RACONTEUR

Thinking outside the network security box

Forcepoint

Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organisations while driving digital transformation and growth.

Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

RACONTEUR

Publication sponsored by
Forcepoint

Contributors

Charles Orton-Jones
Tamlin Magee

Contents

Cyber 2.0: the new armoury protecting the enterprise

How SASE technologies are helping organisations navigate network security for a hybrid future

Charles Orton-Jones

"From this evening I must give the British people a very simple instruction. You must stay home." These words in March 2020 by the prime minister kicked off lockdown #1 in the UK and triggered a revolution in the way companies operate.

Overnight every company became distributed. Susan from marketing worked from her laptop in her bedroom. Keith from accounts logged into cloud services via a 4G dongle from his kitchen. Data flowed from phones to cloud systems, from PCs to on-prem centres. For IT teams the entire enterprise geography changed.

Meanwhile, another group of professionals was hard at work. Ransomware criminals were expanding their activities. In the same month, the Hammersmith Medical Centre got hit – the private details of thousands of patients would be leaked out of spite as the centre refused all ransom demands. It was one of hundreds in the UK alone.

Between 2019 and 2020, ransomware attacks rose by 62% worldwide, and by 158% in North America alone. The result? A total rethink in the way IT security works.

"The pandemic has accelerated the pace at which businesses have had to adopt new technology," says Andy Jane, chief technology officer at Onecom, a telecoms provider. He points out that the old approaches – firewalls, virtual private networks (VPNs), and wide area networks (WANs) – simply couldn't cut it. The post-covid enterprise needs a new set of security tools fit for the challenge.

65%

of global enterprises will employ unified communications solutions that are deployed over SD-WAN by 2023

Gartner 2020

The new arsenal

The old firewall is gone – we now have next-generation firewall. The concept of spotting bad actors is being replaced by zero trust, which ensures nothing is trusted by default and only authorised devices can connect, to be policed round the clock.

The acronym SASE, pronounced "sassy", standing for secure access service edge, unifies multiple security concepts of this new ecosystem under a single, unified umbrella. And at the centre sits the workhorse, allowing traffic to flow across the distributed network: the software-defined wide area network (SD-WAN).

"SD-WAN is the application of software-defined networking technologies to wide area, enterprise networks," says Steven O'Sullivan, head of cybersecurity practice at Enzen, a consultancy. "It is used to secure WAN connections between branch offices, remote workers and data centre facilities that are geographically dispersed."

SD-WAN means companies can ditch the costly and fragile multiprotocol label switching (MPLS). Instead, companies pay for ordinary internet service provider (ISP) services from different providers and use SD-WAN to blend them together. It can even bundle 3G, 4G, 5G and ethernet into the mix. The result is an uplift in speed and reliability.

"Effectively a network overlay, SD-WAN is carrier agnostic and transport layer independent," says O'Sullivan. "It promises reduced operational costs, greater control over network applications and simplified management. Additionally, with an SD-WAN, a business has the benefit of multiple layers of security to protect against internet and branch cyber threats."

The bundling of multiple transport methods, such as three ISP connections into a unified pipe, is particularly attractive to organisations where downtime is catastrophic. "This is seen in organisations such as the UK's National Grid NG IT RIIO-2 plan," says O'Sullivan. "It is investing in SD-WAN infrastructure to deliver network routing securely, and to take advantage of lower-cost public networks for WAN connectivity and provide direct internet access in support of cloud and SaaS services. This will also allow them to reduce the frequency of bandwidth upgrades to our internet gateways."

There's one more plus. SD-WANs offer network control via a simple and centralised interface. For the utility sector, along with banks, defence, and retail, this is very attractive. "An important reason for the popularity of SD-WAN in the utilities sector is that it enables significant improvements in cybersecurity while reducing costs," says O'Sullivan. "Management, granularity and control become much easier for the people managing the networks, especially the operational technology aspects. With the implementation of SD-WAN security, the teams and personnel responsible for the care and maintenance of process networks gain holistic visibility and granular control over connectivity into and out of the facility."

Naturally, there is considerable innovation in the field of SD-WANs. The concept is fluid, and different providers bring their own philosophies. SD-WAN has already evolved from a connectivity infrastructure to a services platform. The first evolution of the technology worked at the networking communications layer. You had to write your own traffic routing rules, as it didn't have the context to do so. The latest in SD-WAN technology works at the application layer, meaning it now has the context to learn itself without as much human input.

> **An important reason for the popularity of SD-WAN in the utilities sector is that it enables significant improvements in cybersecurity while reducing costs**

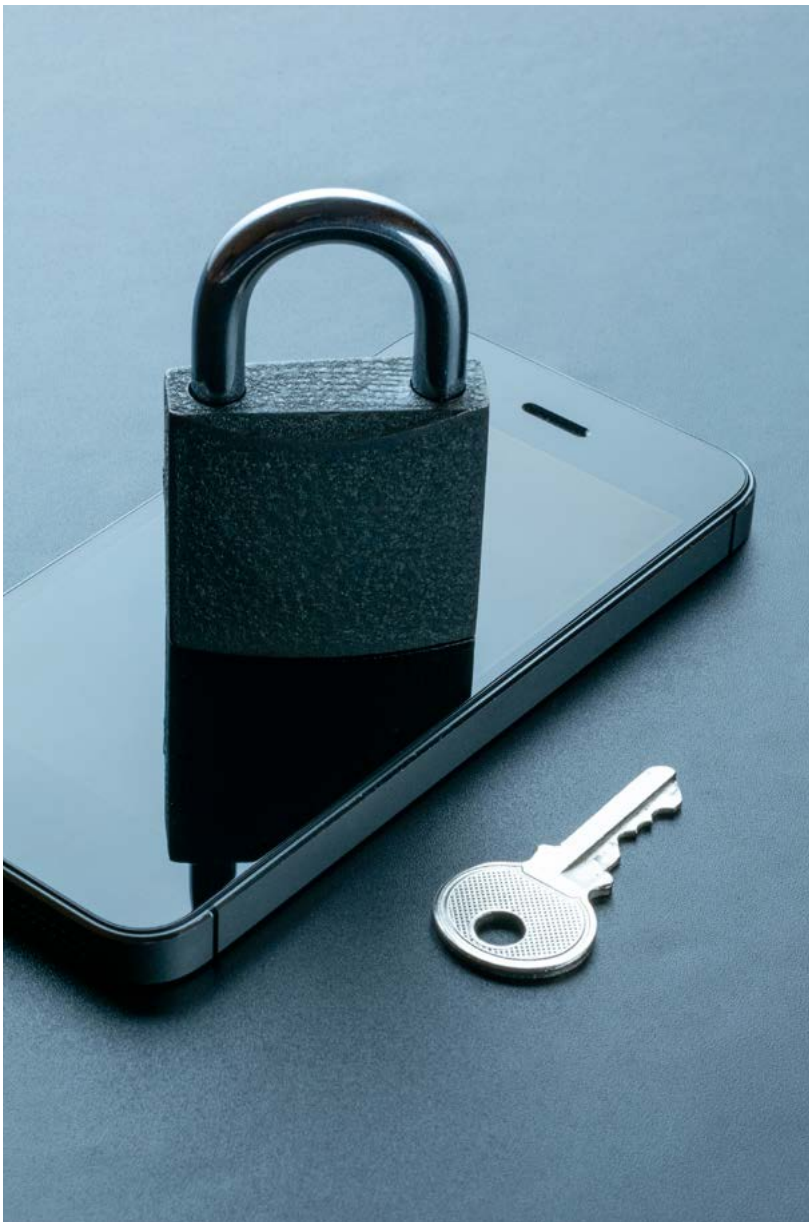
The result

The arrival of SASE technologies is a blessing for IT staff. The new systems are easier to run, quicker to install, and include the vast array of devices and cloud services used by a modern corporation.

The pandemic threw challenges at businesses. Now they are responding. In the long run, this new era of hybrid working may be more productive and more secure than ever before. For IT teams who want to give Susan and Keith guaranteed access to all services from wherever they are, safe from hackers and ransomware gangs, these are life-changing technologies.

Lessons from 2021's biggest ransomware attacks

In an increasingly complex digital world, ransomware threats are getting more sophisticated – and security professionals must be on their guard



Tamlin Magee

Security leaders often cite ransomware as the number one threat that keeps them up at night.

By September 2021 there were at least 500 million logged ransomware attacks, and these were only the ones that were discovered. The old maxim that organisations will suffer attacks 'when' rather than 'if' has certainly come to pass.

This year, attacks became more daring, sophisticated, and damaging, from taking health systems offline to crippling critical infrastructure. What were the biggest ransomware attacks of 2021, and what can security leaders learn from them?

Colonial Pipeline

Three million barrels of fuel are ferried between Texas and New York by the 5,500-mile-long Colonial Pipeline every day, the largest refined oil system in America. So when, in early May, a major ransomware attack shut down operations for five days, America's East Coast was starved of fuel.

The infamous SolarWinds attack of 2020 touched on industrial control systems, but the Colonial Pipeline incident eclipsed it with regards to damage to critical infrastructure, leading president Joe Biden to declare a state of emergency.

Attackers were believed to have gained access through a compromised virtual private network password. According to investigators, the account was no longer in use, but the password was an open door into the network, exemplifying the devastation possible with less than watertight account management – and the necessity of zero trust policies everywhere.

Joseph Blunt, CEO of Colonial Pipeline Co, ultimately authorised a $4.4m payment, seeking to bring the pipeline back to life as quickly as possible, telling the Wall Street

Journal he thought it was the "right thing to do for the country".

Unfortunately, while the attackers provided a decryption tool following the payment, it wasn't enough to bring systems back online: a stark reminder there's no guarantee businesses can revive operations when they pay ransoms. However, $2.3m of the payment was later recovered – and by 14 May, the cybercrime group responsible, Darkside, told the New York Times it was shutting down, citing unspecified "pressures" from the United States.

Kaseya

Any managed service provider's (MSP's) worst nightmare came true when MSP Kaseya found up to 1,500 of its customers were hit by a ransomware attack, proving how catastrophic supply chain attacks can be. Over 1 million systems were shuttered overnight – forcing a leading Swedish supermarket chain to close 800 of its shops.

The 'REvil' gang, a notorious group that offers ransomware 'as-a-service' to its customers, was responsible, and demanded an enormous $70m payout to restore normality.

The source of the attack, a vulnerability in a virtual system administrator (VSA) remote monitoring package developed by Kaseya, was identified early on. Although Kaseya responded promptly, alerting customers on 2 July and issuing a security warning about VSA services, the damage had been done.

Biden again intervened – this time speaking with Russian president, Vladimir Putin, who is suspected to tolerate the existence of cybercrime groups within Russia. In the days following, a universal decryptor was given to Kaseya by a "trusted third party", helping victims to restore their files.

Indictments against two hackers suspected to be associated with REvil were unsealed in November 2021 by the US Department of Justice. The pair face a combined 260 years in prison if convicted on all charges.

It's noteworthy that this supply chain attack was enabled by vulnerabilities in remote monitoring software, and underscores the need for vigilance, especially with distributed systems.

Meanwhile, the mammoth victim count suggests hackers will continue to pursue supply chain attacks against managed service providers, according to Chris Krebs of the US's anti-cybercrime group CISA, who warned they're a "much more economical" approach for launching breakout attacks, and are difficult for end customers to defend against.

68.5%

of businesses globally were affected by ransomware attacks in 2021

CyberEdge 2021

Irish Health Service Executive

When the infamous WannaCry malware slithered throughout the world's networks in 2017, healthcare organisations were among the most affected. Severe though the impact was, it paled in comparison to that faced by the Irish Health Service Executive in 2021 – which was forced to take all of its systems offline after suffering the largest ever attack against any health service systems.

The HSE became aware of the attack, which targeted data in the organisation's central servers, on 14 May 2021. As a precaution and while it assessed the situation, it shut down all of its systems. Although the attack vector remains unconfirmed, it was suspected to be launched with the TrickBot, IcedID, or BazarLoader malware – usually associated with phishing.

Major disruption followed, including the cancellation of critical procedures for patients like urgent radiation treatment.

The HSE refused to pay the $20m ransom. While the organisation escaped funding cybercriminals, immediate costs reached €100m – and CEO Paul Reid said these could climb to over €500m.

Russia-based cybercrime group Wizard Spider claimed responsibility and said it had gained access to the HSE systems for two weeks before the attack, underscoring the importance of stringent network monitoring and regular patching.

Additionally, the attack made clear that no target is off the table for cybercriminals – with this incident sparking serious consequences for regular citizens, many of them at their most vulnerable.

> **By September 2021 there were at least 500 million logged ransomware attacks, and these were only the ones that were discovered**

COMMERCIAL FEATURE

An SD-WAN masterclass

What exactly are the benefits? And how does an SD-WAN work alongside a next-generation firewall? Forcepoint CTO Petko Stoyanov offers an expert guide

Charles Orton-Jones

"Not many people understand SD-WAN (software-defined wide area network)," says Petko Stoyanov, chief technical officer of Forcepoint, the company that pioneered the technology. "When workers open a document or send a file to their colleague, they don't stop to think about how it all happens."

The same is true of IT teams. SD-WAN is a powerful tool, but often misunderstood. So, to clear up the pros and cons of a software-defined wide area network, Petko, alongside his Helsinki-based colleague Olli-Pekka Niemi, CTO of network security at Forcepoint, is here to offer a masterclass.

Let's start with the basic concept, says Stoyanov: "It's mesh internet access. Traditionally companies use an MPLS (multiprotocol label switching) to connect a location, but if that goes down, all connectivity is gone. SD-WAN offers resilience against failure. A location can connect via multiple ISP (internet service provider) connections, instead of a single MPLS. The SD-WAN bundles these multiple connections together, so if one fails there's no problem. Connectivity remains. So resilience is the major reason for adopting SD-WAN."

The way data is routed improves. Stoyanov explains that under the MPLS model data is often routed via a central point such as corporate HQ. This throttles bandwidth, increases latency, and leads to a frustrating user experience. And if the central location goes offline, an entire organisation can be brought down. "We see retailers with hundreds of locations making this mistake," he says. "The data is routed via a central office, which is inefficient. By switching to SD-WAN the traffic is routed without this bottleneck. So the speed is improved, and if a single ISP or location goes offline, nothing else is affected."

Cost is a major reason for the rise of the SD-WAN. An ISP connection is usually half the price of one MPLS. Even three ISP connections to a location can be cheaper than the MPLS they replace, which gives enterprises bargaining power: "We have clients who connect locations with three ISPs meshed with SD-WAN," says Stoyanov. "Each year they look at which is the most expensive and switch it for a better deal. It keeps costs very low."

Forcepoint Secure SD-WAN offers intelligent routing. This means connections are assessed by the technology and balanced to deliver maximum performance. Stoyanov says: "Forcepoint Secure SD-WAN is application sensitive. It can select different ISPs or net-links depending on the traffic quality or

requirements. So, if we know one ISP is very good for very large files and another is best for real-time response, then application data is routed via the best link for each task. Video takes one path, backup files another."

This capability may sound arduous to manage. In fact, a benefit of Secure SD-WAN is its simplicity. Rules can be set centrally, and the set-up is surprisingly straightforward to manage. "SD-WAN simplifies administration," says Olli-Pekka Niemi. "Policies are centrally managed via an easy-to-use console. It's possible for admins to manage the entire network with a single vantage point. Connections can be created or terminated on demand. It's extremely attractive for companies with complex geographical spreads and a variety of cloud environments and devices."

A major question asked of SD-WAN is how it fits in with a next-generation firewall. "SD-WAN is not a firewall," says Stoyanov. "A next-generation firewall incorporates a lot of the technology offered by SD-WAN, such as dynamic routing and VPN. But a next-generation firewall brings in security capabilities, such as intrusion detection and intrusion prevention."

The key is to dovetail the components together. Major vendors ought to offer a suite designed to create complete security and connectivity: "Our firewall is a fully functional Secure SD-WAN product. It integrates with the entire Forcepoint portfolio, including cloud web security, CASB, and advanced malware detection known as AMD. The components work seamlessly together."

All these reasons explain why SD-WAN is booming in popularity. So, who is it right for? "Any companies working across multiple sites should seriously consider making the shift to SD-WAN," says Stoyanov. "This can even include small companies that can't risk a location going offline. The improved resilience and lower cost offered by the technology means there are huge gains, even for companies in non-technical sectors. Retail, for example, is a major adopter."

In banking and defence, where security and up-time are at a premium, SD-WAN is now the default. Other sectors, such as education, are catching up fast, due to data security demands.

Niemi offers this final note of advice: "Every enterprise requires fault tolerant connectivity, with a lower total cost of ownership. That's what you get with SD-WAN. Combine it with a next-generation firewall, with security, and you are adopting the best networking approach available today."

> **When workers open a document or send a file to their colleague, they don't stop to think about how it all happens**

How Next-Gen Firewall and Secure SD-WAN helped Big Star secure its retail chain

Poland's largest clothing chain prides itself on great customer experience. In order to provide that experience, it requires strong network connections from the core data centre out to its 200 retail stores to support multi-region distribution of pricing, music and point-of-sale data.

For Big Star, the end of costly MPLS leases coupled with Covid-19 was the catalyst for change. During the pandemic, pressure built to ensure a high return on all OpEx and CapEx. The existing network architecture lacked central management of the WAN (wide area network) and LAN (local area network) together and visibility of user behaviour. On the recommendation of trusted solution provider Monolit IT, Big Star opted to switch to Secure SD-WAN with Forcepoint, integrating cost-effective local ISP links with Forcepoint Next-Gen Firewall security to centrally manage and secure multiple sites.

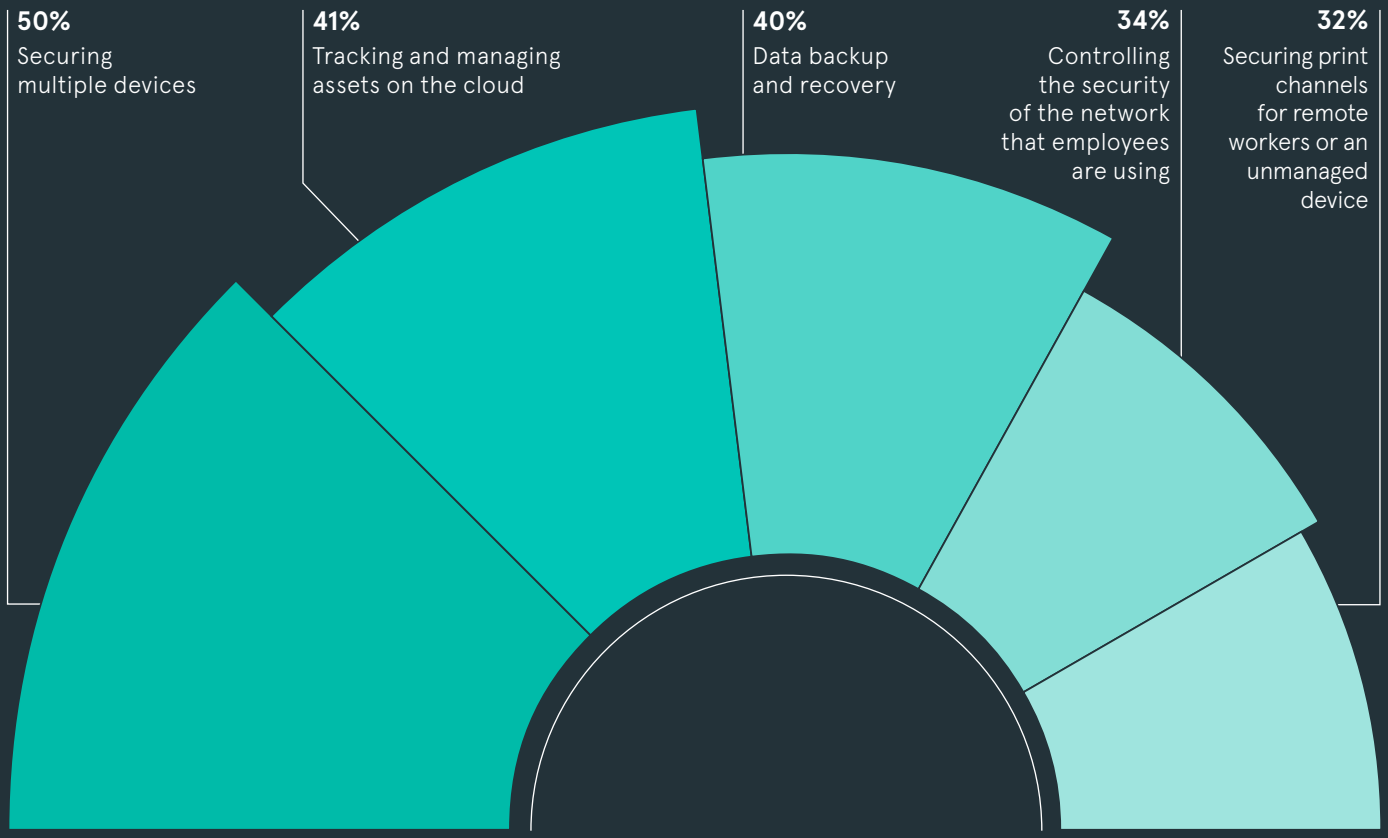
With Forcepoint's strong network security offerings efficiently connecting and protecting the clothing empire, Big Star now has a security strategy that aligns with its business strategy of providing excellent service. "The Forcepoint portfolio offers several notable user-centric solutions and services that can greatly improve the security of Big Star," says Filip Janczar, manager of IT security, Big Star. "We've already been working with Monolit for more than ten years and we see a bright future with them and with Forcepoint as our core team of trusted security advisors."

Clouded vision and hybrid headaches? Choose zero trust

A DISPERSED WORKFORCE HAS MADE CYBERSECURITY MORE CHALLENGING

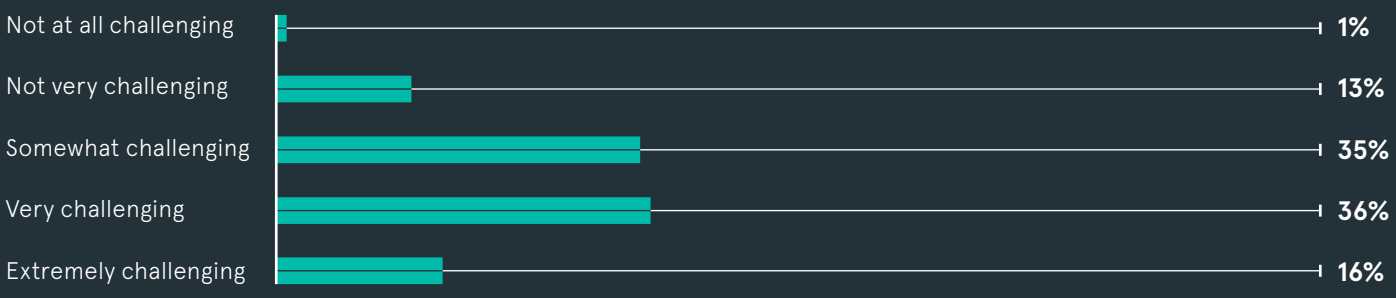
IDG and Forcepoint 2020

Top challenges remote workers pose to security



MOST ORGANISATIONS FIND SECURING CLOUD APPLICATIONS PARTICULARLY CHALLENGING

Challenge of securing applications, data, and infrastructure in the cloud



IDG and Forcepoint 2020

A ZERO TRUST APPROACH FORMS A VITAL PART OF MANY ORGANISATIONS' CLOUD SECURITY STRATEGY

Thales Group 2021

32%

of global respondents said that zero trust security has a great impact in shaping cloud security strategy

40%

of global respondents said that they rely on some concepts of zero trust to shape their cloud security strategy

24%

of global respondents said that zero trust did not affect their cloud security strategy

IN THE NEW WORLD OF WORK, A ZERO TRUST APPROACH HAS A LOT TO OFFER

Thales Group 2021

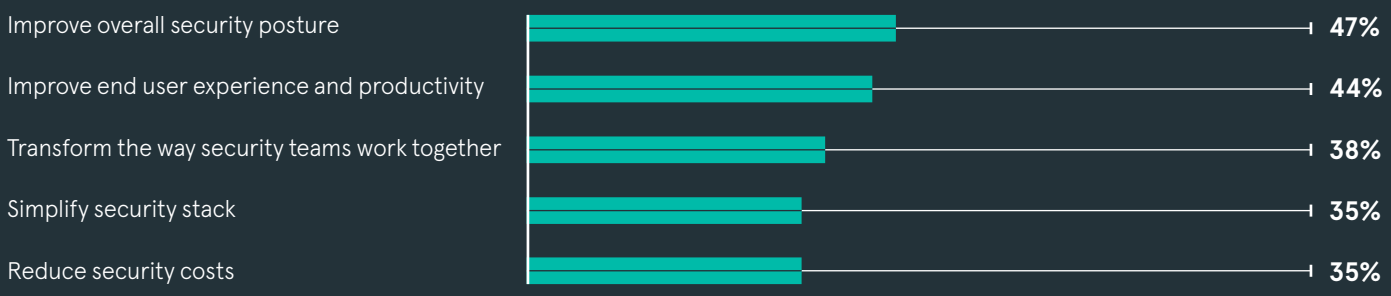
72%

of organisations accelerated their adoption of a zero trust strategy due to Covid-19

96%

of organisations say that zero trust is very or somewhat critical to their security strategy over the next two years

Top motivators for a zero trust approach



Microsoft 2021

Applying zero trust principles to everyone, everywhere

Zero trust is now an essential strategy for securing the 21st-century organisation

Tamlin Magee

'Zero trust' – it's a phrase that would be devastating to any interpersonal relationship. But in the world of cybersecurity, trust is not particularly advisable, not when attackers are using increasingly sophisticated methods to access networks, spoof accounts, and spread every security leader's worst nightmare: ransomware.

Simply put, zero trust is a security model that takes for granted that threats are omnipresent inside and outside networks, explains Scott J Shackelford, cybersecurity program chair, IU-Bloomington, Indiana University. Instead, it relies on continuous verification via information from multiple sources, and assumes the inevitability of data breaches – with a view to ensuring damage is limited, systems are resilient, and recovery is quick. This puts it at odds with the traditional 'castle and moat' model of perimeter security that relies on protecting a central location and the data in it.

The phrase was first coined back in 1994 by associate professor at the University of Ontario's Institute of Technology, Stephen Marsh, and repopularised in 2013 by analyst John Kindervag when he was at Forrester.

But it wasn't until recently that the phrase really gained momentum, following a paper from the USA's National Institute of Standards and Technology, Zero Trust Architecture, that outlined its six essential principles: a single strong source of user identity; user authentication; machine authentication; additional context (like device health); authorisation policies in order to access applications; and finally access control policies in the application itself.

During the boom in distributed working during the pandemic, zero trust could hardly be more relevant. Case in point: a report from Cybersecurity Insiders found that 57% of organisations believe insider incidents increased over the previous year.

In fact, one of 2021's most devastating ransomware attacks was the result of compromised remote credentials, with details stolen from a former Colonial Pipeline employee's VPN (virtual private network) account granting access to the network and ultimately starving America's east coast of fuel.

"Identity is definitely the new perimeter, and to use identity effectively you need as much context as possible," says FTSE 100 CISO and cofounder of Savanti, Richard Brinson. "It's not just 'is this person who they say they are?', it's about where they are, what device they're using, what time of day it is, and whether the actions they're taking are unusual. It's difficult to get right, but improving identity and access management should be at the top of the priority list for all security teams."

With the reality of distributed work only set to gain pace, a new approach to security is necessary: one that carefully monitors all elements of a network inside and out, and intersects with the technologies necessary to remain competitive in a modern organisation in an agile, cloud-first world.

57%

of organisations feel insider incidents have become more frequent over the past 12 months

Cybersecurity Insiders 2021

40%

of enterprises will have strategies to adopt SASE by 2024

Gartner 2020

> **Identity is definitely the new perimeter, and to use identity effectively you need as much context as possible**

However, organisations should be wary of treating zero trust as a kind of panacea: there's been a huge amount of hype around the term, adds Brinson, despite the fundamentals being sound.

"Personally, I think the term can be misleading and unforgiving in a corporate environment," Brinson explains. "You have to trust something – authentication systems, for a start, otherwise nobody is getting access to anything. And the term doesn't sit well with executives who are trying to empower employees and allow them greater autonomy and flexibility in ways of working. I prefer the term adaptive trust, where you can raise and lower the bar for authentication based on the context of what is being requested, which is what you actually implement in a real-world scenario."

To get to the root of the issue, security leaders should remember that zero trust is more of a philosophy than a technical solution, then they can implement technologies to match the approach.

"Deploy security controls that can challenge harder when the risk is higher," Brinson suggests. "You need solutions that provide you with high confidence in the identity of users and devices, an understanding of the context of individual requests for access or data, and central to making everything work is a policy that orchestrates when to allow, when to deny, and when to request additional verification."

This is where networking technologies like secure access service edge (SASE) fit in – a bundling of network and security controls that's based on digital identity, enabling access on a case by case basis. Gartner predicts 40% of companies will adopt SASE by 2024; a neatly packaged collection of services that can verify end users and devices according to aspects like location, device, IP address and network.

Meanwhile, migrating an organisation's information systems from in-house to cloud services can boost zero trust, but only if it's done right, says Shackelford: "This calls for creating new applications in the cloud rather than simply moving existing applications into the cloud.

"But organisations have to know to plan for zero trust security when moving to the cloud."

RACONTEUR

Forcepoint