

Does your business need SASE?

Whether your business is Hybrid, Remote, or In-Person – SASE has you covered!

Use Case	Zero-Trust Network Access (ZTNA)	Internet Security	Complete Office Security & Networking
Description	Improve security for internal applications for all users regardless of location.	Secure users' online and SaaS traffic with comprehensive, always on internet security regardless of location.	Comprehensive security and networking for offices and data centers, including all users and devices.
Products Impacted	<ul style="list-style-type: none"> Works with existing Firewall; adds protection for remote users with new cloud firewall. Replaces legacy VPN and IDPS. 	<ul style="list-style-type: none"> Works with existing Firewall; adds protection for remote users with new cloud firewall. Replaces Secure Web Gateway (SWG) and DNS filters. 	<ul style="list-style-type: none"> Simplifies security and networking via software-defined perimeter. Replaces Firewall, SDWAN, SWG, DNS, VPN, and IDPS.
New Capabilities for Businesses	<ul style="list-style-type: none"> Data Loss Prevention (DLP) Threat Prevention and Intrusion Detection/Prevention Improved digital experience 	<ul style="list-style-type: none"> Cloud Access Security (CASB) Threat Prevention and Intrusion Detection/Prevention Improved digital experience 	<ul style="list-style-type: none"> All the above, plus: IoT security for phones, printers, cameras, etc. (VoIP) Built-in global secure SD-WAN

Glossary

Data Loss Prevention (DLP)

A category of practices and products that aim to minimise the negative impacts of a network breach, like lost, stolen, or leaked data.

Domain Name System (DNS)

The internet's protocol for translating URLs into the IP addresses that machines require to resolve an internet request and communicate with or display a website.

Cloud Access Security (CASB)

A type of software focused on maintaining data stored in the cloud by enforcing strict rules to protect against unauthorised access, data leaks, or other security incidents.

Firewall

A network security system that monitors and controls incoming and outgoing network traffic based on security rules.

Internet of Things (IoT)

The network of physical objects, or "things," connected to the internet allowing devices and machines connected to the internet to communicate with each other. Examples include smartphones, vehicles, industrial equipment, and medical devices.

Intrusion Detection & Prevention System (IDPS)

A type of software that protects business networks by analysing all incoming data for suspicious or malicious activity to ensure business security.

Secure Access Service Edge (SASE)

A cloud-based zero trust architecture that requires no on-premise hardware.

Secure Web Gateway (SWG)

A security solution designed to protect networks from cyberthreats by blocking access to malicious websites, preventing malware downloads, and detecting other web-based attacks.

Software-Defined Wide Area Network (SD-WAN)

Network software and technology that relies heavily on cloud-based technology to simplify network management and improve security.

Virtual Private Network (VPN)

A tool used to keep your internet connection secure and protected from threat actors.

Voice over Internet Protocol (VoIP)

Technology that offers a way to make phone calls via the internet rather than using traditional phone lines. Examples include Skype, Zoom, and WhatsApp.

Zero-Trust Network Access (ZTNA)

A security measure where users can only access the applications and data they need to access and nothing more. This approach is essential because it creates a secure environment where all users and devices must be authenticated before accessing business data.