How-to guide

The secrets of a successful SASE migration

Contents

How to navigate the complexities of integrating into a SASE environment

More and more businesses are turning to Secure Access Service Edge (SASE) to help them boost their network security while streamlining their operations. But transitioning and integrating into a SASE environment can be a complex process. What are the potential pitfalls, and how can businesses overcome them? Verizon experts offer their top tips.

Network security needs to work harder and smarter than ever before. Cyberthreats continue to increase. Attackers are growing ever more sophisticated. At the same time, with many businesses now heavily reliant on multi-cloud environments to access their applications and data, the resultant expanding attack surface area also contributes to the challenge. Despite many employees being office-based for part of the working week, continuing to operate flexible working exacerbates this further.

> All this increases pressure on the security of an organisation's network. It's no surprise, then, that more businesses are adopting SASE.

SASE, by definition, is Software Defined Wide Area Network (SD WAN) combined with Secure Service Edge (SSE) technologies. It provides a fully integrated wide-area network across any connectivity mechanism (e.g., cellular, public internet or private network) combined with an end-to-end security stack. By integrating network and security into a single framework, SASE enables organisations to benefit from simplified policy management and increased security. Additionally, SASE can fortify access management with a Zero Trust approach, so that only authorised users and devices can connect to the network. It also supports modern, distributed cloud environments by eliminating the hardware and configuration management limitations that come with traditional network security models.

With SASE, companies can streamline their operations by moving to a more holistic approach. They can enhance their protection from cyber-threats and provide secure, anywhere access for a hybrid workforce. However, transitioning to SASE doesn't come without its hurdles. It can be a complex process, involving many challenges – from managing a complicated integration across multiple technologies to the need to create new business processes.

The challenges of adopting SASE

1 Migrating from legacy environments and technology

One thing Verizon often hears from customers is that two of the key drivers dictating when they embark upon a transition to SASE are their existing vendor contracts and technology lifecycles. As IT organisations start to consider the replacement of IT infrastructure following its depreciation cycle, it becomes evident the impact a major technology upgrade will have on business processes and ultimately users as we are all now so much more dependent on technology to do our jobs. Therefore it is essential that a migration or upgrade programme is planned carefully to minimise disruption to the business and its users.

Jeff Paterson is one of Verizon's UK-based Solution Architects who supports large, global enterprises. He says, "It's not simply a case of replacing the legacy architecture with a shiny new SD WAN or SASE environment. There is always an integration challenge. Selecting an SD WAN technology, coupled with the SSE component, which has proven technical capability to integrate with these legacy hybrid environments – as well as natively with CSP/cloud environments – is key to enabling the transition and transformation to a holistic SASE solution."

2 Vendor choice and alignment from network and security teams

Many organisations also face the challenge of bringing network and security teams together to work in a consolidated way for the first time. Network and security technologies historically had best-of-breed vendors who were experts in their specific area. Only a few could attest to being experts in both. While everyone agrees conceptually that SASE is the right solution, getting network and security teams to agree on which vendor(s) to move forward with has been a challenge for some. Getting everyone aligned on which vendors to choose often requires additional time for thorough analysis and discussion.

> “
>
> It's not simply a case of replacing the legacy architecture with a shiny new SD WAN or SASE environment. There is always an integration challenge.
>
> **Jeff Paterson**
> Solution Architect, Verizon Business

3 Where to begin: integrating multiple technologies

Bringing together technologies from different vendors and making them work seamlessly together can be complicated, as they may not have been designed to interoperate seamlessly like a single vendor solution would. This includes provisioning and integrating cloud security into the SD WAN solution as well as configuring the SaaS policy. If a single-pane-of-glass (SPoG) dashboard is required, it can be incredibly complex to achieve when needing to combine insights from different technology vendors.

Businesses also need to cater to the fundamentally different requirements of their network and security teams. For example, security teams often need full access to security policy configuration so they can respond to events and threats in real time. In contrast, network teams may only need limited access to SD WAN policy configuration so they can work with self-service autonomy while not inadvertently introducing catastrophic changes.

So, how can businesses navigate these challenges and ensure a successful SASE implementation that meets their business objectives?

Plan for success

It's essential to plan your integration carefully, making sure you know what's involved at every stage and who's responsible for each element. Build out a clearly signposted roadmap to achieve your perfect end state and make sure everyone's aligned. "Define your objectives clearly," says Jeff Paterson, "or seek help from and work with your chosen partner to agree upon the overall goals and, importantly, have this documented for agreement and signoff by all stakeholders."

“

> Define your objectives clearly or seek help from and work with your chosen partner to agree upon the overall goals and, importantly, have this documented for agreement and signoff by all stakeholders.
>
> **Jeff Paterson**
> Solution Architect, Verizon Business

Involve the right people — at the right time

Integrating SASE is a complex process with many moving parts and lots of people involved. It's essential to make sure all the required stakeholders are briefed on the project and fully invested in a successful outcome. Without ensuring everyone is on the same page, this could cause a "lack of alignment between network and security teams, which can result in a fragmented approach when selecting vendors, and can lead to developing architectures and designs in silo, for the SD WAN and SSE components," suggests Fyllon Papadopoulos, Associate Fellow, who is the technical lead for SASE in the Tier 2 Design Authority team in Verizon Business.

If the integration of these components is carried out as an afterthought, it could introduce challenges for the resulting SASE solution. "Depending on the vendor choices made, the provisioning of SSE tunnels on the SD WAN endpoints might not support automation, resulting in significant configuration overhead," says Fyllon Papadopoulos. "Or the tunnels might not automatically failover, because of a lack of tunnel health checks or APIs between SD WAN and SSE components, requiring manual intervention. Or it might be that the security inspection which we want to implement for a certain class of applications requires an SD WAN policy which is complex to configure."

To avoid this pitfall, it's important for network and security teams to work closely together from the earliest stages of the project to:

- Align on vendor selection and interoperability
- Ensure the overall architecture and design deliver on intent
- Leverage economies of integration and consolidation
- Make sure the technology supports specific use cases

Agree on the scale of the project

Depending on your specific business needs, budget and current setup, you need to decide what kind of implementation is right for you. It's important to establish this at the start to avoid running into overspending or implementing something that doesn't meet your needs. As Jeff Paterson says, "Do you focus on the crown-jewel applications which enables your organisation to function, or do you extend this further into all applications across your company – a task which could easily run into hundreds or thousands of applications – with the associated increase in time, effort and expenditure?" Building the right plan at the outset will lead to a more effective, streamlined implementation.

> "
>
> Do you focus on the crown-jewel applications which enables your organisation to function, or do you extend this further into all applications across your company?
>
> **Jeff Paterson**
> Solution Architect, Verizon Business

Consider a phased approach

There's no one-size-fits-all method for implementation, so businesses need to structure their adoption around their specific needs. However, for a large enterprise, migrating networks and security all at once is generally considered too labour intensive and risky to business continuity. "Where customers have a large footprint and lots of legacy applications, we tend to adopt a phased approach," says Mike Hannan, Security Solutions Architect, Verizon. "We focus on limiting the scope to critical applications, where we carry out proof of concepts, smaller pilots, the move to larger pilots, and then full production rollouts."

"

> Where customers have a large footprint and lots of legacy applications, we tend to adopt a phased approach.
>
> **Mike Hannan**
> Security Solutions Architect, Verizon Business

Be realistic about timeframes

Just like there's no one single approach to adoption, there's also no guaranteed length of time it will take. "If you are looking to migrate the network and the security, that's a big shift to tackle all at once," says Mike Hannan. "You might not only need a professional, experienced partner, but also a lot of internal resources too." As such, it's important to be realistic about the scale of the project, what you need to achieve, and what you can get done in the time you have. "Phasing an approach can help to make this more achievable," continues Mike. "Perhaps tackling remote access first, then moving to site communication, thus gaining visibility to be able to make Zero Trust decisions."

> "
>
> If you are looking to migrate the network and the security, that's a big shift to tackle all at once.
>
> **Mike Hannan**
> Security Solutions Architect, Verizon Business

Find the right partner

Integrating SASE can be very complex, so you may need to work with a partner who knows how to achieve the desired results. “Select and work collaboratively with a provider who has the experience and proven capability of designing, implementing and operating complex, secure networks across whichever geographies you reside in,” says Jeff Paterson.

With such a significant IT transformation, you may need guidance and support from a partner who has experience with network and security infrastructure transformations in other large enterprises and who can work with you to establish what you need from your SASE environment, then roll it out and help you support it going forward. “It is essential to partner with a provider with a track record of delivering secure connected networks to underpin your business,” says Jeff Paterson, “so you can have the confidence that both the initial implementation and integration with any existing environment will be handled smoothly, and the knowledge that the ongoing administration and management of the service is well understood by operational teams.”

“

> It is essential to partner with a provider with a track record of delivering secure connected networks to underpin your business.
>
> **Jeff Paterson**
> Security Solutions Architect, Verizon Business

Talk to us

Wherever you are in your transition to SASE, Verizon can help. We have over 20 years' experience in network design, managed takeover of existing IT estates, transformation and management of secure networks. Our highly experienced teams carry numerous vendor and industry certifications. As such, they excel at pairing business needs with the right, best-of-breed technology. And we continue to invest in our NOC and SOC functions to provide digitally native, automated co- and fully managed secure network solutions.

Find out how Verizon can help you plan and manage a successful SASE integration at Verizon.com/business/en-gb.
Sign up for emails to learn more about our security and SASE solutions here.

Resources

SASE Management

Streamline security across your organisation. SASE Management merges network and cloud security, helping you connect people, data and devices at the edge, office and cloud.

Learn more >

Partners

By collaborating with the best in-class providers across the ecosystem to provide seamless, superior solutions, we help organisations improve performance and realise value faster.

Learn more >

Digital Enablement Platform

Integrate your APIs with Verizon to streamline your inventory, incident and change management through our Digital Enablement Platform.

Watch video >

verizon
business