Guide

SASE: **A competitive edge**

How a Secure Access Service Edge model can boost security and speed in a fast-moving world.



Key takeaways

- Secure Access Service Edge (SASE) helps ensure security by embedding zero trust principles into all aspects of hybrid operations. It also boosts resilience against shocks like natural disasters and cable cuts.
- By safely allowing work and processing to happen at the edge of the network, latency is reduced and emerging tools can perform at their peak.
- SASE gives businesses the flexibility to expand into new markets, deploy policies appropriately and integrate new systems and users quickly.
- It provides a flexible architecture and security controls in which AI tools can be utilized with less risk.

Context:

Work today can happen from anywhere, making it vital for businesses to secure all connections at the edge of their enterprise network. Businesses must make resilience a priority, especially as so many rely on the cloud for operations. But they must also stay agile if they are to remain competitive in a fast-changing marketplace.

Solution:

A SASE framework, incorporating Software-Defined Wide Area Network (SD WAN), Secure Service Edge and zero trust access principles, is an essential component of modern enterprise operations. By protecting access points at the edge of an enterprise network and optimizing their performance, businesses can move more confidently toward their goals, with greater flexibility in how and where work happens, as well as a greater choice of technology.





Protecting enterprise at the edge must be a priority

Our modern world of work is faster and more mobile than ever. With new ways of staying connected and productive come new demands on security.

It's normal now to log onto your laptop and complete a day's work from anywhere. You might not think twice about accessing secure apps from home, a co-working space or even the commute. And if you work in a field like healthcare or manufacturing, you're probably used to accessing real-time data on the health of patients and maintenance status of machines.

For a great many employees and customers around the world, enterprise workloads are now experienced at the network's edge. Our reliance on edge computing – that is, distributing computing resources out to edges of an enterprise environment – is actually a relatively recent development. In fact, the security architecture needed to protect data and people at the edge was only formally defined by Gartner in 2019[1] in response to increasing demand for out-of-office and Internet of Things (IoT) working.

This now-critical architecture is called SASE.

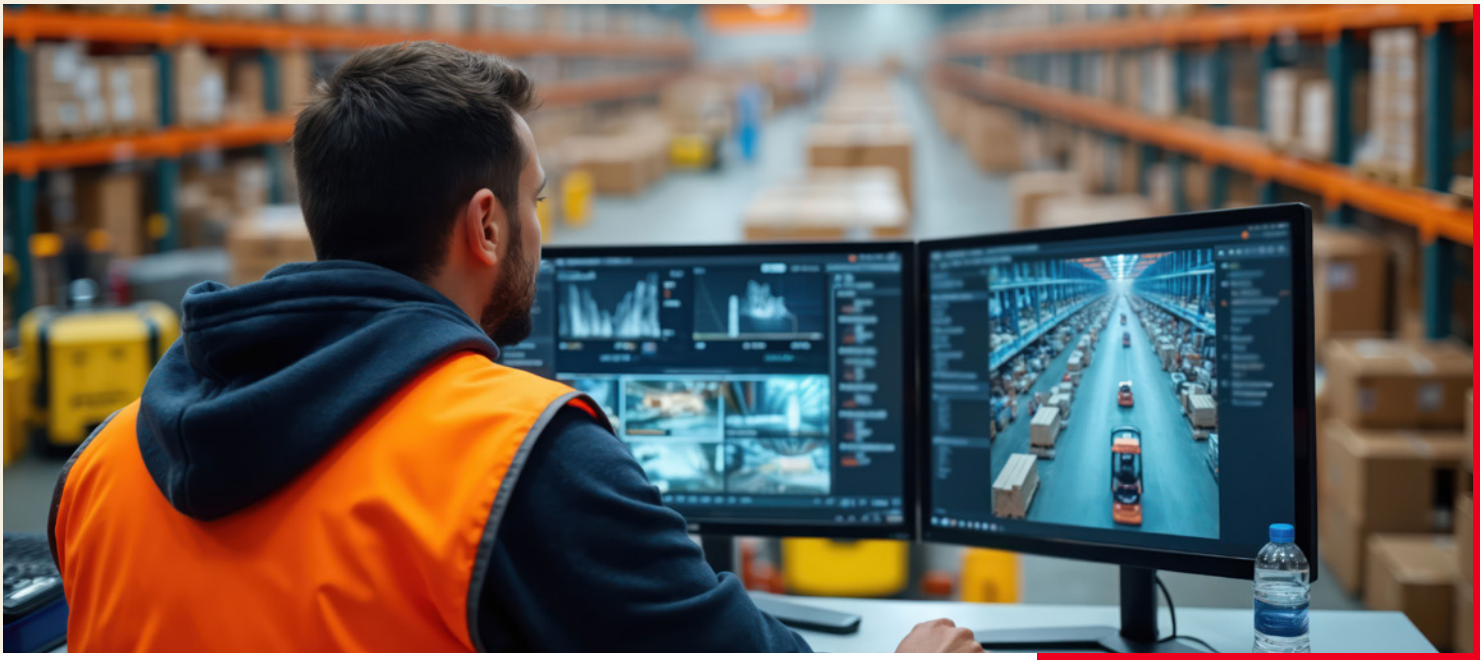
You likely experience elements of SASE every day. In a world of distributed, fast-paced and AI-assisted work, such security measures are vital. After all, if your enterprise network – the invisible engine powering practically every aspect of modern productivity – can be accessed from anywhere by both humans and AI tools in real-time, centralized firewalls and manual checks aren't going to cut it.

The pressure on edge security is even greater as agentic tools come online and demand instant, autonomous access to information. And that's not even touching upon the new reality arising in which AI has begun to escape user control, performing unwanted actions autonomously.[2]

The truth is that all enterprises now operate in a world of disruption, innovation and evolving cyber risk. A secure, resilient network, that still enables authorized users and AI tools to operate with agility, will be a true competitive advantage.

And that calls for SASE.

> "Fundamentally we live in a data-driven world. Data integrity is vital."
>
> **Colin Wilson**
> Enterprise Architect,
> Verizon Business.



What exactly is SASE? And why is it so important?

The move to cloud-first working has boosted speed and efficiency but has also forced a rethink about approaches to enterprise security.

“Around 2007, the world started to move to the cloud,” explains Alistair Neil, Managing Director of Advanced Solutions, International at Verizon Business. “And now, a vast majority of IT infrastructure is cloud based. Businesses have had to quickly change from security models that were broadly hardware based to those that would suit this new world... SASE is the integration of network and security, delivered from the cloud for the cloud.”

SASE is used across a broad array of industries, delivering security controls as a cloud service to the connections at the edge of the network, rather than a central server.

Of course, as cloud-capable businesses would have already seen, latency is drastically reduced when computation and data storage move closer to the source of that data. Without SASE, this would not be a feasible way of working.

Under a SASE model, a connection like a user, device or piece of IoT hardware under an enterprise’s wide area network (WAN) must be able to prove its identity and compliance before being granted access. As opposed to gatekeeping the network with a central firewall, SASE enables greater independence, faster processing and greater operational agility.

We certainly wouldn’t have self-driving cars on the roads without secure edge computing. Your on-device AI assistant would be too big of a risk to allow use in a work environment without SASE. Remote monitoring of machinery and assets in the field would also be a much more difficult, time-consuming prospect.

Our world is one built on complex, multi-cloud environments. SASE helps defend against the threats that would seek to exploit them.

The components of SASE

SD WAN

The software-defined (typically virtualized) WAN, enabling information to be sent to the edge via encrypted overlay tunnels.

Secure service edge

The cloud-centric security framework, including firewall-as-a-service, secure gateways and security brokers.

Zero trust access

The ‘never trust, always verify’ principle in action, requiring authentication at every connection point and minimizing privileges.

How does zero trust security work in the AI era?

Zero trust is a key component of SASE. Users, devices and AI tools cannot simply be allowed free rein of your enterprise network, just as you wouldn't let strangers wander freely into your office.

"How do you get around a SASE environment?" says Neil. "You need to be continually monitored, authenticated with every movement."

"The best analogy is the airport. When you go there, you give them a ticket, you show them a passport, you go through security, to your gate, then show your documents again. You confirm with the attendant that you are 'seat 35'. Everywhere you go, you must confirm who you are, what got you in and where you are going," he says.

Zero trust security requires all entities accessing the network to have a unique identity. Just as an airport must check a passport photo against a passenger's face, a zero trust system must check usernames, passwords and biometric markers against its own database. Such a system must also rely on real-time context clues (like time and location) to test the validity of a connection. In the case of our metaphorical airport, security would not let a suspicious passenger through to the gates if the flight on their boarding pass left the next day.

But the rise of AI and agentic tools tests this well-established methodology.

"I don't think companies are really considering the security implications here." says Neil. "There are so many layers to security when you start thinking of AI."

Wilson notes that managing AI security risk isn't just a technical problem, either. "The challenge with truly autonomous systems is that there are no people to intervene. So, you've got to build in hard and fast governance policies that control the agentic execution of tools from the very start."

Zero trust principles can be applied to AI tools and autonomous agents just as they can users. As long as you can assign these tools a unique identity and understand the context of their actions, security controls will be able to account for agents, AI browsers and autonomous hardware.

AI tools developed and operated in regions outside your own can pose a significant risk, as their 'black box' nature can make understanding data flow difficult. Neil suggests that organizations in areas like defense, finance and government create digital enclaves, with AI tools running on ring-fenced systems.

Of course, building a safety-first, zero trust culture will be crucial for maintaining data sovereignty. Understanding and safely managing agentic AI will mean understanding the agents' footprints, maintaining visibility over their activity and strictly enforcing policies at the execution stage.

Key AI security implications

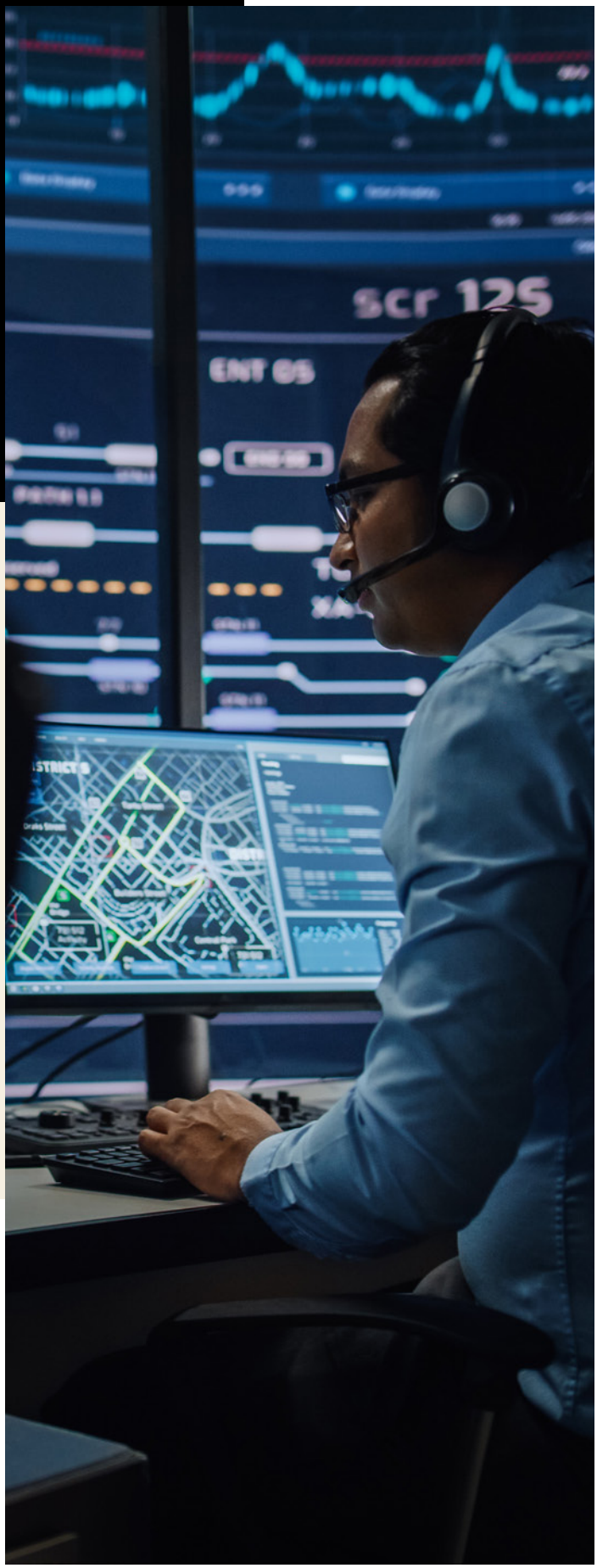
How secure is data from rogue AI access and external threat actors?

Is your corporate data sovereignty intact? And are you compliant with data sovereignty regulations within your region?

Could data be unknowingly sent or exfiltrated?

Is the model itself secure and protected against prompt injection?





Is SASE just about security?

SASE was designed to prevent unauthorized access to your enterprise network. But that isn't the only reason why a business should embrace it.

In fact, SASE enables enterprises to be more agile, build resilience and even identify operational efficiencies, potentially reducing costs.

By providing flexible, cloud-based access to network resources and security controls, SASE can help you achieve diverse business objectives while remaining protected against evolving threats. Delivered by a Tier 1 partner like Verizon Business, able to combine network security and network performance in one service package, the potential benefits are even higher.

Verizon's SASE solution reduces the complexity of managing multiple tools across multiple networks which can help free up valuable IT time. With less time spent being reactive and only one contract to manage, budget and capacity can be reallocated to areas of the business that power growth.

> "SASE provides you with huge amounts of flexibility. It gives you a range of security controls that can protect you, your devices and your business. And it can all be centrally managed, so policy and configuration management can all be done and orchestrated easily."
>
> **Alistair Neil**
> Managing Director, Advanced Solutions International, Verizon Business.



How does SASE make my business more agile?

As businesses expand, open new offices, and onboard remote workers and tools, IT teams face pressure to deploy policies as fast as possible. Manually configuring hardware becomes a non-starter beyond a certain scale, as does managing multiple contracts for security tools.

SASE empowers teams to secure their enterprise network at the edge, even as it grows, protecting the decentralized workforce and hybrid-cloud applications in near-real-time.

Being able to route traffic directly to the cloud or nearest edge node, instead of 'hairpinning' it through distant corporate data centers, will dramatically reduce latency. This means faster application response times and near-instant remote deployment.

Put simply, you can move faster when you know the risks ahead of you are minimized.

What about SASE outside the office?

Across sectors like manufacturing, agriculture and logistics, operational technology (OT) plays a vital daily role. However, as OT begins to blend with IT – through the proliferation of IoT hardware and smart sensors, for example – the need to secure these technologies becomes greater.

Widening the edge of your enterprise network may unlock new operational efficiencies, like predictive maintenance and more intelligent supply chain management, but it also widens the potential attack surface. Deploying technology like this will require the same zero trust approach, with sensors, IoT devices and OT treated like any other user.

Embracing AI while staying agile

The shift toward agentic AI will profoundly impact all aspects of enterprise networking, perhaps even more so than the previous shift to hybrid work. These agents require incredibly low latency and an immense amount of bandwidth. The risks associated with this can be mitigated by working with a Tier 1 partner like Verizon Business, who is able to deliver a comprehensive SASE program and even support dedicated AI networking.

How can Verizon Business help?

Directly connected to over 100 cloud providers globally, Verizon Business is capable of connecting users, devices and applications from edge to edge safely. Our Tier 1 internet peering means fewer network hops and greater efficiency. We also offer options like Secure Cloud Interconnect and Secure Digital Interconnect for high-performance connectivity, allowing you to run core applications on Infrastructure as a Service platforms.

We offer global optionality, encompassing physical and virtual connectivity. This flexibility extends to Local Area Network (LAN) and wireless LAN solutions, vital for future-proofing your network and reducing latency as more AI and IoT tools run at the edge of your network.



Will SASE make your business more resilient?

Prominent businesses have been victims of high-profile cyberattacks in recent years. One major European auto manufacturer was forced to shut production for months following a breach, causing a huge impact on the bottom line. Even cybersecurity firms are not immune, with one software provider targeted, resulting in widespread outages across the services it supplied.

While we can't speculate on the exact cause of these breaches, we do know that the more connections to an enterprise network and the more tools employed, the broader the enterprise attack surface. Risk has increased further with the introduction of AI.

"Entire industries are facing the fact that machines can now target unknown vulnerabilities and exfiltrate data in seconds," says Alistair Neil. "The challenge is changing the architecture so that you're not preventing the business from using the tools it needs to while still protecting the infrastructure you already have."

To maximize efficiency, AI agents will need to act on behalf of users, make API calls, query databases and move data across clouds. A framework like SASE is critical to authenticating and governing these tools, ensuring they don't access data they're not supposed to.

SASE can also help defend against the rising tide of adaptive malware and convincing automated phishing attacks. SASE allows security teams to push threat intelligence updates to the edge instantly, protecting teams from zero-day threats and giving them the knowledge they need to stay safe.

On top of all this, by helping to safely distribute computation and data to the edge, layers of redundancy are introduced that can help businesses bounce back quickly from shocks like natural disasters or cable cuts. SASE helps enterprises transition from a high-risk, centralized infrastructure to a resilient, flexible one.

How can Verizon Business help?

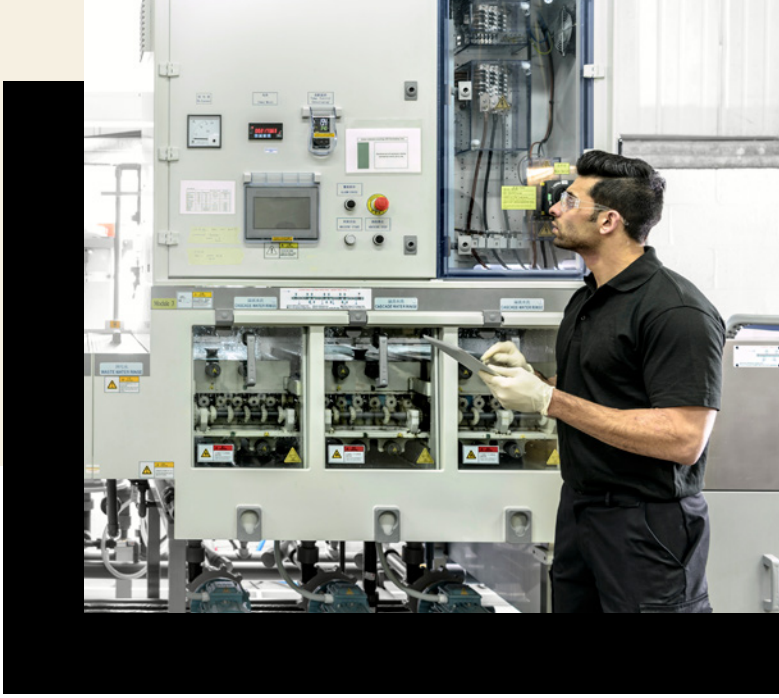
Our Tier 1 status and robust network reaching over 180 countries provides us the scale and stability – in the form of redundancies and failsafes – needed to stay operational through incidents like cable cuts, security breaches and natural disasters.

We leverage our extensive experience in managing risk and security to ensure that your business can get ahead of risk, stay productive at the edge and bounce back quickly should the worst happen. Verizon's SASE solution leverages robust, secure and global network infrastructure to ensure local resilience.

Global monitoring, for your protection

Verizon operates a vast network, overseen by Security Operations Centers across the globe, active 24/7/365. These centers monitor billions of network events daily to proactively hunt threats and mitigate attacks targeting multinational enterprises and government organizations.

How do we remain flexible while embracing SASE?



Seizing opportunities in today's fast-changing enterprise environment means being both open to change and ruthlessly efficient.

While distributing work to the edge does, naturally, make day-to-day work more flexible, it can add pressure on IT and security teams. Managing multiple contracts and tools can add to this burden.

SASE offers a simpler way to centrally manage and administer security, then distribute it to every connection at the edge. This way, you maintain a 'single version of truth', ensuring consistency of policy enforcement and virtual access rights.

As Neil says, "With SASE, expansion into new markets is easier, as are mergers and acquisitions. If you want to pull new partners or workers into a network without putting it at risk, you can do so in a really controlled manner."

Can SASE help us stay in control of AI?

As AI agents are granted more autonomy and deeper access to enterprise networks, it becomes all the more necessary to set and enforce policy and governance at the execution layer.

A comprehensive SASE solution provides a simple way to set AI policies across the network, including bandwidth allocation, network prioritization and even token budgets. This not only allows you to stay in control of AI and automation in the field but also prevent human users from inadvertently exceeding usage limits.

Can Verizon help us better manage our enterprise network?

"Increasing IT complexity requires retooling, automation and AI. You just can't do it with people alone anymore." suggests Wilson. "If you want to manage complex networks, you need the right platforms with scale and intelligence."

Certainly, enterprise at the edge requires a great deal of control and oversight. A single, unified policy framework can help to deliver secure, configurable connectivity across even the widest WAN. But manageability requires visibility.

Verizon's AI operations technology provides the network telemetry and vendor insight – drawn from our work across almost 200 markets – to create valuable insight delivered in an intuitive way.

"The pace of change won't slow down," says Neil. "Which is why our platform supports configuration through a self-service portal and APIs, allowing you to manage thousands of users and devices through a single pane of glass, under a single contract."

How MNS adds further benefits

Managed Network Services (MNS) takes the proactive management of hardware, routing and security protocols off your plate, allowing your teams to focus on strategic business goals.

Verizon Business MNS leverages the power of AI to accelerate processes – including bulk access point provisioning, code upgrades and data gathering – and better meet the demands of hybrid workforces through automated change and service requests.

With seamless, API-enabled integrations and a self-service portal, MNS takes the burden of managing an edge environment away while helping you stay in control.

You can learn more about MNS and begin your journey at verizon.com/business/en-en/products/networks/managed-network-services/



Alistair's key considerations for SASE in the AI era



There's no denying that AI has changed work and the management of enterprise networks forever. Alistair Neil, Managing Director, has seen this transformation happen in real time and has used his experience of working with global clients to compile the three most important questions that businesses must ask themselves:

1. What AI tools should we be utilizing? And what might bad actors use to target us?
2. What kind of cybersecurity, protection and controls do we have in place? And what do we still need to implement?
3. How are we defining proper governance of AI in our business?

How can Verizon Business help us become more resilient, secure and agile?

The SASE industry is growing fast. In fact, by 2030, the market is expected to be worth over $17 billion.[3] But not all solutions are made equal.

For enterprises looking to benefit from the flexibility of edge computing without putting the invisible engine of their network at risk, choosing Verizon Business as a strategic partner will be transformative.

With over 20 years of experience in the design, deployment, and management of network and security infrastructure we put our knowledge and expertise to use in all our engagements.

We leverage best-of-breed technology partners to ensure you have access to the tools you need to protect and scale your business, as well as seamless integrations. Combining our relationships with leading SASE vendors with the foundational layer of a Tier 1 network allows us to deliver solutions far greater than the sum of their parts.

You can also operate in confidence knowing that Verizon is continuously monitoring for cyber threats. Our Computer Security Incident Response Teams are able to quickly respond, determine remediation steps, and help to identify root causes and their evidence. We'll also run leadership teams through simulations to understand potential scenarios, then build training specific to your business to help you respond appropriately to cyberthreats.

We ensure that our SASE solution, and our broader Managed Network Services offering, don't simply amount to a way to offload services. You also benefit from proactive troubleshooting, a truly collaborative approach, and centralized network and security management. All of this helps to drive impact, accelerate time to market and enhance customer experiences.

This success is part of why we've been named a Leader in both the Gartner® Magic Quadrant™ for global network services, and in the IDC MarketScape: Worldwide Managed SD-WAN 2020 Vendor Assessment.

Beginning your SASE journey

Navigating the complexities of SASE requires a partner capable of supporting you at every stage of the journey. It's a challenging road, but the risks that come with not transforming are greater.

"The reality is, almost everyone is in need of an evolution," says Neil. "We walk our partners, step by step, through the process, helping to avoid technical debt."

Our consulting, transition and project management teams provide the expertise and resources to guide you safely from high-risk legacy environments to a transformed cloud-based platform. And, by choosing Verizon Business as your partner, you benefit from all of this support with a single contract and simple billing.

SASE may be a security framework, first and foremost, but with Verizon Business, it unlocks new levels of flexibility, resilience and agility – all crucial to maintaining your edge in a fast-moving, competitive market.

Connect with our enterprise strategy team today for an insight-led discussion on unlocking these benefits across your own enterprise network. For more information visit verizon.com/business/en-en/solutions/adaptive-networks/





1. Gartner, The Future of Network Security is in the Cloud, 2019
2. The Guardian, Sharp rise in incidents of AI escaping users' control, research finds, 2026
3. Grand View Research, Secure Access Service Edge Market (2025 - 2030), 2026

© 2026 Verizon. This content was created with the assistance of artificial intelligence and validated by humans. OGSB1350423