

Creating an
industry-leading
Secure Access Service Edge
(SASE) proposition



A GUIDE BY

CONNECT

According to Gartner, there are major benefits to working with a single SASE vendor who can provide the full range of technologies, capabilities, and network coverage today's hybrid and remote working model demands. This is exactly what Connect offers, with our comprehensive SASE solution, Global Network, and flexible deployment options.

Why SASE? Why now?

Many organisations have been supporting remote and hybrid working for a number of years, but now, the world has changed. Since the pandemic hit, remote working has become the norm, and the role of office is evolving to become a collaboration space. This has put major strain on the technology infrastructure, from collaboration platforms and tools, to the networks that connect remote workers.

A primary concern is security. In the past, it was possible to protect the majority of applications and traffic behind office-based firewalls, but no longer. A few offices have now been replaced by hundreds, or even thousands, of distributed endpoints, meaning centralised security tools are now impractical, and often totally ineffective.

For all of these reasons, leading analysts - in particular Gartner - are charting a shift from centralised firewalls, VPNs and other access and security technologies, to more distributed solutions at the network edge.

This approach, which has become known as Secure Access Service Edge, or SASE, supports faster, more reliable, highly secure connectivity between employees, cloud platforms, apps, and other IT resources.

In other words, it's a networking architecture - a way of thinking, even - designed for remote and hybrid working.

What is SASE?

Gartner describes SASE as a collection of edge technologies that “combines network security functions such as Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), Firewall as a Service (FWaaS) and Zero Trust Network Architecture (ZTNA), with WAN capabilities (i.e. SDWAN) to support the dynamic secure access needs of organisations.”

It suggests these capabilities should be deployed in the cloud and delivered “as a service”, with comprehensive ID checks, device checks and compliance policies built in to ensure that only authorised users access apps and services.

Critically, SASE also allows organisations to encrypt and decrypt content at line speed, providing greater performance for remote and hybrid workers. Unified communications sessions are monitored continually to assess constantly changing risk levels.

Overcoming common SASE deployment challenges

While SASE promises clear performance and security benefits compared to centralised solutions, not all SASE offerings are created equal.

Many only provide a single piece of the technology jigsaw, which can create significant complexity, both during the deployment process, and for ongoing management. Equally, many SASE vendors offer security at the network edge, but no networking capability – which potentially creates operational and performance issues with no clear view of where the cause or responsibility lies.

To overcome these challenges, Gartner recommends that organisations work with either a single SASE vendor, or two vendors with a close partnership and pre-integrated solutions. The challenge is finding such vendors, especially as SASE is a relatively new area.

Why Connect is the ideal SASE partner for your business

Connect has designed and built our SASE solution in a way that minimises deployment and operational risk for your business.

- 1** By pre-integrating best-of-breed SASE technology components and capabilities, Connect provides a single point of contact and responsibility for your edge security and QoS environment.
- 2** Our global network, which connects over 40 tier 1 carriers and around 700 datacentres, ensures that your remote and hybrid workers can connect into your cloud apps and other IT resources quickly, reliably and - above all - securely, wherever they work.
- 3** All the elements delivered as a service are backed by our experienced, professional managed services team, providing outstanding SLAs and clear accountability for performance.

In this document, we provide the detail behind our SASE proposition, demonstrating how we fully meet Gartner's requirements and recommendations for a successful SASE implementation. If you have any questions or would like any additional information about our SASE capabilities, please [contact us](#).

Gartner Summary: Digital business transformation inverts network and security service design patterns, shifting the focal point to the identity of the user and/or device - not the data centre. Security and risk management leaders need a converged cloud-delivered **secure access service edge** to address this shift.

Gartner[®]

Building a SASE solution: Connect's comprehensive, best-of-breed approach

Gartner's definition of SASE clearly outlines the full range of technologies needed to support today's remote and hybrid working strategies. By replacing centralised security and management platforms with SASE capabilities, organisations can maximise security, improve application performance, and streamline management of users and IT resources.

Based on the needs of our customers, Connect has designed and built our SASE solution around nine key 'pillars'. Outlined in detail below, these fully meet the requirements outlined by Gartner in its 2021 'Strategic Roadmap for SASE Convergence'.

1) Zero Trust - ZT

Zero Trust (ZT) is an IT security model that requires **strict identity verification for every person and device trying to access resources on a private network**, regardless of whether they are sitting within or outside of the network perimeter.

At Connect, we support the Zero Trust model by segmenting and protecting all devices on your network individually (microsegmentation). We can apply protection across servers, applications, user devices and IoT devices – either via an agent or, in the case of certain IoT devices, using an "agentless" model.

Connect's Zero Trust capabilities allow organisations to understand the health and status of every device on your network from a security perspective. Additionally, you can ensure that devices and technologies connected to common networks are protected from a security breach affecting a specific device. This protection can be defined at the IP networking level, by port, or according to protocols or processes.

For user access to servers and applications, Identity as a Service (IDaaS) is used to provide Identity Services to simplify the user experience whilst enhancing authentication and authorisation.

Connect Zero Trust capabilities are delivered by our ZTNA, IoT, IDaaS, and FWaaS solutions.

For more information about the principles of Zero Trust, please see **Appendix A** at the **end of this document**.

Building a SASE solution: continued

2) Zero Trust Network Architecture - ZTNA

To support modern remote and hybrid working, organisations need clearly defined access control policies for all end users. Additionally, end user devices need to be identified and secure before they access IT resources and, in particular, sensitive operational or customer data.

Connect delivers this high level of security with our ZTNA approach, which firewalls all end user devices (endpoints) individually. In this way, we protect devices used to access the network, regardless of their location, simultaneously reducing the need for “East to West” firewalls. To further increase security, we deploy gateways around our Global Core Network, allowing for user traffic to be secured from the device to the security perimeter known as “north to south”.

In addition to these benefits, the Connect solution supports “split tunnelling” to enable direct routing of traffic for remote working. This capability, which optimises QoS for remote workers, is supported by our SWG and FwaaS offerings.



3) Identity as a Service - IDaaS

Ensuring that any person accessing systems, data and applications is appropriately authenticated is a primary requirement for IT and enterprise security.

Connect enables this with seamless integration of multiple user directories and data sources and multi-factor authentication solutions. The result is a unified, highly efficient IDaaS solution that also supports Single Sign On for an enhanced user experience.

4) Internet Firewall as a Service - IFWaaS - Network

The Connect SASE solution incorporates IFWaaS within the network. This cloud-hosted solution creates a controlled gateway for connecting to the internet (both ingress and egress). It provides standard firewall capabilities, along with tools for effective management and troubleshooting of internet bandwidth.

Advanced features of our IFWaaS solution - including IDS and IPS - are available as service options. As a part of our wider SASE portfolio, our SWG solution provides URL filtering and Internet access controls.

Building a SASE solution: continued

5) Firewall as a Service - FWaaS - Hosts

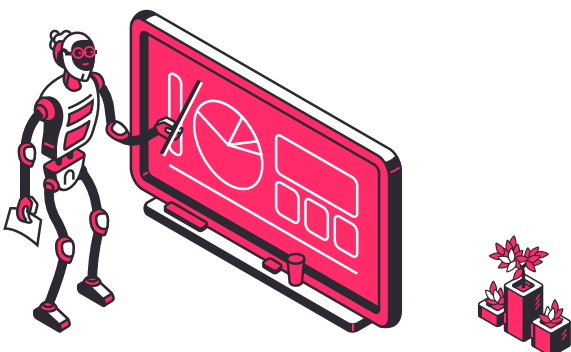
The Connect Zero Trust solution incorporates FWaaS for servers and endpoints by individually 'firewalling' connected devices, even if they are managed centrally. This means that end user devices are protected, regardless of location, while also reducing the need for 'East to West' firewalls.

Again, URL filtering and Internet access controls are provided by our SWG solution.

6) Operational Technologies / Internet of Things - OT/IOT

In all kinds of business locations, from offices to logistics parks, there are a wide range of network-connected devices and sensors that have not historically been managed, monitored, or security protected.

The Connect SASE solution segments these devices and secures them with a Zero Trust appliance, ensuring that the risk of security breaches is minimised.



7) Cloud Access Security Broker - CASB

With organisations moving ever more of their mission critical workloads and data to the cloud, security and access control have become critical.

To maximise the security of cloud services, Connect offers CASB that sits between your internal systems and the cloud. This allows you to extend your internal security capabilities and policies into cloud services, ensuring that access is only granted to authorised users.

The Connect CASB is integrated with our Zero Trust and IDaaS authentication software to enable appropriate and proportionate levels of access control for your critical cloud services.

8) Secure Web Gateway - SWG

To protect devices and applications across the network, you need tools that ensure compliance with corporate and regulatory policies and detect and eliminate malware from user-initiated internet traffic.

The Connect SASE solution performs all the required security and compliance checks, without the need to transit traffic through particular points on the internet. This enables more direct routing of traffic between end users, corporate IT resources, and cloud services – reducing latency and optimizing the user experience.

Building a SASE solution: continued

9) Software Defined Wide Area Network - SDWAN

To optimise application and service performance and deliver great user experiences, you need virtual WAN infrastructure that supports any combination of transport services (including MPLS, LTE, and broadband internet services). Connect provides this with our SDWAN capabilities, which offers smart routing for end users' sessions, with full integration into our Zero Trust solution.

Our SDWAN solution provides a range of benefits, including WAN simplification, which enables:

- Lower costs
- Increased bandwidth efficiency
- Significant application performance
- Increased security and data privacy
- Zero trust network solution

Our managed service wrap

All of the elements of our SASE solution are managed by Connect's own team to ensure outstanding performance, easy configuration changes and a hassle-free upgrade path.

Our ethos of jeopardy management, built on constant monitoring of all elements, means that the overwhelming majority of issues that could affect service are resolved before our clients even know about them.

A fast-track to SASE with the Connect Global Network

Connect's Global Network enables us to create and offer unique solutions with a cloud-first focus and full integration with existing networks and services. The Global Network underpins our unique SASE proposition, with the full range of SASE capabilities hosted and managed through a single skilled partner.

By providing both a full suite of SASE software and a global network footprint, Connect meets Gartner's criteria as an end-to-end SASE provider that can fully support organisation's current and future remote working strategies.

Our integrated solution reduces the on-site infrastructure footprint for our customers, and enables seamless, global integration with Tier 1 carriers, datacentres, and cloud service providers.

The following key SASE services are all deployed in the network, reducing latency:

- ZTNA
- IDaaS
- IFWaaS (Network)
- FWaaS (Host)
- OT/IoT
- CASB
- SWG
- SDWAN

The Connect Global Network differentiates our SASE proposition by providing:

- A Zero Trust gateway into a secure global private network
- Easy integration of SASE capabilities into existing networks and infrastructure
- Global termination zones for ZTNA
- SDWAN traffic routing and management across the network
- Direct private access to cloud services
- A range of voice capabilities, delivered directly over the network, including:
 - Global SIP platform that provides voice services in more than 100 countries
 - Session Border Controller (SBCaaS), which is delivered as a service and fully certified for MS Teams direct routing
 - Private delivery of voice

The Connect Global Network.



Data Network Services (at a glance):

18

Network nodes covering
5 continents

40+

Tier 1 carriers

100+

Countries where we offer
Ethernet services

700+

Global Data Centres connected

100+

Cloud services accessed directly



Flexible SASE deployment options for every scenario

Connect offers a range of deployment options to meet the unique needs of our customers. Specifically, we are able to deploy our solutions in the cloud, on agents and devices in customer or third-party networks, or from within the Connect Global Network.

The following table shows the full range of deployment options we offer:

Technology	Cloud	Agents & Devices	Connect Network
ZT	✓	✓	✓
ZTNA	✓	✓	✓
IDaaS	✓		
FWaaS	✓	✓	✓
IFWaaS	✓		✓
OT/IoT	✓	✓	
CASB	✓		✓
SWG	✓	✓	✓
SDWAN	✓	✓	✓

Our value-added SASE services for cybersecurity and project delivery

Security Operations Centre (SOC)

Our 24/7 Security Operations Centre provides proactive monitoring and management of key SASE systems and technologies, helping you to detect and mitigate risks and protect your systems and data more effectively.

Cybersecurity consulting and services

Our cybersecurity consulting and services help you to define and address potential vulnerabilities, minimizing the risk of a security breach across your distributed environment.

The services include:

- security strategy
- cyber risk assessment
- security audits
- incident response
- training and awareness
- security certifications
- compliance
- security policy framework
- cyber threat management
- managed intelligence services
- continuous vulnerability monitoring service
- managed vulnerability scanning services

Project management and delivery

Our project planning, management and delivery services help you to transition to SASE quickly and with minimal operational and financial risk.


Our project-related services include:

- workshops
- configuration
- PoC
- testing
- implementation
- security sign-off
- managed transition and handover to operations


To find out more about any of these additional services, please talk to your Connect account manager.

Ticking all the boxes: how our solution aligns with Gartner's recommendations and roadmap for SASE


In this section, we demonstrate how our SASE solution meets the requirements and recommendations of Gartner's 'Strategic Roadmap for SASE Convergence' for 2021.

Gartner 2021 Strategic Roadmap for SASE Convergence	 SASE Solution
Requirements	
<p>To protect anywhere, anytime access to digital capabilities, security must become software-defined and cloud-delivered, forcing changes in security architecture and vendor selection.</p>	<p>ZTNA + Connect Global Network</p>
<p>Perimeter-based approaches to securing anywhere, anytime access has resulted in a patchwork of vendors, policies, and consoles creating complexity for security administrators and users.</p>	<p>ZT + ZTNA + OT/IoT + FWaaS + IFWaaS</p>
<p>Enterprises that consider existing skill sets, vendors, and products and timing of hardware refresh cycles as migration factors will reduce their secure access service edge (SASE) adoption time frame by half.</p>	<p>Connect SASE</p>
<p>Branch office transformation projects (including software-defined WAN [SD-WAN], MPLS offload, internet-only branch and associated cost savings) are increasingly part of the SASE project scope.</p>	<p>SDWAN + Connect Global Network</p>

Ticking all the boxes: Continued

Gartner 2021 Strategic Roadmap for SASE Convergence	 SASE Solution
<p>SASE is a pragmatic and compelling model that can be partially or fully implemented today.</p>	<p>Connect SASE <i>(which includes our modular, flexible deployment strategy)</i></p>
<p>Recommendations</p> <p>Security and risk management leaders responsible for infrastructure security should develop a roadmap for the adoption of SASE capabilities and offerings.</p>	
<p>Short term:</p>	
<p>Deploy zero trust network access (ZTNA) to augment or replace legacy VPN for remote users, especially for high-risk use cases.</p>	<p>ZTNA</p>
<p>Inventory equipment and contracts to implement a multiyear phase out of on-premises perimeter and branch hardware in favour of cloud-based delivery of SASE capabilities.</p>	<p>Connect SASE + Connect Global Network</p>
<p>Consolidate vendors and cut complexity and costs as contracts renew for secure web gateways (SWG), cloud access security brokers (CASBs) and VPN. Leverage a converged market that emerges combining these security edge services.</p>	<p>ZTNA + FwaaS + IFWaaS + SWG + CASB</p>
<p>Actively engage with initiatives for branch office transformation and MPLS offload in order to integrate cloud-based security edge services into the scope of project planning.</p>	<p>Connect Global Network</p>

Ticking all the boxes: Continued

Gartner 2021 Strategic Roadmap for SASE Convergence	 SASE Solution
Longer term:	
Consolidate SASE offerings to a single vendor or two explicitly partnered vendors.	Connect SASE
Implement ZTNA for all users regardless of location, including when in the office or branch.	ZTNA + IFWaaS + SDWAN
Choose SASE offerings that allow control of where inspection takes place, how traffic is routed, what is logged, and where logs are stored to meet privacy and compliance requirements.	Connect SASE + Connect Global Network
Create a dedicated team of security and networking experts with a shared responsibility for secure access engineering spanning on-premises, remote workers, branch offices and edge locations.	Connect SASE

Strategic planning assumptions

By **2024**, 30% of enterprises will adopt cloud-delivered SWG, CASB, ZTNA and branch office firewall as a service (FWaaS) capabilities from the same vendor, up from less than 5% in 2020.

By **2025**, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch and edge access, up from 10% in 2020.

Yet by **2023**, to deliver flexible, cost-effective scalable bandwidth, 30% of enterprise locations will have only internet WAN connectivity, compared with approximately 15% in 2020.

Connect SASE takes you on this journey

Get started today

With solutions to support every functional requirement and recommendation outlined in Gartner's Strategic Roadmap, Connect is ideally placed to meet your own SASE needs. In particular, we are uniquely positioned to meet the recommendation for working with a single SASE vendor across all requirements.

The combination of software, services, and networking capabilities offered by Connect are unique in the marketplace, giving you a single point of contact and responsibility for your SASE deployment.

To find out more about our SASE capabilities and how we can help you achieve your technology and business goals with edge solutions for security and QoS, please [contact us today](#).

Appendix A: The Principles of Zero Trust

What is North to South?

In the context of networks and security, North to South relates to communications to edge or perimeter systems, networks and data.

What is East to West?

In the context of networks and security East to West relates to the access between systems and devices on a common network, LAN and WLAN – within the perimeter.

What is segmentation?

In the context of Zero Trust, it is the act of segmenting a defined group of networks, users, devices or applications from other networks, users, devices or applications.

What is Microsegmentation?

Microsegmentation in the context of Zero Trust is the act of segmenting access at the device level enabling targeted isolation, control and monitoring.

Connect with us.

To discuss a communications challenge or find out more about our capabilities, get in touch with us [today](#).