing data centres.

Data centres are expected to use 20 per cent of the word's energy by 2025. While companies across the world depend on them to store data, there are new technologies that can improve their energy efficiency and operational effectiveness, if we take advantage of them. Here Neil Ballinger, head of EMEA sales at automation parts supplier EU Automation, explores the data centre of the future.

During the dot-com bubble of 1997 to 2000, companies needed fast and consistent internet connectivity to establish a presence online. Installing the equipment to do this was not viable for many small companies. Internet giants at the time started building large facilities, then known as internet data centres, to provide these businesses with data storage solutions. Since then, data centres have become smarter and more efficient. But, what emerging technologies are set to shape the next generation of data centres?

According to the DataAge 2025 study, almost 20 per cent of data created will be real-time in nature by 2025.

Sitting on the edge.

According to the DataAge 2025 study, which was recently commissioned by Seagate, almost 20 per cent of data created will be real-time in nature by 2025. This means that manufacturers need to build on their central cloud computing architecture and develop the ability to process and secure more data at the edge.

With edge computing, data analytics is only partly reliant on network bandwidth as most of the computing takes place locally — either in the device itself, the edge data centre or in the fog layer. Naturally, this will increase the speed at which this data is processed and becomes available.

Huge data centre models won't become obsolete, but the rise of edge computing could see a large number of small data centres built closer to industrial sites and business parks.

Keep cool.

Thermal management of high-power data centres poses a challenge for data centre managers, due to the high operational costs associated with an inefficient facility. Typically, server rooms in data centres are cooled using classic ambient air-cooling with cold water-recirculation coolers. For high power applications, water-cooled racks are used too.

Water and hybrid air plus water cooled data centres are an alternate cooling solution. This method combines liquid cooling systems, such as rear door heat exchangers located within the racks themselves, with a traditional raised floor cold aisle air cooling system.

Such a solution may be used when the equipment in a data centre is upgraded to higher end or higher power equipment, which may not be manageable with the existing air-cooling system.

Using artificial intelligence.

Artificial intelligence (AI) technology has existed for decades but is now going mainstream thanks to the advent of big data, deep learning algorithms and AI-focussed processors. The technology can now be used in conjunction with data centre infrastructure management (DCIM) software to analyse power consumption, capacity planning and cooling, as well as the overall health of critical systems.

AI can also help to reduce energy consumption. Google recently acquired DeepMind, an AI start-up, to use the technology to reduce costs and improve efficiency in its data centres. The system was able to achieve a 40 per cent reduction in the amount of energy Google used for cooling the data centre.

According to the International Data Corporation (IDC), half the components in large data centres will offer integrated AI functions by 2022, allowing them to operate autonomously. This, along with the other emerging technologies making their way into data centres, could drastically reduce energy consumption in these facilities, improving their functionality and reliability for businesses across the world.

www.euautomation.com

●

NEW DEVELOPMENT

The Latest V2I Cooperation For Smart City.

RoboSense.

RoboSense, a leading autonomous driving LiDAR perception solution provider, has teamed up with DT Mobile, the China's top communication equipment manufacturer, on the deployment of the first Vehicle-to-Infrastructure (V2I) solution based on the MEMS solid-state LiDAR in Xiong'an New Area, Hebei, China, which marks the beginning of MEMS solid-state LiDAR to be used in V2I projects. Prior to it, there are several pilot projects of RoboSense LiDAR solution for V2I operating in Hangzhou, Shanghai, and Shenzhen. The RoboSense LiDAR developed according to the roadside perception needs of the V2I system, gives autonomous vehicles eyes from the sky to accurately sense every traffic participant, ensuring traffic safety and efficiency as well as information services applications.

> ***The RoboSense LiDAR developed according to the roadside perception needs of the V2I system, gives autonomous vehicles eyes from the sky.***

Xiongan New Area in North China's Hebei province is on the cusp of building a smart city with new technologies. Its first "5G and smart bus" V2I pilot project was jointly built by Hebei radio and television information network group (HBTN), China Communications Construction, and DT Mobile. The HBTN is responsible for the deployment of the 5G network environment; China Communications Construction is in charge of the construction of the road infrastructure; DT Mobile manages the transformation of the vehicle end, C-V2X equipment, and end-to-end solutions, while RoboSense provides one-stop roadside LiDAR solution (including sensor hardware and perception algorithm software).

As the main hardware in the project, LiDAR breaks through the limitations of conventional sensors as cameras (easily affected by ambient light) or millimeter-wave radars (with low ranging accuracy). LiDAR can actively emit lasers to detect and collect 3D environment data in real-time with high ranging accuracy, adapting to different light environments and can operate24 hours a day. The RS-LiDAR-M1 is intelligent, low-cost, stable, and reliable, with a simplified structure and small size, which meets the needs of future mass deployment of 5G and V2I construction.

The RoboSense RS-LiDAR-Algorithms offer the V2I project with accurate and reliable perception and rich extended functions. Before RoboSense's establishment in 2014, the founding team of RoboSense, including the founder Dr. Steve Qiu (Chunxin Qiu), has been developing point cloud perception algorithms for more than 7 years. To date, RoboSense has been cultivating in this field for more than 12 years.

The RS-LiDAR-Algorithms maintain high accuracy while ensuring a very high detection rate on road, which greatly improves the LiDAR's perception ability, and adapt it to a variety of road, weather, and traffic conditions, not only in simple road conditions, such as highways, but also roads with complex challenges, such as intersections with Chinese characters during peak commuting hours and in dense traffic. The RS-LiDAR-Algorithms solve a large number of corner cases and ensures that all kinds of traffic participants are accurately detected even in extreme cases.

"We are very pleased that RoboSense and DT Mobile have reached strategic cooperation on V2I solution for 5G-based smart city development," RoboSense COO Mark Qiu said. "In addition to increasing investment by combining both parties' advantages, we will also vigorously carry out the test and verification of the solution to ensure the safety of autonomous driving applications, further advancing the development of the automotive industry with the new technology breakthroughs on the Vehicles-to-Internet."

About RoboSense

Founded in 2014, RoboSense (Suteng Innovation Technology Co., Ltd.) is the leading provider of Smart LiDAR Sensor Systems incorporating LiDAR sensors, AI algorithms and IC chipsets, that transform conventional 3D LiDAR sensors to full data analysis and comprehension systems. The company's mission is to possess outstanding hardware and artificial intelligence capabilities to provide smart solutions that enable robots (including vehicles) to have perception capability more superior to humans. Market-oriented, the company provides customers with various Smart LiDAR perception system solutions, including the MEMS, mechanical LiDAR HWs, fusion HW unit, and the AI-based fusion systems. Garnered the AutoSens Awards, Audi Innovation Lab Champion and twice the CES Innovation Award, RoboSense has laid a solid foundation for market success. To date, RoboSense LiDAR systems have been widely applied to the future mobility, including autonomous driving passenger cars, RoboTaxi, RoboTruck, automated logistics vehicles, autonomous buses and intelligent road by domestic and international autonomous driving technology companies, OEMs, and Tier1 suppliers

www.robosense.ai.

●

NEW REPORT

Banks Ramp up Tech Recruitment in Response to COVID-19

Robert Walters and market analysis experts Vacancy Soft.

New tech roles in banks has increased by a staggering +46% in the last three years – making traditional banks the most prominent recruiter for tech professionals.

To date, a third of overall job vacancies within banks is now tech related – jumping from less than a quarter (23%) just three years ago.

The findings come from a new report from global recruiter Robert Walters and market analysis experts Vacancy Soft - which highlights the impact of COVID-19 on the banking sector – Fintech: Challenger to Competitor.

> **“In turn, banks and financial services firms have woken up to this and have been growing their tech teams at a much faster pace than their fintech challengers.”**

Tom Chambers, Senior Manager – Technology at Robert Walters comments:
“Lockdown and social distancing measures mean that banks have had no choice but to scale back their retail operations, instead pushing customers towards digital platforms.

“With the most at risk to COVID-19 also being the ones who traditionally were the most reliant on counter services, the societal challenge will be to help the elderly use banking services online - where their motivation is that they simply don’t have a choice.

“Assuming they successfully make this switch, retail banking as we know it will be changed – or in some instances disappear - forever.”

A cultural shift
With the UK having one of the highest adoption rates of digital and online banking in the world – growing by 32% in the last 10 years – it seems the digital cultural shift was already taking place.

In fact, adoption rates of online banking in the UK was at an all-time high of 73% in 2019, with the majority of users accessing platforms via smart phones (64%), compared to over tablets or computers (34%).

Robert Walters analysts predict online banking penetration to reach 90% by the end of 2020, driven predominantly by COVID-19, the fast-growing presence of fintechs, and the increased investment from banks into their digital product.

Ben Litvinoff – Business Director at Robert Walters comments:
“Traditional banks have come under criticism for their service offering during the COVID-19 outbreak, with calls from for the financial services industry to work more closely with fintech counterparts to better utilise data and improve customer service.

“In the past five years alone, we’ve seen banks race against the clock to create smartphone friendly apps, which provide the same level of service and accessibility as some of the popular fintech platforms.

“However beyond apps, fintechs have remained one step ahead in their digital offering and during the pandemic have been well-placed to take market share on digital lending, guaranteeing deposits, direct debit payments, and fast-paced decision making powered by AI and data.

“In turn, banks and financial services firms have woken up to this and have been growing their tech teams at a much faster pace than their fintech challengers.”

Banks play catch-up
In the last three years the percentage of tech vacancies in overall job roles advertised for banks has increased by +7% (to make up 30% of overall jobs), and has decreased by -2% in fintechs (to make up 46% of overall jobs).

Tom Chambers, Senior Manager - Technology (London) comments:
“Despite Brexit, the UK remains an attractive hub for fintechs. Growth of the sector can be illustrated by the ongoing increase in vacancies since 2018 - up +16% in 2019, and +53% since 2017.

“However when looking at the slight slowdown in tech roles within fintech, the impact of Brexit and regulation can certainly be seen here. Professional vacancies within legal, change management, and risk grew in fintechs as companies have been forced to prepare for leaving the single market.”

Dan Simmonite, Business Director at Robert Walters, comments:
“Banks have had to alter their business processes in response to the way in which their customers currently are (or will) engage with technology.

"Where banks have been off-shoring or looking at ways to automate or streamline traditional roles, the cost saving from this is going back into a heightened investment into digital infrastructure – where the teams are based in the UK."

This change is most evident when you compare the decline of traditional job roles within banks in the UK – a decline of 42% over the past three years (equivalent to 100,000 jobs) – to the growth of tech roles, currently standing at +46% increase in the last three years.

It also seems the trend of regionalisation within banking shows no signs of abating, with tech vacancies in the regions increasing by +50% since 2017 and +7% in 2019.

In London, tech vacancies within banking has increased by +23% over the past three years, and by +0.45% last year.

Ahsan Iqbal, Director of Technology (Regions) at Robert Walters, comments:

"Where in some cases banks are offshoring or nearshoring traditional roles, the strength of tech talent in the UK has meant that tech departments are here to stay.

"Tech hubs outside of the capital – namely Birmingham, Manchester and Liverpool – have now built strong foundations rivalling what is available if the City or Shoreditch for a lower cost.

"As living costs also continue to be a concern for professionals, the regions will be able to hold onto or attract tech talent that would have otherwise left for London and other European cities."

www.robertwalters.co.uk, www.vacancysoft.com.

●

Research Finds Android Handsets Suffer from Region-specific Security Issues.

Region-specific settings and configurations leave users vulnerable in some countries but not others.

Android dominates the global smart phone market and is used on many of today's most popular phones. But research from security consultants with cyber security provider F-Secure demonstrates that devices from some of the biggest mobile phone vendors in the world suffer from region-specific security issues that affect users in some countries but not others, resulting in a fragmented landscape of security problems.

Devices examined by the researchers include the Huawei Mate 9 Pro, the Samsung Galaxy S9, and the Xiaomi Mi 9. The exploitation process for the vulnerabilities and configuration issues, as well as the impact, varies from device to device. What makes the discoveries significant is the implication that the security of devices sold globally offer different levels of security to users in different countries. Depending on the way vendor's configure devices, this can essentially lower security standards for some people but not others.

According to F-Secure Consulting's UK Director of Research James Loureiro, the presence of these security issues on popular devices expose the significant security challenges caused by the spread of customized Android implementations.

"Devices which share the same brand are assumed to run the same, irrespective of where you are in the world – however, the customization done by third party vendors such as Samsung, Huawei and Xiaomi can leave these devices with significantly poor security dependent on what region a device is setup in or the SIM card inside of it," said Loureiro. "Specifically, we have seen devices that come with over 100 applications added by the vendor, introducing a significant attack surface that changes by region."

For example, the Samsung Galaxy S9 detects the region that the SIM card is operating in, which influences how the device behaves. F-Secure Consulting found that they could exploit an application to take full control of the device when the Samsung device's code detected a Chinese SIM card, but not SIM cards from other countries.

Research conducted on Xiaomi and Huawei mobile phones found similar issues. In both cases, the researchers were able to compromise the devices due to region-specific settings (China for the Huawei Mate 9 Pro, and China, Russia, India, and others for the Xiaomi Mi 9).

F-Secure Consulting discovered the vulnerabilities over the course of several years while conducting research in preparation for Pwn2Own – a bi-annual hacking competition where teams of hackers attempt to compromise various devices through the exploitation of previously undiscovered vulnerabilities (zero-days).

F-Secure Consulting Senior Security Researcher Mark Barnes says these discoveries highlight a new, potentially very insightful, area of vulnerability research.

"Finding problems like these on multiple well-known handsets shows this is an area that the security community needs to look at more carefully," said Barnes. "Our research has given us a glimpse of just how problematic the proliferation of custom-Android builds can be from security perspective. And it's really important to raise awareness of this amongst device vendors, but also large organizations with operations in several different regions."

F-Secure Consulting demonstrated attacks using these vulnerabilities at several different Pwn2Own competitions and shared their research with the Zero Day Initiative (Pwn2Own's organizer) and the participating device vendors. All vulnerabilities used in the attacks have been patched.

F-Secure Consulting operates on four continents from 11 different countries. It provides cyber security services tailored to fit the needs of banking, financial services, aviation, shipping, retail, insurance, and other organizations working in highly targeted sectors.
www.f-secure.com

●

IT News and Business

OpenStack Ussuri Release

The OpenStack community have released Ussuri, the 21st version of the most widely deployed open source cloud infrastructure software. The release delivers advancements in three core areas:

1. Ongoing improvements to the reliability of the core infrastructure layer
2. Enhancements to security and encryption capabilities
3. Extended versatility to deliver support for new and emerging use cases

These improvements were designed and delivered by a global community of upstream developers and operators. OpenStack software now powers more than 75 public cloud data centers and thousands of private clouds at a scale of more than 10 million compute cores. OpenStack is the one infrastructure platform uniquely suited to deployments of diverse architectures—bare metal, virtual machines (VMs), graphics processing units (GPUs) and containers.

For the Ussuri release, OpenStack received over 24,000 code changes by 1,003 developers from 188 different organizations and over 50 countries. OpenStack is supported by a large, global open source community and is one of the top three open source projects in the world in terms of active contributions, along with the Linux kernel and Chromium.

OpenStack pioneered the concept of open infrastructure ten years ago. Since then, it has rapidly become the open infrastructure-as-a-service standard. Recently, new workload demands like AI, ML, edge and IoT have given rise to the project's support for new chip architectures, automation at scale down to the bare metal and integration with myriad open source components. Intelligent open infrastructure—the integration of open source components that are evolving to meet these demands—creates an infrastructure that is self-monitoring, self-replicating, and delivering a versatile set of use cases.

OpenStack has emerged as the preferred open source infrastructure choice for containers, VMs and bare metal in private cloud. The Ussuri release reinforces what OpenStack is well known for—namely, solid virtual machine and bare metal performance at massive scale.
www.openstack.org

Gartner Says Global IT Spending to Decline 8% in 2020 Due to Impact of COVID-19.

Spending on Cloud Services is Bright Spot in 2020 IT Spending Outlook.

Worldwide IT spending is projected to total $3.4 trillion in 2020, a decline of 8% from 2019, according to the latest forecast by Gartner, Inc. The coronavirus pandemic and effects of the global economic recession are causing CIOs to prioritize spending on technology and services that are deemed "mission-critical" over initiatives aimed at growth or transformation.

"CIOs have moved into emergency cost optimization which means that investments will be minimized and prioritized on operations that keep the business running, which will be the top priority for most organizations through 2020," said John-David Lovelock, distinguished research vice president at Gartner. "Recovery will not follow previous patterns as the forces behind this recession will create both supply side and demand side shocks as the public health, social and commercial restrictions begin to lessen."

> ***CIOs have moved into emergency cost optimization which means that investments will be minimized and prioritized on operations that keep the business running.***

All segments will experience a decline in 2020, with devices and data center systems experiencing the largest drops in spending (see Table 1.) However, as the COVID-19 pandemic continues to spur remote working, sub segments such as public cloud services (which falls into multiple categories) will be a bright spot in the forecast, growing 19% in 2020. Cloud-based telephony and messaging and cloud-based conferencing will also see high levels of spending growing 8.9% and 24.3%, respectively.

"In 2020, some longer-term cloud-based transformational projects may be put on hiatus, but the overall cloud spending levels Gartner was projecting for 2023 and 2024 will now be showing up as early as 2022," said Mr. Lovelock.

"IT spending recovery will be slow through 2020, with the hardest hit industries, such as entertainment, air transport and heavy industry, taking over three years to come back to 2019 IT spending levels," said Mr. Lovelock. "Recovery requires a change in mindset for most organizations. There is no bouncing back. There needs to be a reset focused on moving forward."
www.gartner.com

MariaDB SkySQL Adds 'Power Tier' for Enterprises. MariaDB Corporation have announced the immediate availability of MariaDB SkySQL Power, the first database-as-a-service (DBaaS) offering that lets enterprises customize options and configurations to fit their distinct requirements. Built on top of SkySQL's Foundation, which delivers the complete MariaDB Platform experience in the cloud, Power adds important benefits such as the ability to customize instance types to maximize efficiency and resource utilization for a lower total cost of ownership (TCO), and the ability to meet specific enterprise security, high availability or disaster recovery requirements.

"With SkySQL Power, we're listening to our customers instead of telling them how they should work in the cloud," said Michael Howard, CEO of MariaDB Corporation. "Traditional DBaaS solutions don't let enterprises express their uniqueness through their deployments. They offer standard database templates forged from spreadsheets, rather than real usage. We're taking a different approach.

SkySQL Power solves the common enterprise problem that traditional DBaaS offerings can't accommodate – easily incorporating custom database requirements into a deployment. Universally, a DBaaS offers convenience through limited sizing options – similar to buying T-shirts or off-the-rack suits, for example. It alsolets customers choose the preferences that fit their specific enterprise needs, similar to a custom tailored suit with countless combinations of fabrics and styles to choose from. With this product the same level of flexibility and precision inherent in on-prem deployments is now possible in a cloud database for the first time.
www.mariadb.com

Private Networks Will Propel Small Cells to 26 Million by 2026.
Enterprise networks, increasingly deployed by private operators, will provide small cells with the sweet spot they have been seeking for so long, and drive the market to 26 million units by 2026.

The cells deployed will be increasingly diverse in form, ranging from compact versions of macro base stations to almost invisible systems embedded in electronic equipment. But the huge majority – 68% of all small cells that will be deployed between 2019 and 2026 – will be for enterprise and industrial use cases.

These conclusions have been reached by the latest forecast from Rethink Technology's RAN Research service, entitled Private networks and shared spectrum: making the 5G enterprise a reality - Small Cells and Private Networks 2019-2026. A key growth driver will be the rise of private networks to support industrial and engineering use cases, increasingly enabled by emerging shared spectrum in mid-band and millimeter wave bands.

While established MNOs will still command the largest installed base of enterprise small cells by 2026, private operators and neutral hosts will be deploying the largest numbers of new cells from 2023 in enterprise settings, and their impact will be highest in mmWave and shared spectrum, which will be key enablers of alternative deployers.

Retail, government, transport, healthcare, and hospitality will lead the way in early adoption of small cell networks, while accounting for the highest cumulative deployments between 2019 and 2026.

A key growth driver will be the rise of private networks to support industrial and engineering use cases, increasingly enabled by emerging shared spectrum.

The RAN Research forecast obtained opinions on small cell deployments and barriers from 66 traditional MNOs, 28 alternative private, enterprise or neutral host operators, and also 72 enterprises across North America, Europe, China, India, and South East Asia. This revealed some continuing frustration – the survey revealed that fundamental capabilities of indoor coverage and data or voice QoS are extremely important to enterprises, ranked on average at over 7 on a scale of 1 to 10, and yet perception of how well these capabilities had been delivered was only around 5.

Most enterprises and industries confirmed their aspirations to apply cellular connectivity for greater efficiency, but too few can yet access networks that are sufficiently reliable, let alone optimized for emerging capabilities promised under 5G, such as low latency. Fewer than half of enterprises reported that mobile quality of service was adequate, and only about 20% would yet trust cellular networks for critical communications.

Yet the report offers hope that four trends, if well supported by regulators, operators, and the broader ecosystem, will enable the required quality and reliability under 4G and later 5G. These trends will support an essential diversity of provider, technology and application. These enablers are:

- greater service diversity and specialization
- shared spectrum to lower barriers to entry
- self-contained RAN and core technologies with open architectures, again to lower costs and barriers to new providers
- and co-investment across the ecosystem with costs and rewards split between enterprises, operators, and other partners.

These, together with more creative regulatory policies regarding industrial spectrum, will help to achieve the reduced TCO and wider monetization opportunities, which are essential to drive operators of all kinds to invest heavily in the indoor use cases.
www.rethinkresearch.biz

Cloudreach Develops Data Visualization Projection Platform on Google Cloud.

Cloudreach has launched a data visualization projection platform developed on Google Cloud that is helping each US state plan, prepare and react to the ongoing challenges raised by COVID-19.

The platform delivers unique and tailored data to each state and its governors. It enables state decision-makers to respond to local requirements on a case-by-case basis and model the impact of potential actions to best protect their constituents. This is achieved through connecting national and local data feeds to the platform and visualizing chosen economic indicators.

It enables state decision-makers to respond to local requirements on a case-by-case basis and model the impact of potential actions to best protect their constituents.

Chris Williams, General Manager, Google Cloud Platform at Cloudreach, said: "US federal and state policy leaders are working against this rapidly spreading novel enemy in unprecedented times. They need a level of insight and understanding into how the pandemic is affecting our daily lives, which is difficult for any human to comprehend because the growth is exponential rather than linear.

"Our platform gives emergency state management and politicians a line of sight to plan ahead, by applying and overlaying projection models so they can plot all potential outcomes, how they overlap, and where decisions need to be made."

Live data

The platform is designed to help public sector leaders make proactive decisions based on live bespoke data relevant to their state, assisting in the implementation of three key areas:

- Reopening the economy: clarity on when to reopen a state's economy.
- Planning for possible 'second wave': heading into the fall and winter, the platform gives states specific and bespoke data that flags the early signs of reemergence.
- Natural disasters outside of COVID-19: providing the appropriate resource to meet the demands of COVID-19 has left fewer resources available to deal with other natural disasters and other emergencies.

Partnering with Google

Developing the tool on Google Cloud enables it to be deployed quickly at scale. Third-party data can be digested and resurfaced as tailor-made visualisations.

"Data is an important resource for governments and organizations responding to COVID-19," said Todd Schroeder, Director, Public Sector Digital Strategy at Google Cloud. "We're proud that Cloudreach will launch this new toolset on Google Cloud, enabling responders and policymakers to leverage data analytics and visualization capabilities and to make data-driven decisions in a complex environment."
www.cloudreach.com

How Green is your Data Center?

DigiPlex have recently published "Will your IT withstand a sustainability review?", a guide to help businesses assess and manage the sustainability profile of the data centers their data resides in.

To date, the environmental damage caused by IT has been largely overlooked, but this is changing. The DigiPlex guide highlights:

- It has been estimated that data centers and digital infrastructure could be responsible for up to 20% of the world's electricity consumption and 5.5% of CO2 emissions within a decade
- One in four Scandinavian consumers would consider using the internet less to reduce environmental damage
- Nearly three-quarters of Scandinavians believe digital service providers should report on their energy consumption and its impact on climate
- The EU Commission note in their digital strategy that data centers are responsible for a significant environmental footprint, and "can and should become climate neutral by 2030."

Data, and the digital infrastructure that supports data collection, use and storage, is essential to almost every business. But few organisations have the frameworks and processes to accurately report on the environmental impact of the data centers their data resides in. As they use a wider range of cloud, co-located and on-premise IT facilities, many struggle to even identify where data and computing resources are located.

Wiljar Nesse, CEO of DigiPlex, commented; "New digital technologies have undoubtedly made the world a better place. But at the same time digitalisation has increased energy consumption. Every internet search, every streamed song and every electronic transaction consumes energy. Each individual action is tiny, but the enormous growth in digital activity now consumes massive amounts of energy.

"Our guide not only demonstrates that politicians, environmental groups and consumers are waking up to this, but provides clear, proactive steps that can and must be taken to mitigate the increasing environmental impact of digital on our planet."

"The data economy has escaped environmental scrutiny for too long – now is the time to take responsibility for the impact of your IT on the climate, before customers, governments and regulators force you to."
www.digiplex.com

Alibaba Records Only 9% Lower Profit than Amazon but Trails by 4x in Revenue.

Data gathered by Learnbonds.com shows that Chinese internet company Alibaba registered 9.3% lower profits compared to United States' Amazon. The data further shows that there is a significant gap in revenues between the two companies by at least four times for the financial year ending March 31, 2020.

Alibaba's revenue steadily grows in three years
For the period under review, Alibaba's operating profit was $12.9 billion, while Amazon had $14.1 billion. In general, Amazon's total revenue was $296.3 billion compared to Alibaba's $72 billion. The revenues for the two companies come from different diversified products like online and offline retail as well as seller and logistics services.

The Learnbonds.com research notes that:
“Chinese e-commerce giant Alibaba registered a slightly lower margin in operating profits compared to Amazon, but there exists a huge difference in total revenue between the two platforms.”

Chinese e-commerce giant Alibaba registered a slightly lower margin in operating profits compared to Amazon, but there is a huge difference in total revenue.

Under the core commerce revenue Amazon registered $223 billion while Alibaba had $61.6 billion. For the cloud revenue, Amazon had profits of $37.5 billion, a difference of 147.2% compared to Ali baba's $5.7 billion. Under other revenues, Amazon recorded $35.7 billion while Alibaba had $4.7 billion.

The Learnbonds.com research also overviewed the revenue for the twp companies over the last three financial years. In general Amazon remains dominant but both companies keep growing in revenues.

Alibaba's current revenue of $72 billion is a growth of 36.62% from 2019's $52.7 billion. For Amazon, this year's revenue grew slightly by 5.6% from last year's $280.5 billion. In 2018, Amazon's revenue stood at $232.8 billion while Alibaba had $35 billion. Between 2017 and 2020's financial year Amazon's revenue has grown by 66.64% compared to Ali baba's 225.79%.

Both Amazon and Alibaba have a similar business model but the American company has an established footing globally. In recent years, Alibaba has been making attempts to overhaul its business model to march Amazon.
www.learnbonds.com

Supermicro Unveils Intelligent Retail Edge.
Super Micro Computer, Inc. have announced an advanced and customizable integrated platform targeting retail and chain store environments. Supermicro's new platform combines proven hardware/software configurations to support the demand for processing the quantities of data emanating from the growing deployment of IoT and other interrelated computing devices.

Supermicro's Intelligent Retail Edge provides an integrated software-defined operating platform that significantly simplifies the deployment, management, orchestration, and networking of Edge infrastructure and applications. The platform runs on Supermicro's IoT and edge hardware, ranging from small edge devices to full-scale rack-based edge servers that can support GPU, FPGA, and other technologies.

“Supermicro's Intelligent Retail Edge solution provides retailers the engine they need to deliver innovative technologies and services to their customers efficiently,” said Raju Penumatcha, senior vice president and chief product officer, Supermicro. “Built on Supermicro's flexible Building Block Solutions architecture and powered by leading-edge software from our partners, this solution is optimized to help address some of the challenges facing the retail industry today.”

Supermicro's Intelligent Retail Edge is offered in three different certified cluster configurations leveraging the industry-proven SuperServer platform that is optimized for specific sized stores, and application workload requirements.

• Entry-level cluster platform based on the E100, a small, powerful fanless IoT/Edge gateway server for small stores with space and power constraints, such as small convenience stores or restaurants, running basic workloads such as Point-of-Sale (POS), video surveillance, and inventory management.
• A mainstream cluster requiring a versatile, high-performance IoT/Edge server based on the E300, has a small physical footprint and superior acoustics for small to medium-sized stores running multiple applications at the edge.
• High-end cluster configuration utilizing the 1019/5019, a short depth rack-mount edge workhorse server with rich storage and networking options and support for accelerator and GPU technologies needed for AI/ML applications for medium to- large-sized stores, such as grocery stores and mid-sized size retailers.

Developed through a collaboration with NodeWeaver and NetFoundry, Supermicro's Integrated Retail Edge platform supports small-to-large clusters for retail applications. “Retail technology is at the beginning of a new era that promises to revolutionize the customer experience, increase efficiencies, and reduce costs,” said Carlo Daffara, CEO and Co-Founder of NodeWeaver, a provider of a universal edge fabric software. “As distributed compute becomes more critical for retail operations, these platforms must be deployed, managed, maintained, and secured on a mass scale. Supermicro's Retail Edge provides the foundational operating platform for this distributed compute layer, and NodeWeaver is proud to be a part of this solution.”
www.supermicro.com, www.netfoundry.io/

Security News and Business

Erasure and Destruction of Electronic Data Grows.
DSA Connect, a UK based IT company that specialises in the permanent deletion and destruction of electronic data, saw enquiries during March increase by 35% when compared to February, and by 52% more than in January. Overall enquiries in Q1 were 55% higher than the same period last year, and revenue was up 46%.

Harry Benham, Chairman of DSA Connect said: “Fraudsters are opportunistic, and many have jumped on the Coronavirus crisis to target employers and their staff. Hundreds of thousands of new websites with suspicious Coronavirus related words have been created, many of which are trying to generate sales from fake supplements.

“Sadly, people are desperate to find out information on Coronavirus and this increases the chances of them forgetting the basics of cybersecurity and visiting unsafe websites where they could become the victim of a scam which could lead to a data breach. As a result of this, we have seen a significant increase in employers contacting us asking if we can remove data remotely from their systems, reducing the chances of data breaches should their employees, who are working from home, become the victim of a phishing or malware attack.”

> ***Sadly, people are desperate to find out information on Coronavirus and this increases the chances of them forgetting the basics of cybersecurity.***

DSA Connect is an IT asset disposal specialist. It specialises in the erasure and destruction of electronic data using tools certified by CESG and approved by the UK National Cyber Security Centre (NCSC). It ensures that all data storage media and equipment is removed from a client’s premises and transported to its secure facility in unmarked, tracked vehicles.
www.dsa-connect.co.uk

RDP Attacks Surged by 330% in the US.
According to data extracted and analyzed by Atlas VPN, remote desktop protocol (RDP) attacks rocketed by 330% amid the COVID-19 pandemic.

The start of the RDP attack increase correlates almost entirely with the start of lockdowns. From March 10, 2020, RDP brute-force attacks spiked in practically all selected countries.

In the US, from March 10, 2020, until April 15, 2020, hackers carried out 32,299,662 remote desktop brute-force attacks. On average, throughout this period, there were 872,964 attacks daily.

Comparing the period of February 9 - March 9, 2020, to March 10 - April 10, 2020, the attacks in the US jumped by 330%

Rachel Welsh, COO of Atlas VPN, shares her thoughts on why RDP attacks sky-rocketed during the pandemic:

“Due to lockdowns, many office-workers gained remote access to corporate windows workstations or servers. Subsequently, cybercriminals took advantage of sometimes inadequately protected networks and permission given in a hurry.

Over 148 million RDP attacks during the pandemic

From March 10, 2020, until April 15, 2020, hackers attacked users in the US, Spain, Italy, Germany, France, Russia, and China a total of over 148 million times combined.

During this period, hackers carried out 32,299,662 remote desktop brute-force attacks on individuals and organizations in the US. Meaning, the US is the most attacked country on the list. On average, there were 872,964 attacks daily in the US.

In Spain, throughout March 10-April 15, 2020, hackers attacked workstations and corporate servers 25,510,199 times. On average, hackers attacked users in Spain 689,465 times per day.
www.atlasvpn.com

F-secure UK Completes Study on Intelligent Transport System Security.
Cyber security provider F-Secure has completed a study that maps out current and future security challenges facing connected autonomous vehicles (CAV) and intelligent transport systems (ITS) in the UK. F-Secure Consulting conducted the research as part of the Cyber Feasibility projects funded by the Centre for Connected Autonomous Vehicles and delivered by Zenzic and Innovate UK.

F-Secure Consulting’s study, which is available for download along with Zenzic’s Cyber Feasibility Report and the other 6 project studies, takes a holistic view in its examination of the various security challenges involved in the design and maintenance of the UK’s ITS networks. These networks represent a vast ecosystem of technologies and organizations that will collect and process large amounts of data to ensure the systems function safely and properly.

F-Secure Consulting's research highlights the tremendous amount of data collected by CAV and ITS systems, as well as the value of the systems themselves, making them attractive targets for a variety of attackers.

According to James Loureiro, F-Secure Consulting's UK Director of Research, this gives CAV/ITS testing sites (testbeds) set up across the UK an important role in helping secure new technologies as they're developed for use in CAV/ITS systems – something he says is a significant opportunity for the country.

"The role of the UK's testbeds in making sure emerging CAV/ITS technologies work together as part of a safe, secure, reliable system cannot be overstated. These sites give security and tech development an opportunity to intersect and inform one another. And with the right governance, support, and expertise, these projects can produce insights that establish the UK as an innovator in securing the technologies and infrastructure that will shape nations across the globe for years to come," said Loureiro.
www.f-secure.com

The role of the UK's testbeds in making sure emerging CAV/ITS technologies work together as part of a safe, secure, reliable system cannot be overstated.

Number of breached records surged by 273% in Q1.
According to Atlas VPN investigation, the number of breached records globally surged by 273%, when comparing 2019 Q1 to 2020 Q1. During the first three months of 2020, over 8.4 billion documents got leaked.

The number of hacked or accidentally exposed files reached a record-high in the first quarter of 2020. The second year in terms of data leaked in Q1 is 2017, which had over 3.4 billion records exposed.

From 2013 to 2019, the combined number of breached records in the first quarters is 8,058 million. Meaning, combining the first quarter breaches from 2013 to 2019 still does not equal the amount of data exposed in 2020 Q1.

Rachel Welsh, COO of Atlas VPN, comments on the dangers of data breaches:

"Gaining access to a users' email address or other accounts is usually just the start of an advanced scam scheme. Fraudsters then send out phishing emails to the users' contact list.

Since the email comes from a trusted source, contacts usually have their guard down and are tricked into giving up their sensitive information including credit card details."

Breaches by region.
Researchers found that in Q1 of 2020 globally, there was a total of 1196 individual data leaks. Out of these, almost 40% happened in the US.

It has to be noted that companies in the US have strong disclosure requirements, which means that a big part of the leaks is being reported. This is not the case in many other countries.

In contrast, as many as 42.06% of data leaks do not have an identifiable source. Meaning, an individual or organization discovered an unsecured cloud or similar servers containing users' information, and nobody knows where it came from.
www.atlasvpn.com

1 in 3 Fall Victim to Phishing Attacks: Lockdown Amplifies Password Security Flaws.
Since lockdown started, a report has revealed a shocking third of respondents have fallen victim to phishing emails, which hackers use to steal passwords – 45 per cent of which were related to coronavirus. The report found that a third of respondents use identical passwords, with employees often sharing passwords with colleagues, as well as between personal and business accounts.

Gartner forecasts that by 2022, 60 per cent of businesses will have cut their reliance on passwords by half. James Stickland, CEO of Veridium, believes the global crisis is acting as a catalyst, forcing firms to innovate stronger authentication technology, such as biometrics, to protect their most valuable assets.

James Stickland comments: "Capterra's findings demonstrate the extent to which businesses and employees worldwide are battling with password security, which is directly linked to the high number of phishing attack victims and rising fraud. Covid-19 is now posing the biggest-ever cybersecurity threat, causing phishing attacks to rise over 600 per cent in since February[2], as malicious actors trick users via fake coronavirus alerts. This is forcing businesses to rethink and overhaul their security strategies in an increasingly vulnerable landscape."

James continues: "Passwords are now widely being recognised as an outdated, easily compromised method of authentication, accounting for over 80 per cent of data breaches. Millions use the same password for multiple logins, leaving valuable personal data at risk. This isn't surprising – employees must remember approximately 27 passwords, putting them under considerable strain. Veridium estimates that enterprises with 10,000 employees spend on average $100 per user each year to manage password resets, amounting to a staggering $1.9 million[5], as well as significantly decreasing productivity across all departments."

He concluded: "Now that millions of employees are working from home, companies are waking up to the weakness of passwords. As a result, more and more organisations are turning towards passwordless, multi factor biometric authentication to mitigate against increasingly sophisticated cyber threats, whilst enhancing the user experience."
www.veridiumid.com

Bluetooth Vulnerability Discovered.

Academic researchers have uncovered security vulnerabilities in Bluetooth Classic that allows attackers to spoof paired devices and insert a rogue device into an established Bluetooth pairing, masquerading as a trusted endpoint. This allows an attacker to capture sensitive data from the other device.

The bugs allow Bluetooth Impersonation Attacks (BIAS) on everything from internet of things (IoT) gadgets to phones to laptops and the issue lies in the pairing/bonding protocols used in the specification.

Deral Heiland, IoT research lead, Rapid7 comments on this vulnerability:
"The pairing process, which is used to establish a long-term key, has been the hallmark for establishing a secure communication channel for the exchange of information for Bluetooth (BR/EDR). Historically this initial pairing process has always been believed to be the weakest link, but once the long-term key exchange has been completed it has been believed that communication moving forward was secure.

"Unfortunately, this research paper sheds new light on several issues allowing potential malicious actors to perform impersonation attacks against communication between Bluetooth (BR/EDR) devices. With these issues ranging from the lack of a mandatory mutual authentication, role switching issues, and being vulnerable to authentication procedure downgrade attacks.

"So what is the risk? First, long-range attacks from across the world are not possible, since Bluetooth (BR/EDR) is a low-power wireless communication most malicious actors would need to be in close proximity, such as 10 to 100 metres, to perform these attacks. Further ranges are possible but would still require the malicious actor to be within line of site and have a directional antenna capable of longer ranges.

"Also, currently there is no exploit code available in the wild yet and hopefully it remains that way. With that said, the Bluetooth Special Interest Group (SIG) has posted an advisory stating that changes to the standard will eventually be made but until that is in place the Bluetooth SIG strongly recommend vendors take action to prevent these vulnerabilities from being leveraged."
www.rapid7.com

GDPR Failings with Home Working Brits as Law Celebrates Its Second Anniversary.

The General Data Protection Regulation (GDPR), the toughest privacy and security law in the world, celebrates its second anniversary recently. Launched on 25th May 2018, GDPR was introduced to protect the data of anyone living, or doing business with, those in the European Union and European Economic Area.

GDPR, over the last two years, has presented a real challenge for SMEs who have had to alter their practices with regards to the storing of personal data, how it is shared and how well it is protected. Although an initial challenge, businesses adjusted and there has not been many fines imposed on businesses, or at least not as many as was expected.

However, recent research conducted by IT support company ILUX, has revealed some eye-opening revelations that business owners should consider around GDPR now that their workers are being forced to work from home. The independent research was conducted with 2,000 home working Brits and revealed that one in ten believed that their expected working practices imposed by their employer are not GDPR compliant. With over 20million people working from home, that equates to 2million potential fines for businesses should a breach occur.

13% of the workforce surveyed admitted that they are using their own home technology for work. Accessing data on a potentially unsecured computer system, via a home network and even printing documents at home, could all lead to a data breach. This could be the catalyst for employees concerns over GDPR compliance and a sign, after over two months of lockdown, that business owners should be checking in with their employees on important issues like compliance.

James Tilbury, Managing Director at ILUX, comments:
"Whilst, as business owners, we may be busy, stressed and frankly trying to keep our heads above water, it is not a time to be complacent. Asking employees to work from home and then not providing the right computer systems and security measures is a recipe for disaster. The last thing any business needs, especially at the time of an impending recession, is to lose valuable data, be the target of a cyber-attack or phishing and be hit with a hefty fine for breaching GDPR guidelines.".

GDPR was brought in to strengthen data protection for individuals across the EU, all UK companies that process personal data must comply or risk significant financial penalties. For a business, not complying could have significant implications on business relationships let alone the potential loss of four percent of their turnover as a fine for the breach.

Tilbury continues: "Employees should only use business devices, not home computers, phones and/or tablets to transfer data. All devices should have the latest patches applied, to ensure security vulnerabilities or other bugs are fixed, as well as anti-virus, anti-spam and web protection. Home computers will, most likely, not have these applied. Nine in ten is a positive figure, better than would be expected, but as a business owner I would be starting to ask myself "Did I plan enough for home working" and get some advice from an industry professional on how you might rectify any GDPR issues in my business, now. Better to be proactive than reactive in these situations."
www.supportforit.co.uk

●

IMPORTANT INFORMATION

2020 Subscriptions are still being taken .

No price increase.

Contact us directly or your agent to ensure unbroken issues.

• SECURITY • VIRUSES
• INTERNET FOCUS • NETWORK NEWS AND PRODUCTS
• NETWORK STANDARDS • IT NEWS
• WEB SERVICES • CLOUD COMPUTING
• BOOKS • SHOW COVERAGE

BACK ISSUES AVAILABLE FOR 2020

SPECIAL RATES FOR NEW CUSTOMERS RECEIVING BOTH ISSUES.

THE SOFTWARE WORLD SERIES
Database and Network Journal
An International Journal Of Database & Network Practice
Software World
Database & Network Journal
AUGUST
VOLUME 48
PUBLISH
THE SOFTWARE WORLD SERIES
Software World
An International Journal Of
ms & Packages
Software World
Database & Network Journal
JANUARY
VOLUME 50
NUMBER 3 2019
PUBLISHED SIX TIMES PER YEAR

**Free Offer:
E-mail us now to receive a free online copy of Database and Network Journal**

2020 RATES:

SOFTWARE WORLD
ISSN 0038-0652

UK £135....Less Agency Discount £122
Overseas..£161.... Less Agency Discount £145

DATABASE & NETWORK JOURNAL
ISSN 0265-4490

UK £135....Less Agency Discount £122
Overseas..£161.... Less Agency Discount £145

*Payment in £ sterling please. Made payable to A.P. Publications Ltd.
We do not accept $ cheques. Bank transfer available by request. (Terms and conditions apply)*

A.P. Publications Ltd. 58 Ryecroft Way, Luton. Beds. LU2 7TU, U.K.
Tel: 01582 722219
www.softwareworldpublication.com
E-mail: smpluton@ntlworld.com

Software World and Database & Network Journal were first published over 50 years ago with the intention of providing interpretative analysis of computer software as it emerged in the future.

Subscribed to by IT Information Centres and University Libraries world- wide they provide a bimonthly compilation of new developments and products of commercially available mission critical software and database applications.

Software World and Database & Network Journal both offer a yearly index of features and products, a valuable reference source.

To renew now contact your agent or A.P.Publications direct.

Steven Patterson
Editor