



Sales Enablement Pack   
Secure Access Service Edge (SASE)

Accelerating your customer’s digital transformation journey

# SASE - Sales Enablement Pack

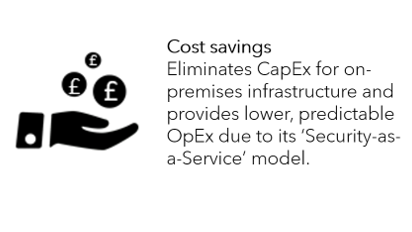
### Accelerating your customer’s digital transformation journey

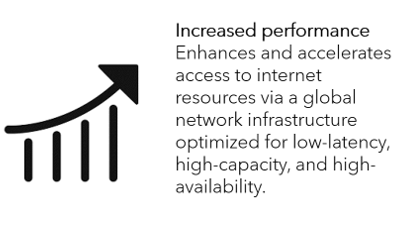
# The accelerated increase in remote users and new hybrid working patterns has escalated the need for cloud-delivered solutions to enable working from anywhere, anytime and any device. Businesses need to ensure that they can enable employees with secure access to their applications while retaining control over data. Our Secure Access Service Edge (SASE) solution helps to accelerate your customer’s digital transformation journey, providing a proven security platform that is data-centric, cloud-smart and as fast as your business.

# What is Secure Access Service Edge - SASE

* As defined by Gartner, Secure Access Service Edge (SASE), pronounced “sassy”, is an emerging framework for the convergence of networking and network security services within a global cloud-based platform to protect users, applications and data.
* Due to the Covid-19 Pandemic, many businesses had to support a distributed workforce, creating additional security challenges as most of their employees were no longer on the corporate network, and could not depend on conventional hardware appliances at the network edge.
* We have partnered with Gartner Credited SASE Providers Palo Alto, Netskope and Cisco to provide our SASE Solution.
* Our SASE solution is a cloud-based web security gateway, that protects the enterprise from the growing volume and sophistication of cloud-enabled threats and data theft, ensuring users can safely and securely use cloud apps and the web to go about their daily business tasks.
* Offering a single platform, with unified cloud-native microservices architecture including elements such as Secure Web Gateway (SWG), Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP) and Threat Protection, all built upon a Global Access Network optimised for high performance and maximum user experience.
* The solution protects users accessing the web by detecting threats such as malware, phishing sites and drive-by exploits, which can easily pass through legacy defences or be whitelisted to bypass defences by leveraging trusted domains with valid certificates.
* Through the use of advanced knowledge of decoding applications and cloud services for content and context with the added benefit of machine learning, our solution enables businesses to be protected against not only known attacks, but also emerging threats.

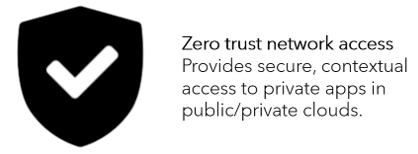
# Why SASE











# 

# Why Expo-e for SASE

A picture containing text, screenshot, font

Description automatically generated

# Traditional Security vs SASE

A picture containing text, screenshot, font, number

Description automatically generated

\*This needs to be slightly reworded to be Channelised

# Features & Benefits

Please note that features below will be solution dependent.

* **Analytics & Reporting** – Providing advanced analytics and reporting on details such as user activity, location and file sharing to contribute to data to produce proactive security measures e.g. SIEM.
* **Anti-Malware/Anti-Virus** – Anti-Malware focuses on new threats, while antivirus keeps you protected against the traditional versions, like worms and phishing attacks, that can still harm your device. The two complement each other, with antimalware designed to supplement antivirus protection as the cyber threat landscape becomes more sophisticated.
* **Centralised Management** – The ability to centrally manage through a portal, providing a single pane of glass model. This allows for efficient control of policies and access across their entire business estate.
* **Client Software Agent** – Use of a Software Agent to provide secure connectivity from the User to the SASE Cloud for filtering and control.
* **Cloud Access Security Broker (CASB)** - CASB helps organisations understand what applications are being used in the cloud, and who is accessing those resources to deliver security controls across SaaS, Web, and IaaS services, and protecting their most sensitive data in the cloud.
* **Data Loss Prevention (DLP)** - Data protection as an integrated part of the cloud security framework. Modern cloud DLP solutions provide full visibility and context awareness of data movement across clouds as well as mitigation of loss and exfiltration.
* **Domain Name System (DNS) Security** – Predictive analytics, machine learning and automation is used to combat threats in DNS Traffic. This allows businesses to block any bad domains, and get a predictive insight into unknown ones, whilst stopping DNS Tunnelling.
* **Endpoint Detection & Response** - Endpoint detection and response technology can help to provide real time alerts to spot the early stages of an attack, as well as uncover how threats may have evaded existing defences, to help provide information on how to stop future attacks from occurring.
* **Firewall as a Service (FWaaS)** – Ensures that branch offices are protected from unknown threats, whilst also providing next-gen security features including threat prevention and URL filtering.
* **Intrusion Detection & Prevention** - Intrusion detection allows security teams to analyse events in your customer’s network for early signs of incidents and threats, enabling Intrusion Prevention systems to stop any attacks to the IT networks.
* **Remote Access for Private Cloud** - Remote access enables users to access files and other system resources on any devices or servers that are connected to the network at any time, increasing employee productivity and enabling them to better collaborate with colleagues around the world.
* **Sandboxing** - Sandboxing protects an organisation's critical infrastructure from suspicious code because it runs in a separate system. It allows IT teams to test malicious code in an isolated environment to understand how it works within a system as well as more rapidly detect similar malware attacks.
* **Secure Web Gateway (SWG)** - Our managed solution gives your customer a SWG functionality to provide visibility into their traffic and monitor suspicious activity, while being able to web filter, preventing theft and the sharing of credentials to unknown sources.
* **SSL/TLS Inspection** – Inspecting encrypted web traffic and cloud services for potential data theft, malware, and advanced threat.
* **URL Filtering** - URL filtering limits access by comparing web traffic against a database to prevent employees from accessing harmful sites such as phishing pages.
* **Web Application Firewall (WAF)** – Is a filter that protects against HTTP application attacks by inspecting HTTP traffic before it reaches applications and protects the businesses servers by filtering out threats that could damage site functionality or compromise data.

# SASE Feature Matrix

A screenshot of a computer

Description automatically generated with low confidence

*\*Need to confirm this is OK for external view?*

# A close-up of a text Description automatically generated with low confidenceSASE Use Cases

# Complimentary Services

### SD-WAN

With the increase of Public and Private Cloud use, it is imperative that WAN performance is at its optimum to cater for mission critical workloads to ensure business continuity.

Our managed SASE Solution can be integrated with our SD-WAN offering to secure the branch edge. Our offering allows your customers to have security in the cloud and branch sites, giving the same level protection as at the headquarters. As there is no longer a need to backhaul internet connectivity to the businesses centralised firewalls, your customer benefits from faster access to business-critical applications and information.

### CSOC

It is vital that businesses can monitor their network usage for any malicious behaviour, while being able to analyse any data received to proactively put security measures in place.

To optimise our managed SASE solution, your customers can choose to add our CSOC services. Integration into our Security Incident and Event Management (SIEM) platform will require installation of a Virtual appliance, which enable logs to be retrieved from the SASE solution, which can then be forwarded over to the syslog server. Our SIEM Platform enables our in-house CSOC team to monitor and respond to any security threats that may be present across the entire business estate, providing a true End-to-End security solution.

# Discovery questions to ask your customer

* How does your company deal with remote user requirements?
* What is the plan going forward? Back to the office, remote or both?
* Have you taken on more Cloud or SaaS Services in the last year?
* Do you have a secure mechanism for accessing the Internet or corporate applications hosted in SaaS, Public or Private Cloud environments?
* Do you want to allow your users to remotely access your corporate applications from their personal devices with secure network access controls in place?
* Do you have a need to monitor network usage for users spread across multiple geographic locations, including a remote workforce?
* Are you working on any Digital Transformation projects?
* Do you need to contain confidential data (PHI, PII, PCI) within approved cloud services?
* How many users do you have that are in branch offices and at remote locations?
* Which regions do your employees work within?
* Which applications do your employees use, where are they hosted and how are they accessed?
* What kind of network security do you have at the moment?
* What kind of remote access solution do you have at the moment?
* Are you concerned about data loss through unapproved cloud apps (“Shadow IT”)?
* Do you need to identify unsafe cloud apps, and monitor unsafe user practices?

# Qualification questions to ask your customer

A screenshot of a computer security centre

Description automatically generated with low confidence

A picture containing text, screenshot, font, number

Description automatically generated

A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a phone

Description automatically generated with low confidence