SASE & ZTNA

Writings from the frontline

techradar.pro

perimeter 81

The leader in Zero Trust Network Access technology

- Protect your network, applications and critical cloud resources
- A radically simple and unified network security platform
- Easily build, manage and monitor your hybrid network
- Activate industry-leading Zero Trust security

Enjoy two months free with our TechRadar-exclusive promotion

Get two months free

Exclusively for techradar.pro readers

*Upon signing up for any annual plan, you will be eligible to receive a two-month refund after the subscription end date.

Challenging times

By Désiré Athow, Managing Editor, TechRadar pro

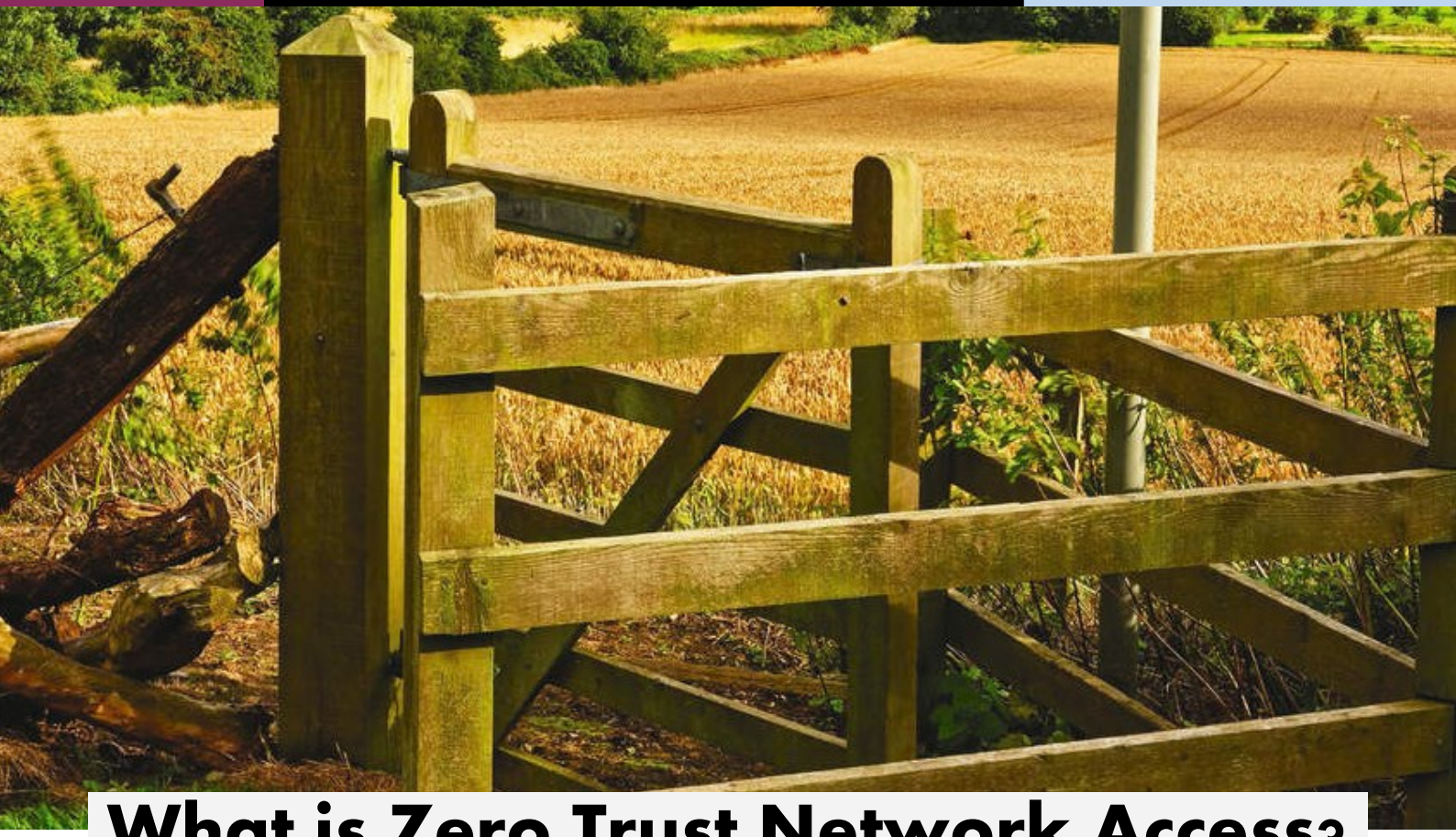
As I am writing this note, Europe is facing one of its biggest existential challenges since the end of the Second World War. But where before major conflicts were often preceded by secret sabotage operations and intelligence gathering behind the enemy lines, technology now allow adversaries to pit virtual swords against virtual shields. A game of cat and mouse that happens in the shadows and where we only occasionally catch a glimpse of what's happening in a universe so close, yet so remote.

The nature and pace of technological evolution means that entities, big and small, can use the same arsenal to achieve their goals. Tight international embargoes didn't prevent units operating within North Korea or the Islamic Republic of Iran from launching waves of cyberattacks in enemy territories on sensitive infrastructures.

Restrictions imposed on Russia (hello SolarWinds) and China didn't prevent them from purportedly ransacking and exfiltrating terabytes, if not petabytes of data from the west, either for the benefits of the regimes in place or for their operatives. Which brings us to **ZTNA** (Zero Trust Network Access)

(Read the rest of this editorial on page 24)

Table of content



What is Zero Trust Network Access?

By Sead Falipasic

Zero Trust Network Access (ZTNA) is an IT security solution encompassing multiple technologies that seek to circumvent challenges associated with the overreliance on the security model based on the concept of perimeter.

As such, this model found its place as one of the key features of the Secure Access Service Edge (SASE) framework which converges networking and security technologies as part of a single cloud-delivered platform. But, how does Zero Trust Network Access actually work, and how does it relate to other seemingly similar concepts?

What is Zero Access?

At the heart of ZTNA is the concept of zero access. It is, in essence, a negation of the popular perimeter-based security model. With this one, there is the default assumption that users and devices found in the perimeter or behind it are to be trusted. The reason for it is the mere existence of a perimeter which, supposedly, filters out the undesirables and leaves all those who manage to pass it to do as they please afterward. This is why any device or a user can get access to whatever assets are found behind the perimeter as long as they pass its initial check.

This approach does not cut it today, simply because any hole in a perimeter can lead to catastrophic outcomes, not to mention the internal threats posed by the malicious actors or devices that are "trusted" simply for the fact that they exist on the other side of the perimeter fence.

The zero access model aims to do away with these default assumptions about someone's or something's trustworthiness based on their relative position in the security perimeter.

With ZTNA, being deemed as a trustworthy actor a second ago means nothing in the following second – you are not to be trusted by default at any time, so enforcing zero-trust policy everywhere and all the time is the order of the day.

Principles of ZTNA model

So, the ZTNA model is simply a practical application of the above "trust no one" principle. On a more granular level, this simple motto is spread out across several key principles.

- Each data source and computing service is treated as a valuable resource.
- All communication is protected regardless of a network location.
- Access to individual resources is granted based on each individual session.
- A policy that governs access to resources is highly dynamic. It encompasses applications and services, requesting assets, the observable state of client identity, and other parameters.
- An organization is tasked with overseeing and controlling the security posture and the integrity of all assets.
- Authentication and authorization for each resource are dynamically implemented and strictly practiced prior to granting access to any actor that requests it.
- An organization is constantly receiving information on the current state of resources, networking and communication systems, and assets with the goal of taking its security preparedness and responsiveness to an optimal level.

ZTNA and SASE

As a core of the SASE model, ZTNA also converges networking and security, but on a smaller scale. As a cloud-delivered model, ZTNA is easy to implement by an organization of any scale. Once it is up and running in the cloud, this service will provide a user with a secure omnichannel (a tunnel) which receives all network traffic for all devices in use.

Filtered in this manner, the traffic will be steeled against the tampering of any type in addition to its flow being constantly overseen. In the process, ZTNA will gather huge amounts of data on the usage of existing resources which gives valuable insights that can easily find their place in future audits and reports.

What happens in case the ZTNA framework detects a security anomaly? Access to all devices related to it is immediately denied. To minimize the number of these instances, all users and client devices will have to be authenticated and verified whenever they ask for access to individual resources, in line with the zero-access approach. This approach is further reinforced by enforcing yet another principle – that of the least privilege, meaning that you are given a minimum level of access in order to perform a particular task and no more than that.

Continue to read on page 8

Time for VPNs to go? Why zero trust is critical to security

By Jonathan Lee, Menlo Security

With remote and hybrid working model here to stay does it spell the end for VPNs? Remote and hybrid working models are common today, but such was not the case prior to the outbreak of the Covid-19 pandemic.

For many companies and organizations, cloud-based working accelerated, born out of necessity rather than convenience. As lockdowns and stay-at-home orders were enforced almost overnight, many traditional organizations were forced to digitize to ensure that they could continue to operate as social contact was limited by law (was it law or government mandate?).

Amidst this turbulence, many turned to virtual private networks (VPNs) as a first port of call – a familiar face when it comes to providing remote access to centralized networks, acting as a relatively straightforward extension of on-premises IT infrastructure.

A recent Menlo Security report shows that this was a popular course of action. In the survey of more than 500 IT decision-makers across the US and the UK, 75 percent of organizations said they still use VPNs for controlling remote access to applications. Further still, this rises to more than four in every five for organizations with more than 10,000 employees.

However, many of those that opted to take this path will have since found that it is fraught with challenges and obstacles. Put simply, this is because they are likely to have uncovered some of the inherent issues with VPNs.

VPNs are tricky and time-consuming to operate, placing a strain on IT workloads and

resources where IT managers are forced to administer individual access requests for multiple users. This creates inefficiencies and unwanted costs for companies - businesses that may well have been looking to make operational savings in light of the economic uncertainty caused by Covid-19.

It is not just the productivity of IT departments that suffers at the hands of VPNs, however. Equally, with too many people trying to access a VPN at one time, networks can quickly become overwhelmed, leading to traffic bottlenecks and limitations in regard to file, data and resource access for all employees.

For this reason, VPNs can become a significant source of frustration – and this frustration is often manifested in actions that can undermine an organization's security posture. Instead of waiting for a VPN to load, employees will often choose to work more quickly, effectively and efficiently by going directly onto their desktops, downloading key data, files and resources to their devices, and leaving them more vulnerable to attack.

Indeed, this is of particular concern given how the endpoint has become a primary focus for many cyberattacks today. Ransomware and malware, for example, work where an endpoint – such as a laptop, or mobile device – is infected with a malicious payload.

The challenge stems from the fact that VPNs simply weren't designed to be the bedrocks of remote and hybrid working models, creating a domino effect of productivity and security issues.

The three key principles of zero trust

Thankfully, with hybrid and remote working models seemingly here to stay in the long-term owing to a plethora of business- and work-life balance-related benefits, many organizations are beginning to consider new options.

The same Menlo Security survey shows that 75 percent of organizations are currently revaluating their security strategies, this finding which is cause for optimism. However, what is arguably more important is that these intentions result in genuinely useful changes that will see organizations adopting scalable, productive, secure and futureproof policies, protocols and solutions.

Zero trust should form the backbone of all security measures today. Unlike VPNs, zero trust is an ideology that has been designed specifically to bolster security and maintain productivity in cloud-based environments, structured around three key principles.

First is the notion of continuous authentication. It demands that all internal and external network users are authenticated, authorized, and continually validated before they are granted access to applications and data.

This moves away from traditional 'castle and moat' approaches to security that assume all internal network parties can and should be trusted – an assumption that has become a great source of vulnerability in the modern-day.

Second is the implementation of the principle of least privilege. This focuses on limiting the access of network users to only those specific applications and areas of the organization's network that they need to do their job effectively. Privileged accounts are the holy grail for attackers, so limiting these within an organization is vital.

Third is working off the assumption that a security breach is always just around the corner – by always anticipating an attack, securi-

ty will remain a central focus that is considered in all key decisions, which will serve to eliminate potential vulnerabilities.

Improving security posture through isolation technology

Zero trust is so effective because it focuses on protecting beyond the perimeter. It sees trust as a vulnerability, and therefore takes an alternative default 'deny' approach.

Indeed, many of the most revered cyberattacks of recent times have been successful because of a lack of defences beyond the perimeter. Without zero trust, hackers that are successful in infiltrating a network can move laterally with ease to elevate their privileges, exfiltrate data, execute ransomware attacks and more.

Currently, little more than one in three (36 percent) of those organizations we surveyed have adopted zero trust as part of their remote access strategy. Yet as companies begin to reconsider their security strategies, there is fortunately an easy way to achieve zero trust in its truest sense.

Enter isolation technology – an innovative solution that eliminates any opportunity for hackers looking to infiltrate an organization's network by creating a digital air gap capable of preventing all malicious payloads from executing on their target endpoints.

In practice, it moves day-to-day activities from the desktop to the cloud to ensure that all content is safely rendered, and total peace of mind provided.

Simply put, if a malicious payload is downloaded, it cannot reach the endpoint, cutting cyber attackers off completely with holistic, reliable protection.

(from page 5)

ZTNA Vs. VPN

ZTNA and virtual private networks may appear similar considering that some of their functions do overlap. Yet, these are implemented and managed in a different manner.

For starters, ZTNA does not leave VPNs without work. You may still need to link separate sites with shared assets and apps via a VPN. What ZTNA brings to the table is its native support for mobiles devices, its focus on vigilance over what happens on the network, prevention of popular attack types, auto segmentation, etc.

Finally, both ZTNA and VPN implement the concept of a secure tunnel, but ZTNA uses newer and more advanced protocols for this purpose.

Conclusion

Zero Trust Network Access (ZTNA) is a framework for the implementation of the zero-trust approach. It is a fundamental component of the Secure Access Service Edge (SASE) framework.

With it, the secure assets of an organization or an enterprise can be accessed only if the ZTNA system establishes the trustworthiness of an actor that seeks any level of access. Unlike what is found with the perimeter-based security models, this does not involve networking a user or device with a server that needs to authenticate the party in question. With ZTNA, no interaction of that type is enabled prior to establishing the trust level associated with a particular actor.

That being said, ZTNA is still an evolving model, but its disruptive potential in terms of eliminating obsolete security practices cannot be overstated.

The great cybersecurity post-Covid dilemma

By Rajat Toshniwal, Pimcore Global Services

Let me start with a short story to set the context. Mark handles the infrastructure for a renowned organization. He holds vital and confidential information and manages access to his company's critical data. The post-Covid world order has brought some significant shifts to the way Mark works. Here's assessing the situation pre - and post-Covid for Mark.

How pandemic impacted the organization security

Due to the pandemic, workplaces moved from office to home. While remote work culture flourished and proved to be a success in terms of productivity, flexibility, and performance, on the flip side, employees working from home became susceptible to much greater risks.

Because home connections are less secure, cybercriminals have an easier entry into the company's network. Remote work culture has exposed significant vulnerabilities in the security model, offering considerably lesser protection and no network perimeters, thereby increasing the surface area of attacks.

CrowdStrike CEO George Kurtz has alleged that Russian foreign intelligence service (SVR) hackers capitalized on the architectural limitation of Microsoft's authentication process by falsely impersonating to jump from customers' on-premises environment onto the cloud and to the cloud application during the SolarWinds campaign.

Remote worker poor practices

With the absence of company premises or an office as an intermediary, threats such as phishing, ransomware, polyglot, and IoT attacks, along with the approaches like daisy-chaining, loom large and can permeate easily, where attackers can easily evade the home network first and then evade corporate defenses.

Research conducted by Tessian, highlights some astonishing insights over changes in user behavior with respect to organizational security policies. Almost 40 percent of respondents indicated that their cybersecurity behavior at home is different from what they practice at the office.

More than a third of those surveyed admitted to picking up bad cybersecurity practices and using security workarounds while working at home. The majority of remote workers allow household members to access corporate devices for personal use. Users neither patched the home Wi-fi devices nor secured it by using the firewall options.

To address the threats properly, we need to understand the main impetus behind the scenes.

• Larger attack surface

More and more home devices are now getting smarter using IoT technologies like smart refrigerators, smart ovens and smartwatches etc., which provides myriad opportunities to the attacker.

Organization will have to adopt the software-as-a-service (SaaS) communication and collaboration services in a much more rapid way to support business continuity. This has opened another communication channel between end-users and services.

The tremendous increase in the time spent on social media sites, helps attackers in carrying out social engineering and phishing attacks. Social engineering attacks have jumped from 20,000 to 30,000 a day in the U.S.

• Develop corporate skills and capabilities against threats

Cyber-attacks are not really a challenge that cannot be dealt with; what really matters is the need to keep a constant vigil as companies try to ceaselessly protect themselves from the ever-present cybercriminals looking to infiltrate defence systems. Cyber risk will have neither a defined solution nor a concrete endpoint. There is a need for an organization-wide security framework that not only defines the policies to restrict the attacks but also what is needed to be done in case of attacks, the measures to identify risks, and the need to on a continuous loop of improvement.

• Humans are the weakest links

A majority of organizations focus their strength and expense on buying advanced security equipment in order to safeguard their systems. But in reality, until and unless employees are properly and regularly trained, organizations will remain susceptible to the majority of cyber-attacks. Cybercrime evolves quickly, and employees need to be kept up to speed and educated continuously; it's pretty much like a health check-up that ensures that the body is responding appropriately.

• Other mitigation frameworks

To mitigate the security risk due to no network perimeter, organizations are shifting towards SASE (Secure access service edge), zero trust, and XDR (Extended detection and response) to ensure the security of remote users and their data. All these approaches are spreading like wildfire in the industry.

SASE

'Secure Access Service Edge' is a term coined by Gartner in 2019. It combines some of today's most popular technologies into a single solution. Incumbent players such as Palo Alto Networks, Microsoft, McAfee, Cisco, Zscaler, Fortinent, Forcepoint, and more have taken steps to launch initial SASE solutions in 2019 and early 2020.

It works on the principle of ZTNA (Zero Trust Network Access), which says no matter from where users are getting connected as long as they can prove their identity and verify the devices with which they are connecting, the connection is secure. Once the verification is over, users can only access the resources to which they are authorized (policy-based). Endpoint clients are used for sending the requests to the nearest inspection points and SDP controllers/gateways are used for setting up the tunnels to access various applications.

In contrast to the traditional approaches like VPN for connecting to centralized office headquarters and from there to other cloud platforms or SaaS-based applications which result in high latency, expensive circuits, and bigger inspection devices to handle the circuit, SASE approach is much simpler, optimized, and inexpensive, it makes its inspection engines available at regional PoPs location through a SaaS model approach.

XDR

Extended detection and response, collects and correlates data across email, endpoints, servers, cloud workloads, and networks, enabling visibility and context into advanced threats. These threats can then be analyzed, prioritized, hunted, and remediated to prevent data loss and security breaches. It highly improves the detection and response speed and provides a framework to investigate the threats more effectively and efficiently.

It is done by combining the capabilities like security information and event management (SIEM), security orchestration, automation, and response (SOAR), network traffic analysis (NTA), and endpoint detection and response (EDR).

Advanced XDR vendors are focusing up the stack by integrating with identity, data protection, cloud access security brokers, and the secure access service edge to get closer to the business value of the incident. XDR enables an enterprise to go beyond typical detective controls by providing a holistic and yet simpler view of threats across the entire technology landscape.

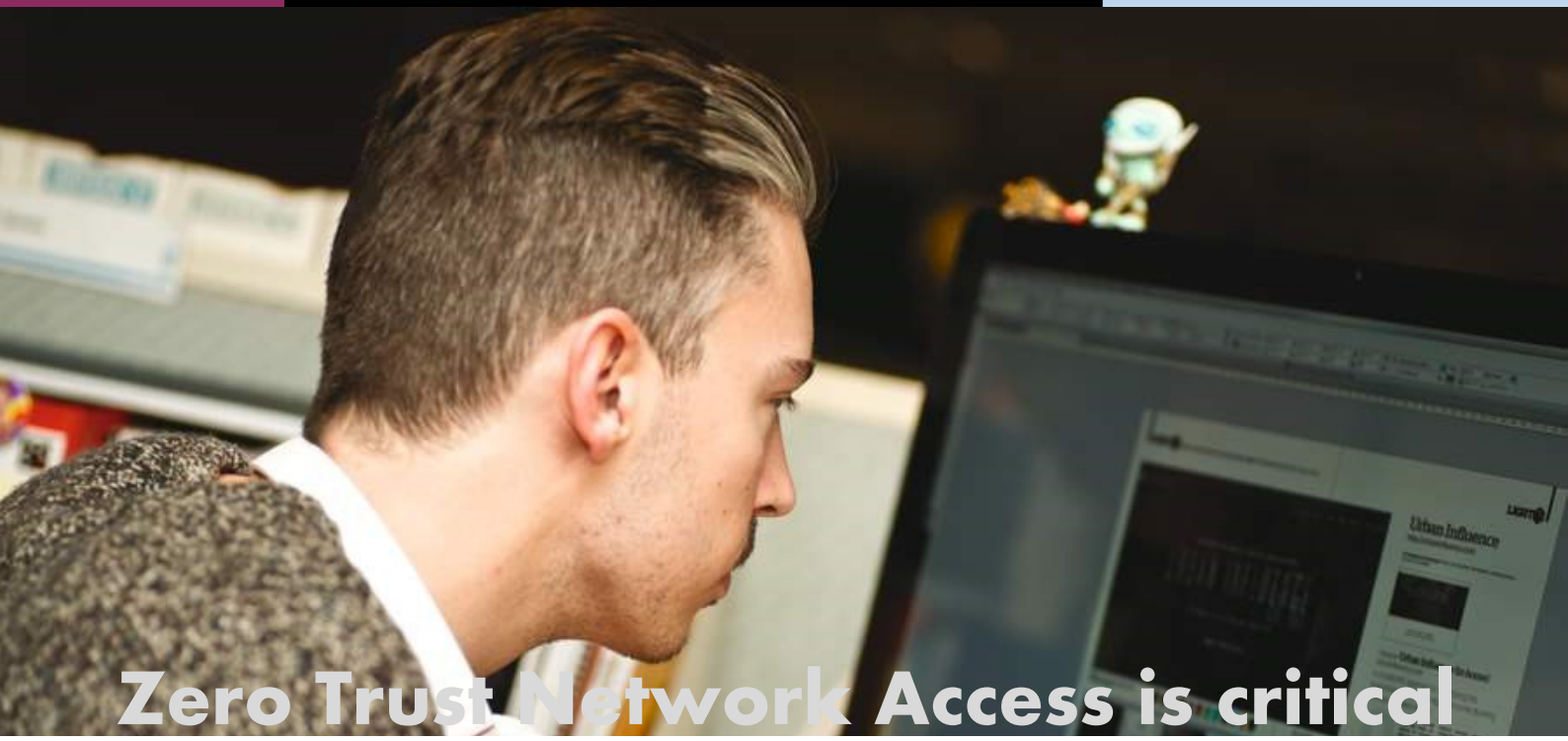
Extended Detection and Response (XDR) holds the promise of consolidating multiple products into a cohesive, unified security incident detection and response platform. XDR is a logical evolution of endpoint detection and response (EDR) solutions into a primary incident response tool.

Conclusion

The unforeseen Covid situation has left many businesses unprepared to deal with a storm of cyberattacks targeting their employees and data, causing a global change towards remote working.

Along with some benefits, it comes with a huge shift in the security paradigm. New risks because of this can be mitigated by implementing proper tools, frameworks, policies, and practices that will help in reducing the overall attack surface area.

Strong passwords, VPN, and best email practices help secure remote working processes; along with it security frameworks like SASE and XDR help in protecting businesses.



Zero Trust Network Access is critical for today's mobile worker

By Aaron Kiemele, Jamf

Today, more organizations are offering the option to work from home, in the office or a mix of both, and company leaders are being forced to contend with the issues that come with this work landscape, looking for options to increase protection and achieve airtight cybersecurity. When many employees were forced to work from home during the COVID-19 pandemic lockdown, organizations quickly found their security measures were lacking in a new work-from-anywhere environment. Now, it's out with the old solutions like VPNs, and in with the new. Enter Zero Trust Network Access (ZTNA).

ZTNA operates on a model that does not grant immediate or ongoing trust to any user, instead granting application access on a strictly need-to-know basis. ZTNA technology zeroes in on each individual user and device, rather than allowing full access to any given network. It's a tighter way to keep a company (and users) safe, working on an individual basis to determine whether an access request is trustworthy at a particular moment in time.

ZTNA determines if a user or device is suspicious by looking at a number of factors, giving you visibility into whether device security is put at risk due to an unintentional slip up, one that could allow outsiders into a company's network and data. Essentially, the ZTNA model has moved forward from trusting the entity to only trusting the transaction. There are a variety of reasons for companies to consider switching to ZTNA—here are a few.

Ideal for work-from-anywhere

Flexibility has proven an important tool in achieving work-life balance, and many employees have shown they're just as productive at home as they are in the office. While some companies are returning to full in-house operations, many will continue to offer remote work options for employees.

However, working from anywhere exposes companies to expanded risk, particularly as employees operate from multiple devices across multiple networks. VPNs and other traditional security simply can't keep up with emerging risks because of its cumbersome configuration and limited flexibility. ZTNA, on the other hand, allows configurable and precise access to applications across networks, with quick and seamless checks along the way. This prevents any nefarious actors or malware from accessing an entire network at once—it's far easier to detect attempted untrustworthy activity when us-

ers, devices, and services are making security decisions at each step along the way. Enhanced security gives companies and employees the freedom to safely work from home, on other private networks or in a public setting without having to worry or be burdened by cumbersome processes.

Enhanced ability to work from any device

Just as ZTNA reduces a user's and organization's risk by limiting the scope of any authentication to a limited application or service, it also gives employees the freedom to work from any device without compromising productivity OR security. From smartphones to tablets, personal laptops to company computers, the average employee accesses sensitive company data across a multitude of devices. It's an important development in the work-from-anywhere model, and one employees rely on to complete tasks and communicate outside of an office setting.

The core philosophy of ZTNA is that trust is not given, it is earned through deep visibility into device posture and authorization. After all, devices can be stolen, multiple people may operate on one device, and mistakes happen. By requiring devices to pass security checks each time a device requests access to an application, company leaders can rest easy, even while knowing their employees operate across multiple devices.

Protects companies from sophisticated attacks

Cyber-attacks are becoming more frequent and sophisticated as criminals take advantage of existing and emerging vulnerabilities around the world. There is no longer a hard shell - soft center, no single point of ingress that could allow an evildoer access to enter an entire network. It lets you segment resources at a very granular level. It removes firewalls as potential keys to the kingdom.

Additionally, in a zero trust world, lateral movement and privilege escalation are much less likely. With constant iterative reevaluation of trust, an attacker can't take the one thing they acquired and leverage it to access your neighbor's machine - they are also going to be expected to have a good systems posture, authorization and repeated authentication to services/data. Hackers are extremely familiar with VPNs, how they work and how to exploit the weaknesses inherent to those systems. Often this weakness is single check or basic authentication that once complete grants trust to all future activity.

VPNs are also expensive and only solve network access security issues if someone can hack or exploit their way into the VPN, they may gain access to an entire host of applications and sensitive data. They neglect to account for authentication of users or devices. ZTNA, on the other hand, adds several layers of protection against increasingly sophisticated criminal efforts.

Many companies have taken notice - a Gartner report found that by 2022, 80 percent of new digital business applications will be accessed through ZTNA. Further, the same study found that by 2023, 60 percent of enterprises will phase out most of their VPNs, trading them in for ZTNA.

To protect against data breaches, it's essential to consistently be improving your security posture to keep up with the criminals who are constantly improving their capabilities. You can't use yesterday's technology to solve for tomorrow's problems. The ZTNA model provides that protection in a far more secure way than VPNs, as it is not a single gatekeeper for all your data, but a real process for ensuring continuous monitoring, evaluation and RE-evaluation of the trust you are leveraging to access a resource. It's the kind of protection users want, presented in a streamlined fashion that can give both users and organizations peace of mind.

Networks have to be secure, but that security shouldn't prevent innovation and forward movement in business. The purpose of ZTNA technology isn't to stop users from accessing company data—it's to empower organizations to move at the speed of business to improve operations, without constantly worrying about the next security breach.

Getting sassy with SASE

By Francois Champagne, Expereo

Networking and security are two of the most important features of any company's technology infrastructure. As the world of work evolves, businesses need to adapt to ensure that they are best equipped to manage shifting demands - like a location-agnostic workforce or ready access to third party apps as a standard requirement of the average employee. Evolution requires a fresh approach and new thinking - and that's where Secure Access Service Edge (known as SASE) comes in.

It is an emerging offering that combines comprehensive WAN capabilities with enhanced network security functions (such as Secure Web Gateway, Cloud Access Security Brokers, Firewall-as-a-Service, and Zero Trust Network Access) to support the dynamic secure access needs of digital enterprises.

SASE shifts the emphasis to authenticating users and devices on an 'as-permitted' basis at the network perimeter, rather than using the 'once logged in, always logged in' approach to an in-house setup. With devices, data, and apps far from the corporate HQ, and connectivity taking place on public Wi-Fi and home broadband, it may no longer be sufficient to secure access only to the network, but to also ensure secure access happens at the level of the application.

The past year has seen a surge in demand for SASE, predominantly driven by the huge increase in people working from home who access applications in the cloud using their own devices.

SASE provides holistic security

A basic concept uniting SASE security is that it's software-defined. SASE is fine-grained in how it grants access to data and applications and how it approves access

to those applications. SASE implementations put authentication closer to the user and device. Before SASE, it was normal for authentication data to make a round-trip to the corporate data center and back since most users enjoyed a direct connection to that corporate network within the firewall.

SASE includes network security functions including Zero Trust Network Access (ZTNA). If a device is user-owned it may be that the owner uses public Wifi, or is sharing WiFi with their family. This means data can leak and is compromised, all issues which ZTNA resolves. ZTNA grants access to specific applications rather than the network as a whole, with IP cloaking making that access invisible even to malware on compromised devices to keep the network perimeter safe. In metaphorical terms, SASE can hide a door, rather than just open or close it, meaning that your data is protected since it only opens to people who know it's there.

Simplified adaptable management for the future

A benefit of SASE is its flexibility. To authenticate users at a company level, the need to operate a one-size-fits-all security infrastructure at the network core is hard and costly to maintain. The cloud-based approach of SASE and the services it provides mean that it can provide security authentication via flexible APIs and protocols.

Reduced costs with security outsourced to the cloud

The cost implications of going cloud-native apply to SASE as much as any other application. By pushing security infrastructure out to the perimeter where the user and their device are, there's less need for heavy security investment in the corporate data center. Cloud services expand or throttle capacity based on what the network needs which means fewer resources need to be spent on maintenance and replacement.

Like much of cloud computing, SASE carries a sound business case. Gartner predicts that by 2025, over two-thirds of corporate organizations (60%) will have solid strategies for adopting SASE across their user bases. Up from 10% in 2020, which would be, partly due to the massive cost savings for businesses when adopting SASE. Gartner also predicts within three years, 30% of corporations will get their SWG, CASB, FWaaS, and ZTNA solutions from a single vendor. That's a six-fold rise from where we are today as businesses consolidate their solutions for ease of management and peace of mind.

The scalability model

With its emphasis on securing the user and not the network, the classic corporate, authentication model becomes scalable. SASE creates an organized list of resources, each user enjoys a set of permissions to access one or more of them, and no extra resources are needed in the IT Suite no matter how large the user base grows. Users can use the network of cloud services and public networks, like work-from-home broadband which again reduces pressure on company headquarters.

An increase in performance

The cloud may appear to be all-encompassing for some users. Their home fiber can reach gigabit speeds; the mobile world is turning 5G; even coffee-shop Wifi frequently exceeds multi-megabit rates. With SASE the network perimeter is defined by protocols in the cloud that apply directly

Continue to read on page 24

In a post-Covid world, the future of cybersecurity is SASE

By Jim Fulton, Forcepoint

You don't need me to tell you our lives have changed a fair bit in the last year. How we shop, how we socialize, how we work - the pandemic has forced us to upend the way we live our lives. Some of these changes will recede once we exit the shadow of Covid-19. But others will stick with us, particularly as the pendulum swings back and people begin to work in multiple places at once - at home a few days a week, in the office, even travelling.

The pandemic has had an accelerating effect: those enterprises who embraced digital transformation have doubled down on their investments, while laggards have found it more difficult than ever to keep pace. Agility. Flexibility. Transparency. These were all nice-to-have pre-2020. But today, they are business staples.

We're now living in the age of the 'unbound enterprise': enterprises that are free from physical and network infrastructure limitations. And while there are a number of hoops businesses must jump through before achieving this status, one of the biggest – and most daunting – is cybersecurity. Simply put, cybersecurity cannot remain dormant. When employees can work from any location around the world, simply defending laptops within the office is not enough. Businesses' IT estates have widened considerably, and with that comes the need for a new approach to cybersecurity.

Embracing a different approach: SASE

Secure access service edge is an emerging cybersecurity architecture that everyone now seems to be talking about. In essence, SASE reinvents networking and security technologies that used to be delivered in hardware appliances throughout the enterprise, replacing them with converged cloud computing services that can be used seamlessly from anywhere. By weaving together ad-

vanced security capabilities including web content inspection, malware scanning, URL filtering, cloud application access and advanced data protection, SASE architectures offer security that is smarter, more dynamic, and 'always on' no matter where people are working – perfect for a world where cybercriminals never rest.

We've recently conducted research in partnership with WSJ Intelligence, surveying 508 CEOs and CISO around the world. One thing that has really stood out is just how perceptions have changed about SASE – and cybersecurity in general – since the world was rocked by Covid-19.

For example, 48% of businesses say they are substantially increasing the use of cloud-based cybersecurity systems, and 58% recognize the need for a more integrated trust framework. This indicates businesses understand the needs for more distributed connectivity and security, and are putting in place plans to make it a reality.

When asked directly about SASE, the enthusiasm is even more pronounced. 90% of CEOs have either already adopted SASE (43%) or are currently evaluating SASE with a view to adopt (47%). It's pretty astounding that this approach has gone from a future dream to an everyday reality so quickly – to the extent that nearly half of businesses have adopted it. It's testament to just how much the pandemic has accelerated technological progress, and forced businesses to rethink how they handle cybersecurity.

Reimagining cybersecurity

And that last point is important. Because as the security needs of businesses change, the role of cybersecurity – and the roles of cybersecurity professionals – changes with it. Some 45% of businesses have accelerated their digital transformation plans as a result of the pandemic. But what's also interesting is that 45% report cybersecurity now has a bigger role in enabling innovation. Furthermore, 41% agree that it delivers a competitive edge.

It's been said defense is the best offence. And in a way, that's true here. For the unbound organization, cybersecurity which is not up to scratch can be one of the biggest limiters of growth. The more a business decentralizes its people and data, more opportunities are created for thieves and attackers to break into systems and steal valuable information.

Having a solid foundation of cybersecurity based on SASE enables businesses to scale up their operations, launch new services, and enable more staff to work remotely without fear of security breaches. Through this lens, cybersecurity isn't just about protection: it's about enablement. It allows businesses to pursue their ambitions and innovate without fear.

Of course, the pandemic isn't over yet. The pace of change is still lightning fast. And even when we do return to some semblance of normality, businesses are not going to want to slow down. Instead, we're already seeing "work-from-home" evolving into the "hybrid workforce" in which people work in different locations throughout the week. It's no coincidence that 74% of funds were reallocated to cybersecurity programs during Covid-19. Businesses have discovered security is one of the keys to unlocking the future, so we are going to see more and more investment

SASE has well and truly become the new de facto standard for delivering cybersecurity. And as we press on into a post-pandemic world, it's exciting to see what innovations this new generation of security will enable.

Better together: Zero trust and SASE

By Anurag Kahol, Bitglass

The exponential rise in remote working caused by the Covid-19 pandemic has left a huge number of organizations suddenly coming to terms with new, highly dispersed IT environments. Such environments pose a number of challenges when compared to the more traditional on-premises alternatives that most organisations are used to, but perhaps the biggest challenge of all is how to secure them effectively.

Two of the best approaches currently available are Zero trust and secure access service edge (SASE), but many organisations mistakenly believe they are mutually exclusive. As a result, cybersecurity teams are trying to rapidly educate themselves on both approaches before deciding which path to take. However, the good news is that they are highly complementary to each other. In fact, in nearly every situation they work best together, supporting security teams as they aim to prevent their environments stretching beyond the bounds of their control.

A fundamental shift has taken place

In the past, companies that wanted to establish secure remote working solutions would typically turn to tried-and-tested virtual private networks (VPNs) to give employees access to on-premises networks from anywhere, via a 'virtual tunnel'. However, the main security premise that VPNs are built on has become increasingly outdated in recent years - the notion of a clear network perimeter.

With a VPN, users judged to be 'trustworthy' can go wherever they like inside the network, while everything/everyone else is blocked from entering in the first place. Such an approach fails to account for critical threats like insider attacks, or the fact that non-employees may need to access the network from time to time as well.

But perhaps the biggest flaw with VPNs is that once someone is inside, they pretty much have free reign to do whatever they want. If a cybercriminal were to gain access via something as simple as compromised credentials, they would be able to go wherever they like and take anything from the network, no questions asked, because the VPN would view them as a trusted user.

Further, during this period, an increasingly large number of companies started to go

directly to the cloud. This resulted in the surge in cloud application usage and consequently, a large blind spot that was outside of the purview of the traditional perimeter. Fortunately, a growing number of businesses realize the inherent dangers of this, which is why IT management teams around the world are revisiting infrastructure in their droves, to find a better balance between productivity and security in this unfamiliar new working environment. Forward thinking organisations are adopting zero trust and SASE solutions together because doing so enables them to combine a least-privilege access approach with an architecture that streamlines how highly distributed users and cloud resources are secured.

A new cybersecurity approach to match the 'new normal'

The need to maintain operational efficiency across remote workforces, means businesses are, understandably, putting more and more of their applications into the cloud. In order to secure these expanding surface areas, they require policies that enforce least-privilege access control via technologies like zero trust network access (ZTNA), secure web gateway (SWG), and cloud access security broker (CASB), just to name a few.

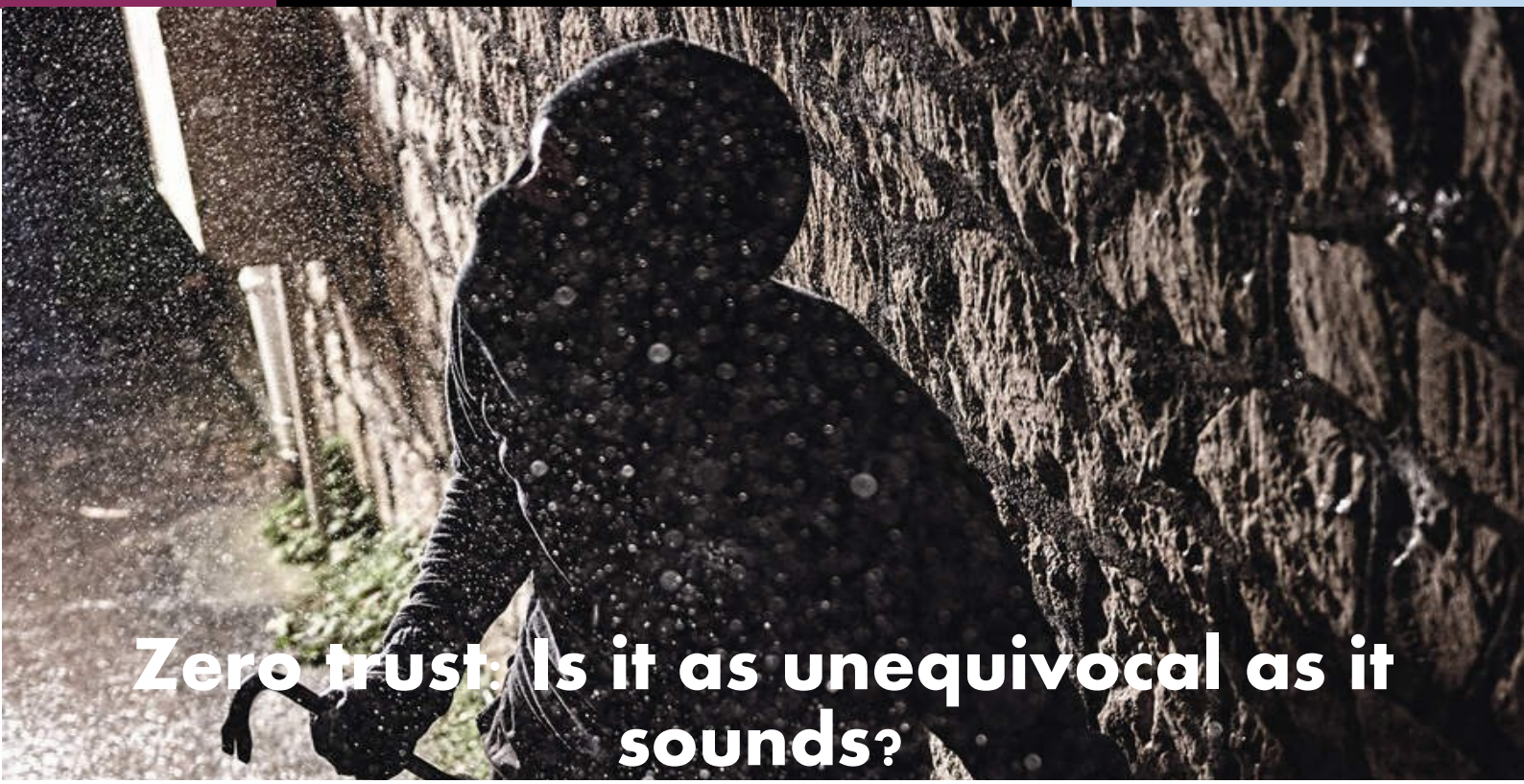
However, when these kinds of technologies are deployed on a one-off basis, it can leave businesses needing to manually replicate policies across different dashboards, which can be a laborious process, costing both time and money. It also limits consistent visibility and control across the IT ecosystem, which is highly problematic. Furthermore, the more solutions that get deployed, the worse the issue tends to become.

While zero trust is a way of thinking that focuses on appropriate authentication and secure access to data and systems on an as-needed basis, SASE refers to cloud-delivered platforms deployed at the edge, which provide far-reaching protections anywhere data goes. As integrated platforms that consist of an array of complementary solutions, SASE offerings are crucial when following a Zero Trust framework.

More consistent, comprehensive protection overall

In some instances, organisations following zero trust security principles can unintentionally drive up the amount of deployed point products, resulting in disparities in levels of protection across different use cases. SASE helps alleviate this issue by preserving and maintaining common security controls across all enterprise resources, helping remove blind spots that can/would otherwise arise. Security professionals can configure policies that control access to web destinations, safeguard SaaS apps, identify shadow IT, and secure apps on-premises, all from a single control point. Not only does this result in more consistent, comprehensive protection overall, but the greater ease of management can save significant amounts of time and money as well.

Over the past 12-18 months, the business landscape has changed beyond all recognition, forcing organisations of all shapes and sizes to adapt along with it. For many, this has been a major challenge, particularly when it comes to securing new, unfamiliar remote working solutions in a fast and effective manner. Often it's down to confusion over the solutions available and a mistaken belief that it's an 'either/or' decision. In fact, by uniting SASE and zero trust instead of choosing between them, organisations can create a reliable and secure environment that enables employees to easily interact both on and off premises, optimizing operational efficiency while keeping sensitive data safe wherever it goes.



Zero trust: Is it as unequivocal as it sounds?

By Neil Thacker, Netskope

Zero trust is today's favorite buzzword, and so of course it is being used liberally, and often imprecisely. Originally conceived when businesses only had a small percentage of remote workers signing in to the corporate network, the common wisdom of the day dictated that you couldn't implicitly trust the authentication of those remote users any longer because they weren't on the company network.

The original Zero trust solution focused on proving the identity of the user and the device. Things have evolved a little over the years, and there are probably now as many different approaches to Zero trust as there are vendors pushing it, but most cybersecurity professionals would agree that the central tenet of Zero trust is to shift from 'trust but verify' to 'verify then trust'.

This is nifty phrasing but in practice it's a problematically finite statement; overly permissive in non-static environments while being simultaneously inflexible. 'Verify then trust' assumes that, once verified, you are good to go. And if not verified, permanent blocking is justified. The first option leaves a significant hole in an organization's defenses, and the latter will impinge upon business productivity.

Continuous adaptation of trust

What is actually needed in a cloud-first, perimeter-less environment, is something that is continuously adapted. The unequivocal verbiage of 'zero' is ill-suited in such a nuanced environment. Context is key and trust judgements require insight to effectively determine grades of permission.

SASE is a fairly new architectural model for securing a perimeter-less IT real-estate, and it has significant advantages when working on a Zero Trust approach because of the visibility and insights it allows. Zero Trust in a SASE environment is more accurately 'continuous adaptive trust' across users, devices, networks, applications and data. The wealth of contextual insight available within a SASE platform removes the requirement to place implicit trust or to base permission decisions on single pieces of information (an IP address for example). Decisions can be based upon a tailored set of constantly reas-

sessed parameters, built using several contextual elements intertwined (e.g. user identity + device identify + time + geolocation + business role + data type). And because with SASE the security policy follows the data, not the user or device, the resource itself is effectively determining the appropriate level of trust, only for a specific interaction, reassessed each time a parameter changes.

Evaluating trust at the start of an interaction alone is insufficient. This trust assessment can and should take place throughout an interaction. During the interaction, context should be continuously evaluated as alterations to the context can result in an adaptation (increase or decrease) in the level of trust that is appropriate, which in turn should alter the type of access granted to the resource.

Managing trust

Of course, it must be acknowledged that zero trust models necessarily add a degree of management overhead. Owners of resources must assume responsibility for carefully assessing and continuously adjusting not just the lists of allowed users for their resources, but also defining the attributes and contextual elements that together determine the level of access allowed to resources. Management of entitlements is often a manual process, but automation is starting to reach the market.

The balance of permission and restriction

The advantages of a continuous adaptive trust approach are manifold, but three stand out as compelling when preparing a business case.

More opportunities to provide some degree of access, to reorient the majority of security decisions away from “no” towards “yes, with conditions.” Inappropriate access is constrained, reducing the blast radius of compromised accounts Visibility into sensitive data types, locations, and movements in improved and constant.

While points two and three are clear risk reduction advantages, the first point is in many ways more crucial when selling the approach internally. Zero Trust appeals to security professionals from the moment you hear the name, specifically because it sounds unequivocally safe and secure. If you don’t trust anyone, you can’t get hurt, so the broken hearted will tell you. But however much security professionals might joke about how much easier our jobs would be without a user base of employees, we must acknowledge that giving access is as much a part of our job as restriction and blocks. Continuous adaptive trust walks that line, using insight to issue and retract dynamic permissions. With it, organizations can maximize business productivity without any unnecessary exposure.

SASE: Is your edge ready?

IT infrastructures are in the midst of dramatic changes, restructuring how applications and data are deployed and consumed. Organizations are beginning to realise that their physical network and security infrastructure must evolve to protect an increasingly perimeter-less environment. Cloud services, security and networking are converging, creating a new model where security and networking no longer comprise discrete applications and devices, but are delivered as software services alongside cloud -based applications.

Gartner has recently coined the term SASE (Secure Access Service Edge) to describe this emerging security and network framework. The analyst house points to seven areas in which security and network teams should review their architecture with a view to achieving the benefits of SASE. Let’s walk through these areas of consideration, explain the benefits that can be gained by

each, and help security and network teams evaluate their own progress to SASE

1) Shift operations from managing security boxes to delivering policy-based security services via a cloud-native, microservices-based environment

An architecture that relies on traditional network and security appliances that are merely ported to the cloud as software is not SASE ready. This common approach does not scale, suffers from interoperability issues, is unable to deliver new features quickly and delivers security services with much higher latency than is acceptable.

A cloud-native architecture can deliver seamless security services that best match risk reduction requirements. It also future-proofs investments in an architecture that rapidly adapts to the changing enterprise network and security market, building new products natively and delivering security services without hindering business productivity or impacting the end-user experience.

2) Converge cloud and web security technologies to simplify configuration and operations, and to reduce cost

SASE infrastructure helps organizations implement consistent security controls across SaaS, Web and IaaS services, minimising available attack surfaces and protecting the most sensitive data. SASE-ready infrastructure delivers Secure Web Gateway (SWG) capabilities alongside other cloud-delivered network and security services such as Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) and Advanced Threat Protection (ATP). This is necessary as enterprises move their applications to the cloud and can no longer rely on on-premise firewalls to protect their data (as these appliances are blind to modern cloud traffic like API calls and JSON). Organizations require a deeper set of security controls to enable more granular visibility into activities performed across SaaS, Web and IaaS services, and spanning both managed and unmanaged devices.

By unifying these capabilities within a single architecture, SASE enables organisations to identify and decode both web traffic and cloud-based applications, deriving detailed context such as personal and corporate instances of the same cloud app (e.g. Office 365, Gmail, Slack). Enterprises are able to obtain a big-picture view of the threat landscape, incorporating context obtained from the integrated security and network services within the SASE-ready platform. Netskope calls this consolidated cloud gateway the Next-Generation SWG (NG SWG) and it extends protection by identifying, managing and securing web traffic and cloud-based applications, detecting and mitigating cloud-based threats, and enforcing data loss protection capabilities—all with a unified policy enforcement engine.

3) Follow a data-centric model and implement context-aware controls to readily detect and prevent sensitive data movement

SASE enables data protection as an integrated part of the cloud security framework. Modern cloud DLP solutions provide full visibility and, in the best cases, context awareness of data movement across clouds as well as mitigation of loss and exfiltration. In order to scale and optimise DLP, policies must be data-centric, applying to and following the data regardless of the endpoint or cloud service.

DLP policy management becomes more simplified within a SASE framework as the same policies can be applied across all cloud applications and websites, ensuring the same set of DLP policies are applied to data-at-rest and data-in-motion. A SASE-ready framework should effectively identify and classify data, providing a granular understanding in support of policies based on context such as us-

er, device-type, file type, data identifiers and more.

4) Protect against cloud-enabled threats, and combine inspection capabilities for threat and data to make an efficient, single-pass inspection solution.

With the rapid rise in cloud-enabled threats such as phishing and drive-by attacks, legacy solutions offer limited visibility and pose a significant risk. What's needed is a cloud-native platform that scales to support real time (fast scanning) and deep scanning (sandboxing) threat protection across the cloud to effectively expose and mitigate any malware and threats.

An ATP solution based on a SASE model can significantly help reduce complexity and cost for SecOps and Incident Response (IR) teams, while enhancing threat mitigation efficacy and scale.

A SASE-based ATP solution can help centralise all security events collected across managed and unmanaged clouds, providing a single, consolidated view into all activities. To be effective, this solution must collect rich metadata from web and cloud traffic for further analysis and investigation.

5) Evolve remote access strategies, adopting a zero-trust approach.

For remote access, security teams have traditionally relied on complex and expensive VPN appliance implementations that do not scale and incur growing maintenance costs while being cumbersome to manage. With the traditional "open" network access of VPNs, sensitive data can easily be exfiltrated, while compromised accounts or insiders can move laterally within a network. SecOps teams require a modern secure access solution that easily scales while allowing remote users secure access to select private applications in public clouds and data centres, regardless of location.

A SASE provider can deliver a cloud security solution that enables application-level access to private applications based on Zero Trust principles. This includes the authentication of users, and device posture checking and classification, before connecting users to select private apps.

6) Use a robust, global edge network that is high-performance, high-capacity and capable of supporting 'cloud heavy' communications.

A vendor's global network architecture determines how long customer data travels to and from the closest Points of Presence (POPs) before it is processed, potentially increasing end-to-end latency. In the end, the underlying network infrastructure affects the scale and efficacy of security controls, with traditional networks being inadequate for a SASE model.

A SASE-ready provider will deploy its services through a global cloud edge network, delivering security services closest to the end-user, optimizing routing and availability, while enabling security functions like DLP and ATP inline. This allows processing to be done quickly with minimal latency and interruption to the end-user. Vendors that backhaul customer traffic to centralised data centres break the SASE model and are unable to deliver all the required network and security services demanded by enterprises.

SASE also allows for a seamless integration of SD-WAN functionality in a cloud-based architecture where SD-WAN functionality is built natively alongside security services, which helps to scale performance and delivery for remote office users. SASE-ready architectures enable SD-WAN edge solutions to be directly connected to the edge cloud network, avoiding the complexity of deploying physical SD-WAN hubs and reducing the cost and complexity of deploying multiple

network and security appliances across the entire enterprise network. This access model can also help simplify multiple overlays that drive up complexity for enterprise network management.

7) Integrate management and administration tools to reduce complexity and increase efficiencies.

Most large security companies provide a portfolio of hardware and software-based security products that have been assembled together through acquisitions. While some integration may exist, SecOps teams struggle with the increasingly complex design, configuration and management of their security infrastructure.

A SASE-ready solution should allow for fully unified management and administration. Beware of products that require separate configurations and dashboards as a way to connect multiple products into common workflows. Integration with third-party security tools is essential and a SASE-ready solution should offer REST APIs, plus threat intelligence sharing based on standards to extend its capabilities.

A SASE framework sees essential security services converge in a cloud-native model which makes use of global, high capacity, low latency edge networks for an optimised user experience. Organizations embracing SASE can expect a simplified environment based on the consolidation of multiple security technologies, as well as reduced costs and a much-improved user experience for both end users and administrators. Crucially, adopting a SASE architecture leaves organizations much better protected against emerging threat factors, and better equipped to navigate data protection requirements. Is your organization's network and security infrastructure SASE ready?

(From page 15)

to the connected user and device; it often improves many existing bottlenecks, including latency numbers which begin to reduce, and network traffic flows that become smoother. Through this key feature, SASE can bring the cloud closer to the user and their location.

A future for SASE

The benefits of SASE are manifold: the authentication infrastructure with Cloud based services, scalability and its potential to increase business performance whilst reducing costs, have been recognized by risk and security managers. SASE has become present in businesses, a feature of current technology strategies for companies across the globe, offering a more secure access solution for remote or office workers. SASE will certainly be part of security infrastructures and applications for a long time to come - more than likely housed under one roof with a trusted supplier.

(From Page 3)

and **SASE** (Secure Access Service Edge), the topics of this e-book. Technologies and frameworks do exist to make businesses and organizations safer in the wake of new security threats. However, without proper education and expertise, embracing them can at worst, lull the customer into a false sense of security.

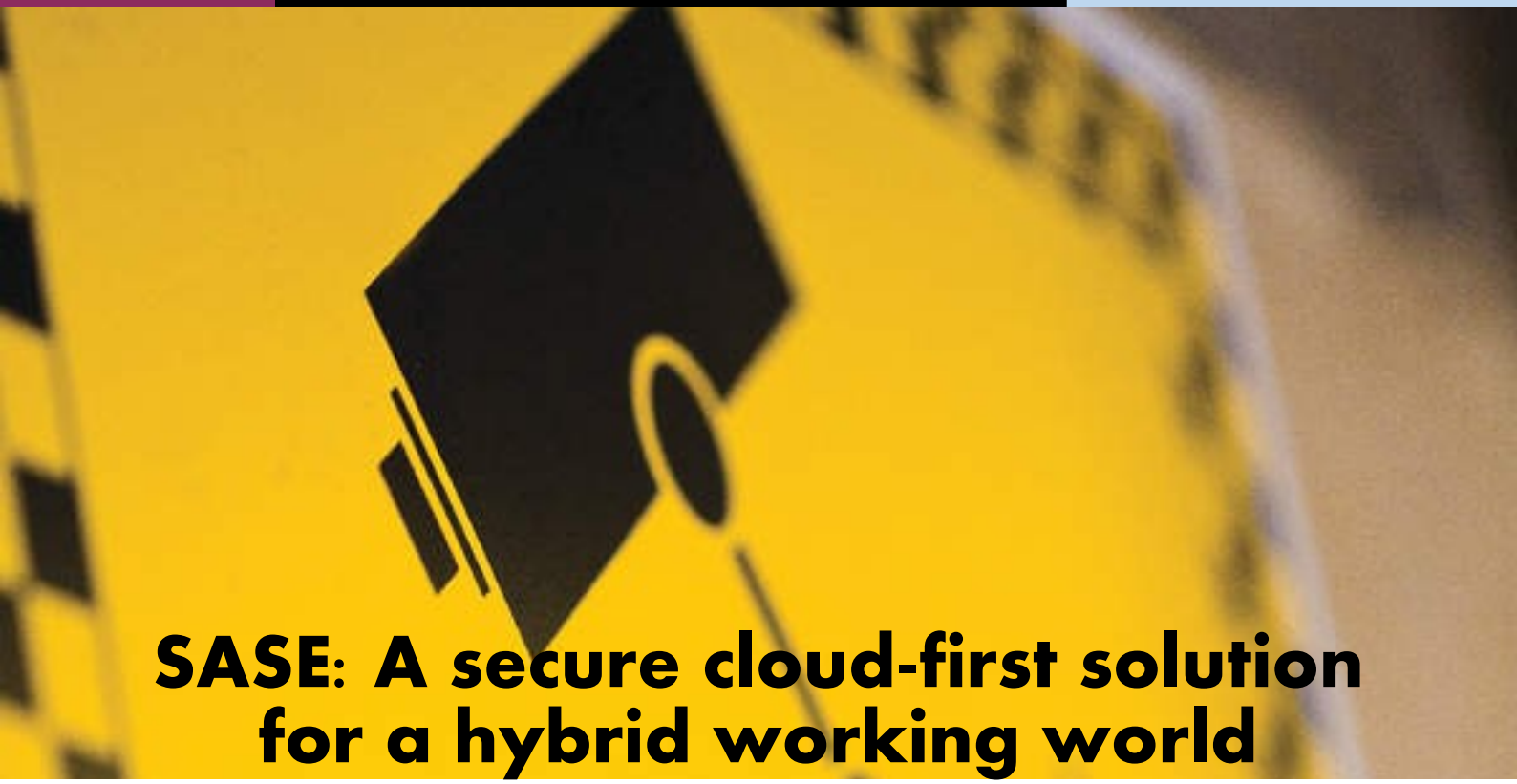
That's why we're here. TechRadar Pro is one of the biggest B2B technology publications in the world and the biggest in Europe. Where technology is likely to play a critical role as we experience an unprecedented level of upheaval. And no, it would be no kneejerk reaction to state that it has never been more critical for you to reassess your disaster recovery and security plans.

perimeter 81

The leader in Zero Trust Network Access technology

- Protect your network, applications and critical cloud resources
- A radically simple and unified network security platform
- Easily build, manage and monitor your hybrid network
- Activate industry-leading Zero Trust security

View the report



SASE: A secure cloud-first solution for a hybrid working world

By Michael East, Menlo Security

Almost 18 months on from the initial murmurings of a new emerging deadly virus, remote and hybrid working models need little by way of introduction.

The world has been swept off its feet and turned upside down by Covid-19 in the period that has ensued, leading many of us to a new normal of working from home. And this rearranged state of employment-related affairs is unlikely to change all that much moving forward.

A recent survey of the biggest UK employers showed they have no plans to return all staff to the office full-time in the foreseeable future. Another survey revealed that 19 percent of workers would like to work from home five days a week in 2022. Indeed, many superlatives have been used to describe the global embrace of more flexible, open working cultures.

Various studies have shown the numerous benefits to both employer and employee alike, relating to everything from boosted productivity, enhanced loyalty and fewer sick days to reduced costs, reduced stress and a better work-life balance.

A two-year study from Stanford University, for example, revealed remote employees to be 13 percent more productive than their in-office counterparts.

That said, it's not all a case of bright skies and red roses. Amidst the mass switch to hybrid and remote working that we have all undergone, there have been many hurdles hidden among the positives.

For Chief information security officers and those of a similar profession, it has been a period of immense challenge. Not only has the pandemic provided several opportunities to cybercriminals who continue to exacerbate an increasingly unfathomable threat environment, but the IT infrastructure that many companies' operations rely on has had to change significantly.

Previously, the vast majority of information security protocols had been built on perimeter-based network security – a concept that assumes all internal entities within a network are trusted, while external parties are not.

In a hybrid working world, however, these boundaries are shifting.

Where people now need access to workplace systems and software on a remote basis, be it from home or on the go, there is no longer a single, defensible line of separation between a company's internal assets and the outside world. In essence, the network perimeter is fading away.

Security and productivity – the remote working challenge

Let's rewind back to March 2020. Across the UK, US, and many other countries, companies were forced to adapt their internal systems and IT support almost overnight to continue operating effectively amidst enforced national lockdowns.

Naturally, companies were thrust into the unknown – how could such a drastic shift occur in such a short space of time?

At the time it was not understood if the pandemic would be short-lived or long-term. As a result, many explored the use of virtual private networks (VPNs) as a temporary bridge to maintain a centralized approach while supporting remote working.

Indeed, VPNs will connect employees in disparate locations to a central network, but they do so in a highly inefficient manner. Central networks had not been built to support remote operations, and VPNs will regularly suffer from bottlenecked traffic that can seriously hamper user productivity, as well as exposing a series of vulnerabilities that may compromise security.

So, how should those companies looking to maintain flexible, hybrid or remote working models proceed in order to maximize security and productivity?

Enter Secure Access Service Edge (SASE). A term coined by Gartner, it defines the simplification of networking and security, achieved by combining both elements within a cloud service that is provided to the source of a connection directly, not via an enterprise on -premises data center.

SASE is not a new technology in itself. Rather, it combines Software Defined Wide Area Networking (SD-WAN) capabilities with a variety of network security functions that are readily available on the market today, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS), and Zero Trust Network Access (ZTNA).

The result is a much tighter convergence and integration of network connectivity and security functions, capable of securing work from anywhere at any time, without hampering worker productivity.

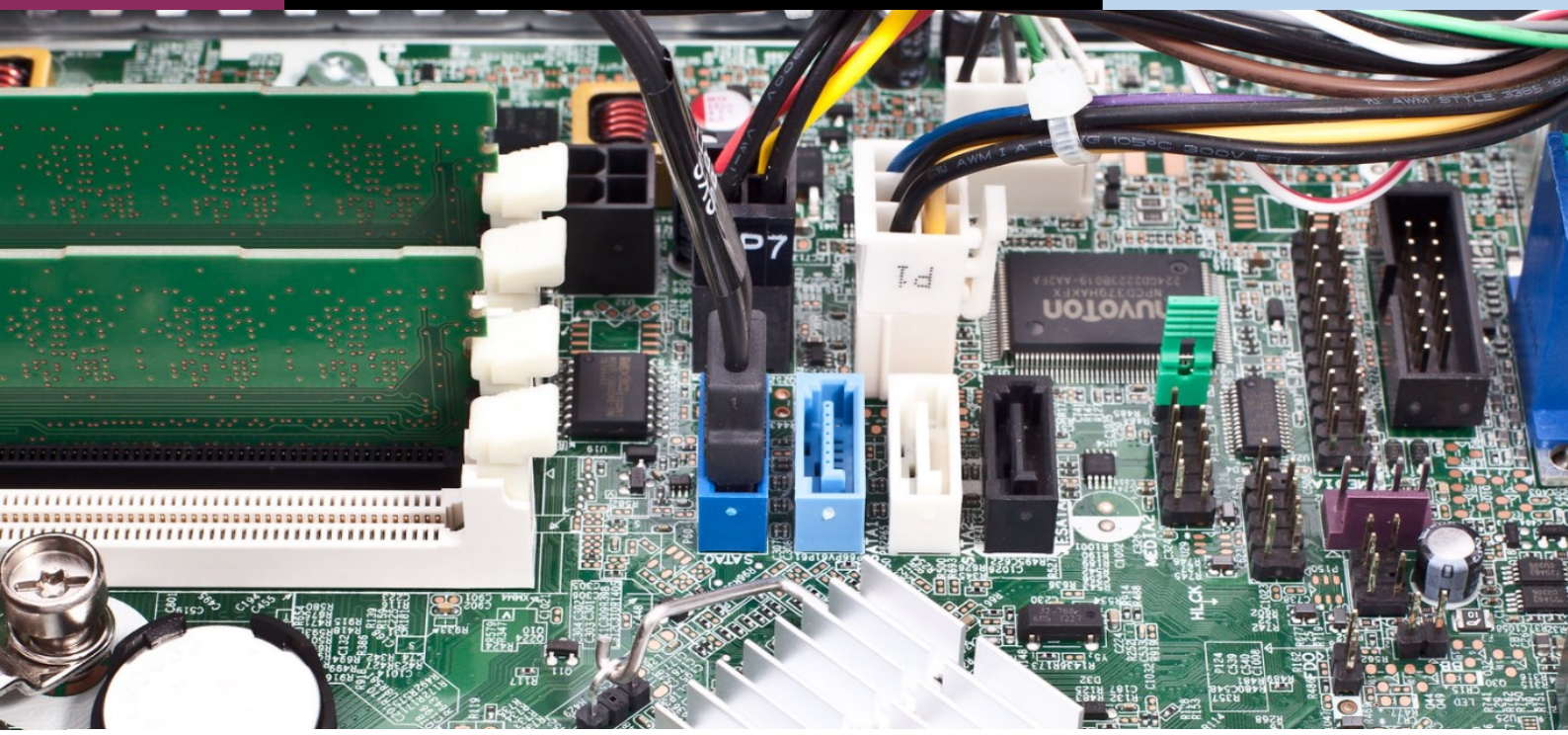
Unlike VPNs and other 'square-peg-round-hole' legacy solutions, SASE has been built on a cloud-first basis. And the various benefits are telling.

It can help organizations to better safeguard data by providing secure access while protecting against advanced threats; it allows employees to seamlessly use the applications they need; organizations can add users and see and monitor data in real-time from anywhere; it delivers consistent security policies to all devices, be it desktops, smartphones or tablets; and it can integrate all tools into a single architecture that is more easily manageable.

Now its time to consider SASE

Indeed, the digital landscape is now ahead of its time. According to a McKinsey & Company study, digital offerings have leapfrogged seven years of progress in a matter of months. And it seems that SASE has followed suit.

(Continue reading on page 31)



Demystifying what SASE really means

By Samir Desai, GTT Global Network

In today's world, many organizations are considering what shape the future of work should take for their operations. Some are embarking on or have already adopted a fully remote way of working, some may be opting for a hybrid working arrangement, and others may return to the office full-time.

Wherever your employees are working from, they will need the same level of access to tools, services and applications. Employees potentially accessing the network from a variety of locations means changes to the corporate network perimeter – and with that comes a new set of security considerations.

Having appropriate cybersecurity measures in place is becoming even more critical for IT teams, as the possible attack surface for an enterprise's network increases with remote working. Secure Access Service Edge (SASE) is an emerging concept that aims to better address the security needs of enterprise organizations needing flexible workforce arrangements.

SASE achieves this by deploying a range of security features into a single cloud-delivered platform. Network connectivity is also seamlessly integrated into the platform enabling the best possible application performance for end-users. As SASE is still relatively nascent, there are currently many different interpretations of what SASE means in the marketplace, making it potentially difficult for enterprises to decide what solution they really need.

The rise of SASE

Let's cast our minds back to the start of the pandemic where our main focus was adapting the IT platform to a remote work environment. This rapid pivot triggered the increased need for secure access to vital data resources, as protecting against corporate network vulnerabilities became a higher priority for IT leaders. Now, organizations are turning their attention towards the latest trend in strengthening secure network access, Secure Access Service Edge (SASE). But what does SASE really mean?

SASE was first coined by Gartner in 2019, defined as a cloud-based offering that combines the functions of SD-WAN with performance-enhancing and security features, such as cloud access security broker (CASB) and zero-trust network access (ZTNA).

Since the term first emerged, the market has been gradually expanding, but the final industry definition of what a SASE deployment should look like is still evolving. There are several approaches to deploying SASE, each with inherent benefits and challenges.

The theoretical ideal is the single source approach, with one technology provider delivering a full SASE solution. Unfortunately, this approach is hindered by the fact that most vendors in the market today cannot provide the full spectrum of the key SASE components, as most organizations that are deploying SASE find themselves needing to select several vendors.

To mitigate complexity, a two-vendor solution offers a fair compromise, with one provider focused on SD-WAN and network functionality and another on the various security features. Deployments featuring three or more vendors are also common, with multiple providers for the security components of the solution. However, some of the leading vendors are on a roadmap to delivering a complete solution, and. industry analysts predict that most organizations will look to consolidate vendors as the market continues to mature.

For many organizations, this has made SASE a new frontier to explore, with myriad features, functionality and limitations to understand and navigate in order to optimize their secure network management.

The state of SASE today

Despite the somewhat sprawling look of the nascent market landscape, SASE is poised to become the next big thing for enterprise network security, as it promises to reduce complexity and costs, improve network performance and latency, and enable businesses to adopt a zero-trust network access approach. But the problem is that because everyone in the industry has their own interpretation of what SASE means, it's difficult to define what a true SASE provider looks like.

Users gain access to the network based on their identity, device and application – rather than the IP address or physical location. The advantage of this is that it will support new ways of working as we come out of the pandemic and employers and employees choose between working in the office, from their homes, or at a nearby café.

Organizations must strike the right balance between user access management and effective, secure remote access to corporate resources. By working with a managed service partner, who can help define and implement policies aligned to a business's specific security requirements, enterprises are able to flexibly adapt their networks to the right security posture as hybrid work becomes the guiding convention.

We see the principal security perimeter shifting from a highly secure yet inflexible corporate LAN environment to being endpoint focused as part of a Zero Trust Network Access (ZTNA) approach under the SASE paradigm. This approach relies on the principle of risk-appropriate trust that is continuously assessed and adapted to comply with the objectives of an enterprise's security posture.

This approach is better suited to enable secure access to cloud applications used by employees working at the office, home or other environments. What enterprises need to be aware of, however, is that as this remains a new technology, providers are still refining their solutions. Today's path towards SASE should reflect this – enterprises shouldn't rush and jump at the latest technology trend but instead, take a step back and consider what their needs are.

SASE is the future

According to Gartner, by 2025, at least 60 percent of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch and edge access, up from 10 percent in 2020. As business leaders start thinking carefully about how they implement this technology in the best way possible, a few key questions can help guide the decision-making process.

Naturally, they should first ask themselves whether the considered solution helps to solve their business challenges. Furthermore, does the solution meet their needs for stable connectivity and user experience? Does the service align to its risk management strategy? Will it provide the level of security robustness that they expect and want?

Businesses will need to look at their network more holistically. Rather than assembling a myriad of networking and security solutions, they'll seek solutions that are more integrated and help reduce complexity while also improving their security posture. All of these new technologies and practices will better equip businesses to adapt to a more flexible distributed enterprise and workforce model that will continue to influence networking and security requirements for the foreseeable future.

Going forward, SASE networking will become popular as IT can manage their network and security seamlessly at the same time. If in doubt, always consider working with a trusted advisor that can demonstrate a keen understanding of the relevant technologies, and is able go through each stage of the network development and protection process to help an organization determine the security solution that is right for them.

(From page 27)

While Gartner and other thought leaders had previously predicted that it would take a full decade to reach organic adoption of SASE, this expected timeframe has now shortened to somewhere between three and five years, as a result of the shift towards hybrid and remote working models.

Of course, there are challenges relating to its implementation. Any cloud platform supporting SASE needs to be intelligent, dynamic and scalable in order to deliver secure access to resources without any dependency on a user's location, for example.

Yet those that are able to position themselves as early adopters will be well placed to reap security, productivity and user-experience-related rewards for years to come, transforming their organizations into more competitive prospects.

The signs are optimistic to this end. According to the latest CyberEdge Cyberthreat Report, 74 percent of IT security decision-makers are currently adopting technology capable of supporting SASE architecture, laying the foundations for such prosperity in the future.

Those that fail to actively integrate SASE into their IT infrastructure in the coming years, however, could risk being left behind in a continued struggle comprising limited security for users and hampered productivity.

Knowledge is power - getting to grips with SASE

By Michael Wood, Versa Networks

The implementation of new technology within a business can often take months to complete. It requires planning, budgeting and research- all of which takes time and effort from multiple teams within the company. Unfortunately, the last year deprived business leaders of the luxury of time, and making digital transformation decisions dramatically accelerated. According to our latest report, 84 percent of IT and security professionals experienced an increase in cloud adoption and other digital transformation projects.

This level of change within technology adoption timeframes can have several impacts on business operations, as many discovered last year. Without sufficient time to prepare, many companies experienced unreliable connectivity and limited real-time IT support. Video conferencing and collaboration apps were greatly affected by this dip in performance for 36 percent of our survey respondents.

Various different solutions were considered and adopted to try and help overcome the network and security issues, however it's come to our attention that not everyone who implements these solutions has a complete understanding of what they are.

Security has been a strong focus for business leaders in recent years as the threat landscape continues to evolve. Despite companies boosting security to the top of their priorities list, 49 percent would still like to see greater efforts made towards strengthening it. SASE has gained more popularity over the past year, with 87 percent of respondents having already adopted, or contemplated adopting SASE as a solution to their security needs within the next year. Breaking this down even further, we can see a growing interest in SASE as a solution, over VPNs. In fact, 34 percent of companies chose SASE compared to the 23 percent who chose VPNs.

Narrowing down the choices

A popular option for businesses looking to update their systems is Secure Access Service Edge (SASE), which addresses both the security and networking sides of a business. SASE is the integration of networking and security solutions, such as Zero Trust and firewall-as-a-service (FWaaS), into a single service that can be delivered entirely through the cloud. With the growing need for a solution that will support a partially or completely remote workforce, SASE's ability to deliver strong security and reliable con-

nectivity stood out for many businesses.

Confusion around SASE

Without a doubt, organizations are becoming more familiar with SASE and its benefits, hence the decision to choose SASE over VPNs. Remote working has revealed a number of security issues with VPNs so businesses are beginning to look elsewhere for their security and network solutions. Currently, a third of businesses have already implemented SASE, with another 30 percent looking to deploy in the next 6 to 12 months. But are organizations achieving the best return on investment (ROI) through their SASE solutions?

Due to the immense pressure placed on organizations to advance the business along the digital transformation journey, it's unsurprising that deployment speed became a number one priority. This means however, that some solutions have been implemented without the teams fully understanding how it can achieve the best results for the business. This is certainly the case with several SASE deployments, as revealed by our survey.

Out of all respondents, only 31 percent could identify the accurate definition of SASE: 'the convergence of networking and security services like CASB, FWaaS and Zero Trust into a single, cloud-native service model.' Without fully understanding the technology's capabilities, it is virtually impossible for companies to make use of its full potential. It's also interesting that out of all respondents who are not planning on implementing SASE, 13 percent admit to not completely understanding its benefits. This clearly demonstrates the parallel between companies not understanding and not deploying.

Other reasons for businesses not choosing SASE include a lack of budget and other priorities. Many companies will be satisfied with their current solutions so won't necessarily see the benefits of investing in new technology, especially ones they still have questions about. If there was greater awareness of this technology and its capabilities, perhaps the findings would differ.

Future-proofing the company

It's been established that security and reliable connectivity are the two main concerns for businesses moving forwards. With many organizations choosing to maintain a remote working practice in their business structure, they need to be able to ensure smooth transitions between the office and remote environments to maintain business productivity. With the threat landscape constantly evolving, it is unsurprising that 32 percent of businesses are concerned about being able to protect their network from the onslaught of security threats.

SASE is equipped to help combat these security and network challenges; the main barrier preventing deployment is lack of awareness. Its benefits range from strengthening network architecture, to delivering greater flexibility across the company through the cloud. The fact that it operates from a single point of control is ideal for teams because it allows for ease of use but can give insights into the entire business structure. It automatically entrenches security into every element of the network architecture giving teams the confidence that all parts of the business are covered.

Over a year since the pandemic first triggered the digital acceleration wave, businesses have now reclaimed the time they were previously deprived of. Taking the time and effort to research and understand the different solutions on offer, such as SASE, will be of great benefit to the entire company in the long run. Only when a business fully recognizes the capabilities of new technology, will they be able to make the informed decisions needed to future-proof their company and protect themselves against unknown threats.