RACONTEUR

Revolutionising cybersecurity

Forcepoint

Forcepoint

Forcepoint is the global cybersecurity leader for user and data protection. Forcepoint's behavior-based solutions adapt to risk in real-time and are delivered through a converged security platform that protects network users and cloud access, prevents confidential data from leaving the corporate network, and eliminates breaches caused by insiders. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of enterprise and government customers and their employees in more than 150 countries.

RACONTEUR

Publication sponsored by
Forcepoint

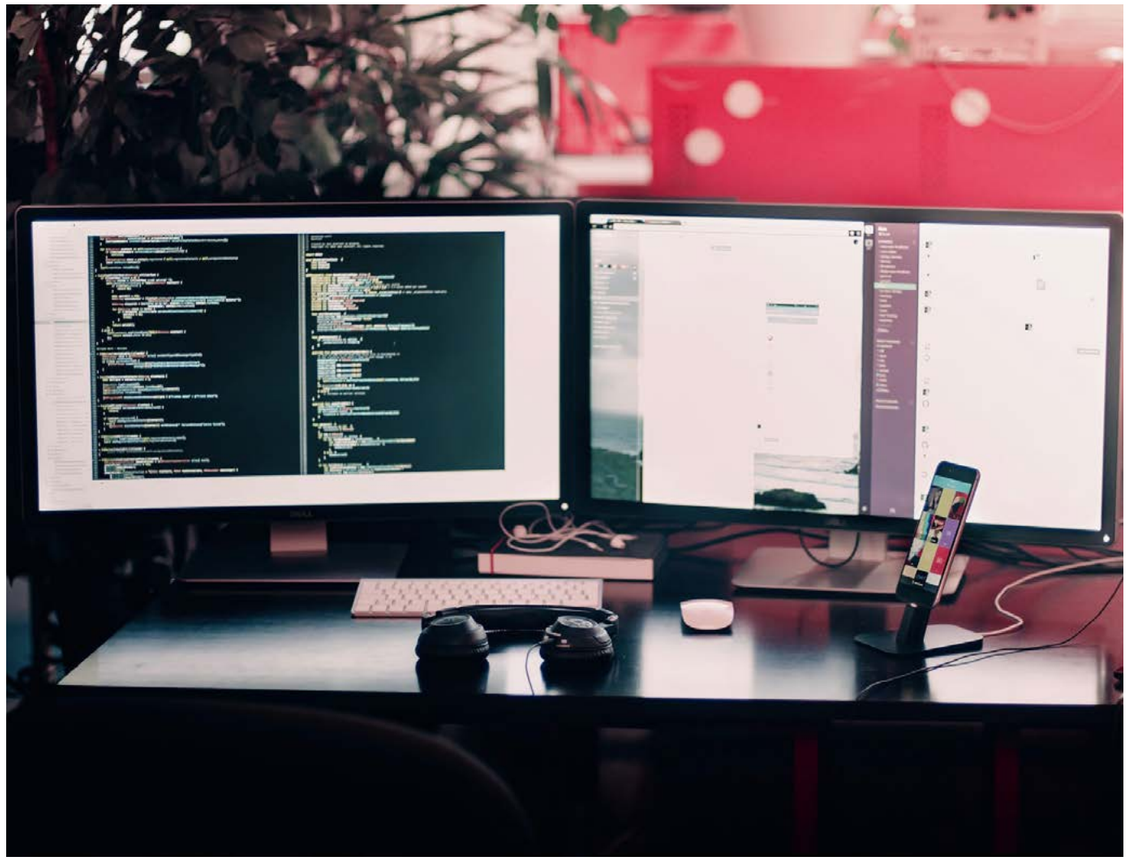
Project manager Georgie Cauthery
Editor Peter Archer
Design Kellie Jerrard, Sara Gelfgren
Production manager Hannah Smallman
Digital marketing manager Kyri Rousou

Contributors
Christine Horton
Nick Ismail
Tamlin Magee

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net

Contents

This report offers practical steps for businesses looking to overhaul their cybersecurity and embed a zero trust approach



TECHNOLOGY

The technology deployment revolution

SASE, or secure access service edge, located in the cloud, offers a holistic solution to provide a secure environment in an era of zero trust

Tamlin Magee

Cybersecurity management at a distance can be a headache, even before the pandemic hit and remote working became the norm for many. That businesses had already moved enthusiastically towards cloud-based ways of working made old forms of network defence, the so-called castle-and-moat approach, less viable. A certain level of control had to be ceded.

Over the years, approaches such as CASB, or cloud access security brokers, firewall-as-a-service and identity and access management went some way towards assisting companies to build better defences. But without a joined-up, holistic deployment strategy, organisations still lacked the visibility necessary to manage security in the digital-first cloud world.

These technologies, and more, are now being bundled together under the umbrella of SASE, secure access service edge, pronounced "sassy", with a service wrap that's easy to sell and pay for, says TechMarketView principal analyst Martin Courtney. Because the framework is cloud native, SASE-led programmes lend themselves well to zero-trust networks, which guarantee no single person is given inappropriate credentials by default.

The idea is to enable secure access on a case-by-case basis, giving users permissions they need to accomplish a specific task, rather than letting them into the entire network. SASE promises to bring reduced cost, less complexity and fewer integration challenges across an organisation, with better visibility.

While SASE isn't the only approach to zero trust, it can deliver a neatly packaged solution, says Courtney, one that delivers the tools needed to verify end-users and devices according to location, device, IP address and network.

Modern solution overcomes legacy

SASE is a modern solution to overcome legacy problems, adds Kevin Curran, professor of cybersecurity at Ulster University. Traditional security is no longer fit for purpose and zero-trust models are simply more relevant in the digital era, he says.

"SASE is a perfect fit to usher in zero trust," says Curran. "Organisations have been fire-fighting for some time, adding connections, systems and people to their networks to provide fast solutions for connectivity."

This led to an ever-increasing hotchpotch, with organisations struggling to provide a snapshot view of what's occurring at any time. "SASE, with its foundation in the cloud, offers a holistic solution to provide a secure environment for these difficult times," says Curran.

However, the extent to which SASE components are successfully combined into a single, manageable interface varies significantly, according to Courtney, as some suppliers are "shoehorning whatever product or solution they can into the mix".

As with most things, it's actually the ongoing integration into an organisation's practices that deliver the real value. Businesses should avoid viewing SASE as an off-the-shelf solution and instead align their operations to it continuously.

"SASE should be introduced slowly in steps, entailing pilot projects and tweaks in a lab environment before deploying

Risk assessment comes first

Every touchpoint needs to be mapped for a SASE strategy to be successful, adds Curran, and that means first conducting an in-depth risk assessment that examines all data storage access, employee authentication and the role third parties play within a network.

"SASE is not as simple as changing one email client for another," he says. "It should be introduced slowly in steps, entailing pilot projects and tweaks in a lab environment before deploying, and it is crucial to ensure SASE is seamless for employees."

Ensuring seamlessness is a cultural question as much as a technical one. Security leaders should begin by instituting strong organisation-wide governance processes, but concurrently combat initial misgivings from staff with user training. Motivations for such sweeping programmes should clearly be explained to all staff.

Perhaps most important is leadership buy-in. Luckily, there are clear lines of attack to communicate value. The benefits of zero trust are somewhat self-evident as a mitigation strategy, but also security and network convergence is strategically important. It enables firms to grow their networks more safely as their businesses grow.

With such buy-in, it should be emphasised that SASE is not a one-off, box-ticking exercise. IT and security leaders should instead view SASE as part of a journey, charting a path strategically in line with the wider business.

54%

of organisations are prioritising initiatives to improve visiblity and security for home workers and cloud infrastructure

Accelerate Technologies 2020

EDUCATION

How to make SASE a board-level priority

IT and security leaders must educate the board on the necessity of a security and data protection framework in the cloud, says Nicolas Fischbach, global chief technology officer at Forcepoint

Nicolas Fischbach, global chief technology officer, Forcepoint

Despite the increase in cyberattacks levelled against organisations and the financial impact of more stringent data protection regulations, boards are still having difficulty prioritising cybersecurity.

However, as organisations continue to evolve as part of their digital transformation, or Industry 4.0 journeys, investment in and the understanding of cloud security solutions must become the utmost priority for senior business executives.

In 2019, Gartner highlighted SASE (secure access service edge) as a more appropriate security framework for modern enterprises. A convergence of existing security and data protection solutions, SASE brings them all together in the cloud. Having this single pane of glass allows security and risk leaders to enable and manage the versatile access requirements to data and apps with more consistent policy controls.

The coronavirus pandemic has accelerated the need for organisations to adopt this security and data protection framework, as employees around the world are forced to work remotely.

To understand the importance of adopting SASE and cloud security, IT, risk, data protection and security leaders must be able to educate boards and effectively communicate its value in protecting a business's two most valuable assets: its people and data.

> **It is important the board understands that SASE will allow organisations to remain productive and innovate, while ensuring compliance and security no matter where their employees or devices are located**

The challenge of communicating security to the board

There are two main challenges in getting security on the board's radar.

The first is that many boards are not effectively briefed on security and as a result it's hardly ever on their agenda, in particular if it's not compliance or risk-register driven.

The second challenge in educating the board comes from changing the perception of security and information protection. Currently, it is viewed more like an insurance policy to protect the business from risks, rather than something that drives business outcomes.

Security, in fact, is an enabler of digital transformation in the cloud and will help drive value to the business. This was perhaps best demonstrated during the early stages of the global COVID-19 lockdown, which saw the mass move to remote working. In this environment, organisations had to enable employees to work from home in a secure manner, to protect company assets and data, while allowing them to maintain productivity and drive innovation.

IT and security leaders now have a golden opportunity to present a re-engineered version of security to their boards that is fundamental to a successful future in the cloud and they should be vocal about it.

Instead of security being viewed as an innovation brake or a contextless must do, the aim should be to highlight SASE as a catalyst to achieve competitive advantage and align it to business goals. This is something the board will relate to.

It should also be communicated that while SASE has the potential to help drive operational excellence, it needs a trusted, reputable and proven platform and solution provider to make this a reality.

At the moment, is there one provider that can deliver a seamless networking and security experience, including the transition from today's to the future state? Will IT professionals be comfortable giving up the real or perceived benefits and freedom of multi-sourcing for one provider's solution? These are questions that need to be posed and answered when making a decision to adopt SASE.

SASE is a journey

Before even explaining the benefits of SASE, IT and security leaders need to start from the bottom up and explain the current security maturity level of the organisation to the board. Once this has been established in line with digital transformation objectives, then conversations can begin around the journey to SASE. It's a journey that will have steps, often going from on-premises to hybrid to cloud first or cloud native.

Organisations will already have existing security deployments and an existing way of operating when it comes to network and cloud security as well as data protection. As such, as organisations phase out legacy solutions and adopt a more dynamic approach to working in virtual environments, it's fundamental that the board understands SASE, just like digital transformation, is a journey that will continuously evolve. It should be viewed as the North Star.

It's also critical to make clear to the board that SASE will touch multiple departments. To drive this agenda, there needs to be, at the very least, a strong business alignment between the chief information security officer (CISO), chief information officer and data protection officer.

The business value of SASE

If SASE is embedded into business workflows, rather than just being treated as an add-on, then it will improve employee experience, enabling them to work productively and securely, without being disrupted by outdated security measures.

As an example, this convergence will help with policy fragmentation which means users will have inconsistent rules applied depending on the application or data they try to access. Also, the end-user experience is often directly tied to these disjointed security solutions, which results in friction rather than acting as a safety net for the user.

In addition, SASE helps reduce the complexity of the CISO's toolbox. Currently, there are too many diverse security tools that are not integrated. Bringing everything together under one framework will reduce the operational footprint and improve the mean time to detect and to respond.

From a business point of view, it is important the board understands SASE will allow organisations to remain productive and innovate, while ensuring compliance and security no matter where their employees or devices are located, which is critical not only in the current era of remote working, but for the flexible working models that have now become the norm.

SASE will help businesses reduce risk, gain visibility across the entire network and create a more automated response to threats that could severely damage the business, both financially and reputationally.

Ultimately, IT and security leaders need to educate the board on the necessity of a security and data protection framework in the cloud. Hybrid IT is now a reality for businesses, with the majority having at least some of their infrastructure deployed off-premises.

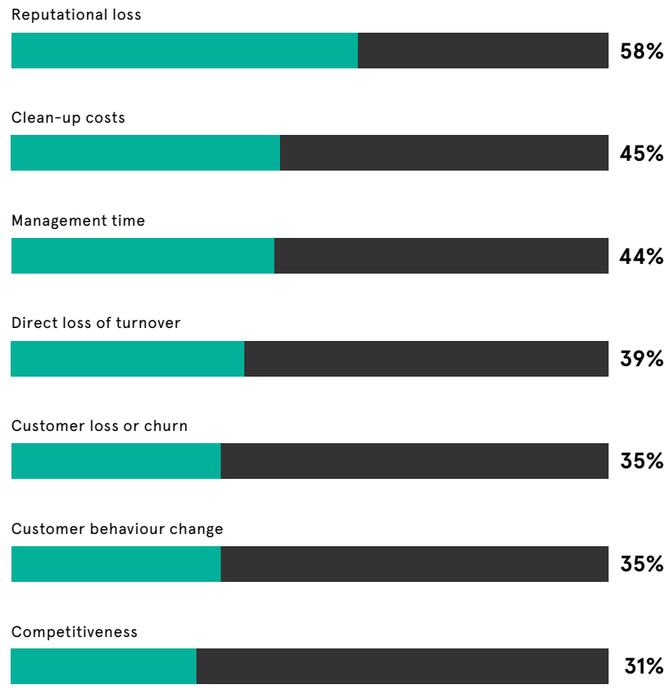
SASE will help organisations gain visibility and provide secure access across endpoints, networks, applications and data. This will help realise hybrid IT's most significant benefit: getting the most out of the cloud as its adoption rate soars.

85%

of organisations have a board member with specific responsibility for cyber security

Grant Thornton 2019

IMPACT OF A CYBER-ATTACK



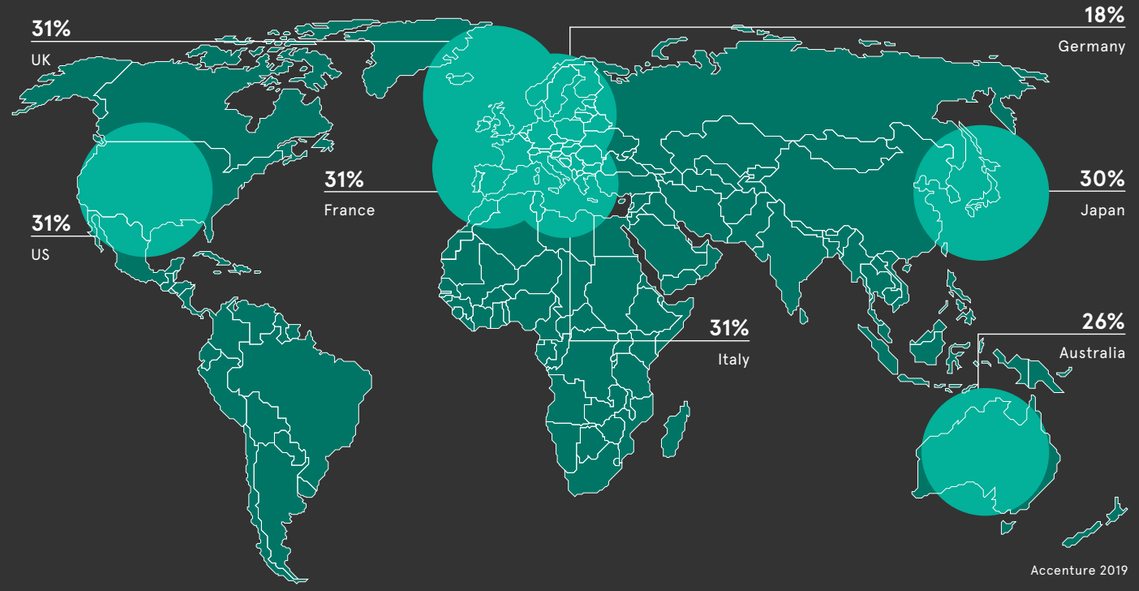
Ponemon Institute and Forcepoint 2020

TRUST NO ONE

The cost of cyber crime continues to rise, with employees often the biggest risk. Many organisations struggle to detect insider threats, but a zero-trust approach can offer the solution

THE CURRENT TECHNOLOGIES AVAILABLE ARE NOT ENABLING A REDUCTION IN CYBER CRIME

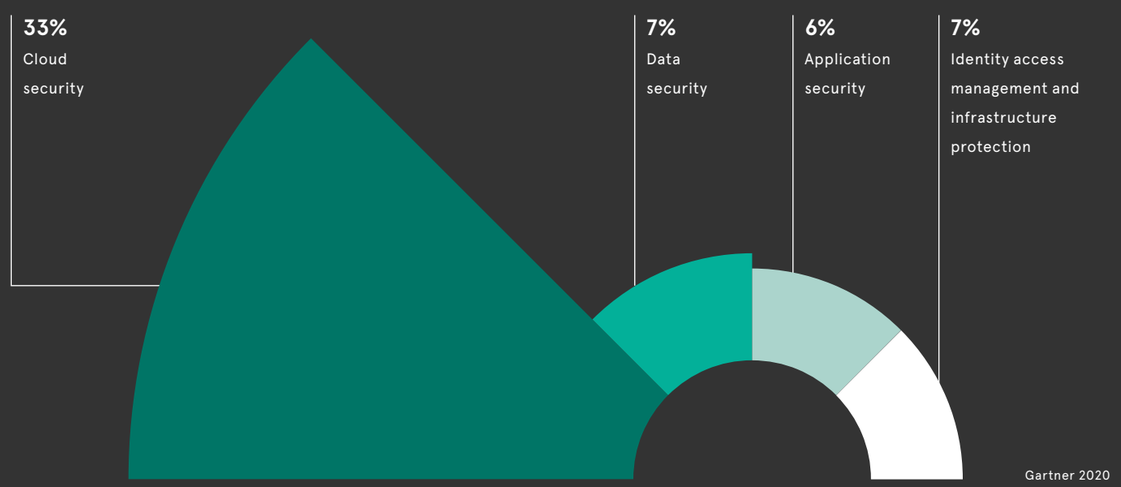
Year-on-year rise in cost of cyber crime, by country



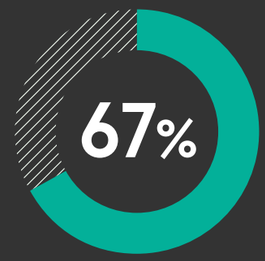
Accenture 2019

WITH CLOUD-BASED SECURITY GROWING RAPIDLY, CLOUD COULD OFFER THE ANSWER

Year-on-year rise in cost of cyber crime, by country Growth of security markets in 2020

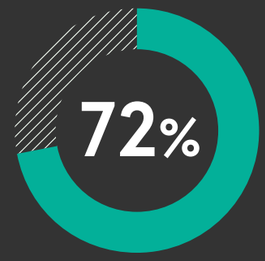


Gartner 2020



increase in cybersecurity breaches in the last five years

Accenture 2019



increase in the cost of cyber crime in the last five years

Accenture 2019

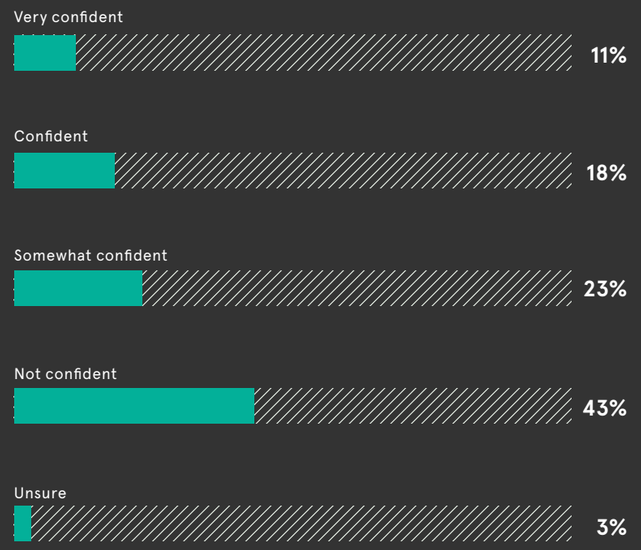
$585m

predicted spending on cloud security in 2020

Gartner 2020

ORGANISATIONS ARE STRUGGLING TO DETERMINE WHETHER THEIR USERS ARE TRUSTWORTHY

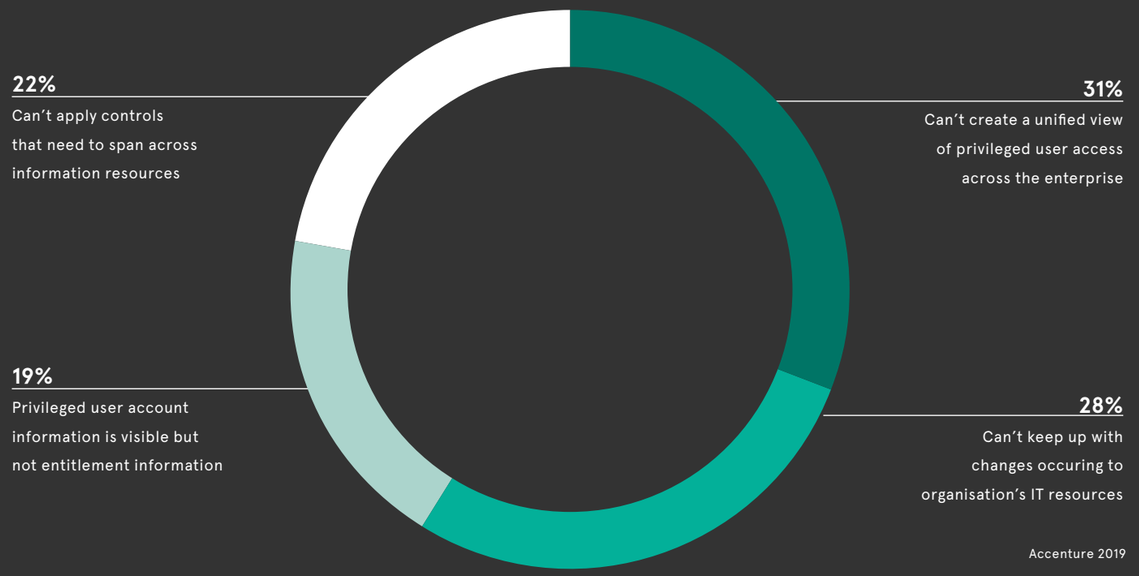
Confidence that an organisation has enterprise-wide visibility and can determine if privileged users are compliant with policies



Ponemon Institute and Forcepoint 2020

...AND CURRENT SECURITY TOOLS MAKE IT DIFFICULT TO DETECT AN INSIDER THREAT INCIDENT

Main reason for organisations' lack of confidence in its users



Accenture 2019

CULTURE

Using the security stack to differentiate your culture

A consistent and enhanced security user experience can differentiate an organisation, winning engagement and loyalty when staff are working from home

Nick Ismail

Almost overnight, the initial disruption caused by the coronavirus pandemic saw a global shift to remote working. This monumental change created a number of technological and cultural challenges that organisations had to adapt to rapidly.

Despite the obvious challenges, the workforce of the future, with millennials and Generation Z at the fore, expect this type of flexibility from their potential employers, and it is often a requirement for attracting and retaining such talent.

COVID-19 certainly accelerated the move to remote work, but it was a trend that was always going to increase, driven by a desire for flexibility from the millennial and Gen Z workforce. As this new normal becomes reality, the question arises how can organisations scale remote access, while ensuring security?

Matt Palmer, director at Cyberclaria, says adding more technology is not the answer, simplification is. "Organisations should replace a complex legacy technology stack with integrated solutions that provide seamless access regardless of where a user is, what equipment they are using, or what systems or applications they need access to," he says.

"Keeping authentication on-premise when the user is operating in the cloud makes no sense; users need to be able to log in once on any device and have a seamless experience."

Creating a better user experience

The accelerated move to remote work has created an opportunity for security and IT leaders to create a better user experience with their security stack.

Currently, the security experience for the user is generally poor and to change this organisations should adopt integrated security solutions that are focused on identity management and cloud scalability. This will ensure the user experience is consistent and flexible, which is necessary in a remote-working environment.

> **SASE is an opportunity to stop using technology to tell staff they don't matter and instead use it to show them they do**

Kelly Bissell, lead at Accenture Security, says security frameworks such as SASE (secure access service edge) enable a consistent access experience in the office or on the road, while adhering to the principles of zero trust.

"Security controls such a trust score can simplify policies, with fewer policies for the same access, to reduce the reliance on user-based authentication and provide a better user experience. Endpoint security controls like containerisation can allow an employee to use their personal device to securely access company resources," he says.

Going one step further in terms of attracting the millennial and Gen Z workforce, organisations should consider adopting technologies, such as biometrics and facial recognition, into their security stack. They are tools younger generations are increasingly using in their social life.

Attracting and retaining talent

Creating an accessible security framework that not only reduces friction with the user, but enhances the employee experience will be vital for attracting and retaining talent, while boosting productivity.

Vince Warrington, chief executive of Dark Intelligence, says this is becoming increasingly important as employees now need to have the same level of user experience working remotely as in the office.

"This means developing solutions that ease their progress rather than restricting it," he says. "We know frustrations with IT equipment lead to poor morale, so the organisations that adapt their security to the new working norms are likely to have an advantage in staff retention and productivity."

Poor morale and constant frustration can also have significant repercussions for security. Employees who have a positive experience with an organisation's security culture are less likely to share potentially sensitive data via consumer applications.

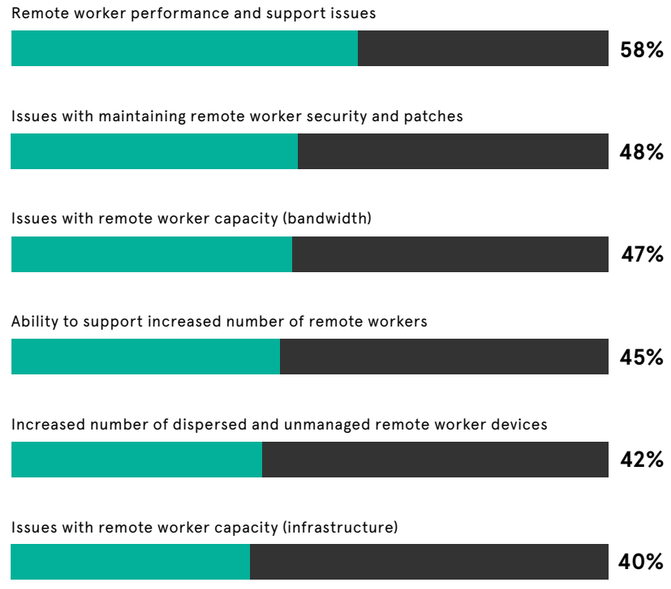
Leaders can use SASE to deliver a strong user experience into the security stack to differentiate their culture and attract the future workforce.

The framework represents the convergence of networking and security. It signals a change to the reality of security being a source of frustration for the user.

By adopting this embedded security functionality, or as Charles Eagan, chief technology officer at BlackBerry, describes it "invisible security", the user experience will be enhanced.

Palmer at Cyberclaria says that in the remote-working era, by providing employees with an inconsistent security perimeter, you are telling them you don't care enough to give them the same experience they would expect as customers. "SASE is an opportunity to stop using technology to tell staff they don't matter and instead use it to show them they do," he concludes.

CHALLENGES BROUGHT BY HOME WORKING AS A RESULT OF COVID-19



Accelerate Technologies 2020

DATA PRIVACY

Solving the trust dilemma

By embracing new approaches, organisations can ensure the security and privacy of their data and systems in the cloud

Christine Horton

Cloud computing was a lifeline for organisations in 2020. It enabled them to quickly stand up new remote workforces and it continues to underpin their day-to-day operations.

Despite this, one feature continues to cause commitment issues around cloud adoption: security.

For the past 12 years, the Cloud Industry Forum has produced an annual report that examines how businesses are using cloud services and their barriers to adoption. "Without exception, every report has identified security as the biggest hurdle and cause for concern by businesses that wish to adopt cloud technology," says chief executive Alex Hilton.

Similarly, recent research by cloud consultancy Contino shows almost half of firms (48 per cent) are deterred from migrating to the cloud because of security concerns. Michael Chalmers, Contino's managing director for Europe, Middle East and Africa, believes the struggle is not so much whether the cloud is secure or not, but between traditional security models and the new world of cloud.

"In the old world, the focus was on defending the perimeter of the system and assuming that everything inside the system was trustworthy. This approach does not work because it gives hackers far too much leeway once they have breached a system. Accordingly, breaches and hacks have been climbing in frequency and seriousness," he says.

Hard shell surrounding a soft centre?

The problem is the cloud is a distributed system, with different users accessing different systems and applications from multiple locations. This forces the adoption of a strength-and-depth approach to security design, which requires layered security throughout each component of the architecture, not just a hard shell surrounding a soft centre.

As such, a zero-trust model has evolved that ensures no user or system, either inside or outside the cloud, is trusted until they have been verified.

"An example of this is the principle of least privilege access," says Chalmers. "This means each user only has access to the systems they need to do their job. This limits the scope of the damage a rogue user or cyberattacker can do, should they gain access to that account. Verifying users is achieved through technologies like multi-factor authentication, identity access management, encryption and permissions systems."

Indeed, Gartner says even the most reluctant organisations should put their concerns to one side, thanks to technologies such as SASE (secure access service edge). This offers a cloud-delivered set of services, including zero-trust network access and software-defined WAN (wide area network), which support secure branch-office and remote-worker access.

> **Key stakeholders are accepting cloud-delivered security as superior and more practical than physical security controls**

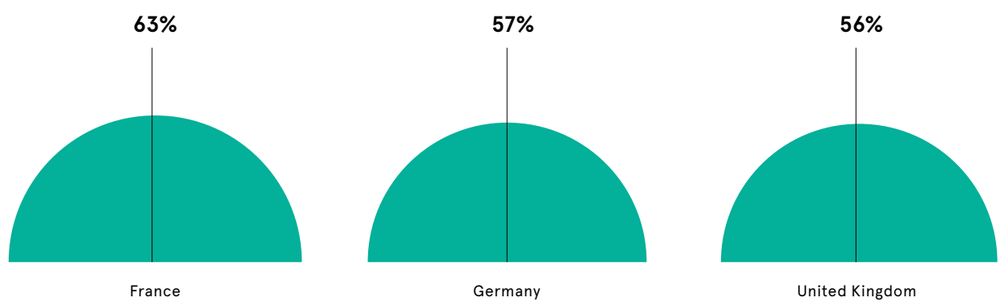
Trust and jurisdiction?

Nevertheless, a common concern in Europe stems from the perception that storing data in the cloud means data falls under the control of non-European entities. This is often wrongly assumed to be less trustworthy and would likely throw up compliance hurdles.

However, Jim Reavis, chief executive of the Cloud Security Alliance, argues coronavirus has disrupted the traditional view of the world defined by national borders. This is because organisations have been forced rapidly to reimagine their organisations in virtual terms as employees are working from home.

"Cloud security frameworks, such as SASE and software-defined perimeter, are being aggressively implemented to support this virtual world," he says. "The key elements to making these frameworks operational and trusted are a dependency on proven identities, authentication, robust encryption and key management with proven roots of trust. As these elements are vetted, key stakeholders are accepting cloud-delivered security as superior and more practical than physical security controls."

ORGANSATIONS MAKING SIGNIFICANT CHANGES IN CLOUD GOVERNANCE AFTER THE INTRODUCTION OF GDPR, BY COUNTRY



Thales Group and Ponemon Institute 2019

LOOKING AHEAD

The SASE-empowered business

SASE, the convergence in the cloud of existing security and data protection solutions, is set to be widely adopted, replacing outdated legacy security measures

Nick Ismail

Gartner, who coined the SASE acronym in 2019, believes secure access service edge will be adopted by 40 per cent of companies by 2024, up from less than 1 per cent at the end of 2018.

Six years is a long time in technology, but Paul Rumsey, operations director at VIVIDA, believes SASE, although still in its infancy, is the logical next step for security. "In five years' time, I would expect it to be an industry standard for businesses, especially with the massive increase of remote workers caused by coronavirus, which is a policy I think a lot of companies will adopt long term," he says.

As the SASE framework becomes more prevalent within organisations, they will have to make sense of all the data this set of technologies creates. In reality, the responsibility should fall to the vendor or platform owner. SASE vendors will be better equipped to collate all the telemetry data coming from the end-user, their location and device, to create dashboards for the chief information security officer as part of the cloud security offering.

"Besides needing to be careful of privacy issues, this data can be kept private and still be used to exponentially increase security and reduce user friction. Additionally, evaluation of when, where and how users interact with applications and features can result in a great deal of useful information to improve user experiences," says Charles Eagan, chief technology officer at BlackBerry.

Zero trust

Zero trust, a key component of the SASE framework, has data at its core and provides continuous authorisation for any type of remote access, linking user risk capacity to whatever resource the user can access.

Behavioural analytics will be crucial for the success of zero trust, providing user risk profiles and scores updated in real time. "This will allow organisations to adjust the level of access allocated to an individual dependent on how risky their behaviour is," says Rumsey. This will enable businesses to adopt a risk-based approach to security.

This proactive attitude to security will also have an impact on an organisation's ability to assess each individual's level of risk based on their user behaviour. The continuous authentication enabled by zero trust, as part of the SASE framework, will create agility in how an organisation can determine end-user access automatically.

"Agility is an important benefit of continuous authentication," says Eagan. "It means even after an authentication event has passed, you can still make a security decision and automate immediate remediation. This allows prevention in most cases and, if not prevention, at least will certainly mitigate damage."

Reducing friction

Organisations are now starting to take note of the benefits of a SASE or zero-trust approach to security.

As the framework becomes more pervasive throughout all systems, it will benefit all employees and, further down the line, customers. Referring to the current security limitations of banks looking to detect and prevent fraud, Eagan says that with SASE and continuous authentication, they can "readily identify fraudulent usage, even if credentials are compromised and used from another device".

This convergence of existing security and data protection solutions in the cloud has the potential to revolutionise security. It will solve a longstanding problem of friction between the user and clunky security requirements, which has often led to frustrated workers and more security incidents.

"By making the relationship more harmonious, we will hopefully see a decrease in the number of security incidents caused by human error," Rumsey concludes.

54%

of organisations are prioritising initiatives to improve visiblity and security for home workers and cloud infrastructure

Accelerate Technologies 2020

> **SASE will solve a longstanding problem of friction between the user and clunky security requirements**

RACONTEUR

Forcepoint