



Optus Managed Security Service Edge (SSE)

Cloud-delivered security. Simplified. Scalable. Seamless.

Optus for Enterprise

yes OPTUS

Modern businesses face a surge of new challenges:

- Users connect from anywhere, often bypassing traditional on-premises security.
- Critical data and apps now reside in the cloud, increasing the attack surface.
- Cyber threats have grown in sophistication – ransomware and other attacks are more organised, automated and relentless.
- Ensuring policy consistency for a remote workforce is difficult.
- Managing a patchwork of legacy tools adds operational complexity and overhead.
- 86% of organisations report challenges with recruiting and retaining skilled security professionals¹.

To address these challenges, organisations need advanced security, real-time threat monitoring and comprehensive protection for distributed workforces and cloud-based operations. Optus Managed SSE does all this for you.

Secure your business across every device, user and location

Optus Managed Security Service Edge (SSE) is a next-generation, scalable cloud security solution that enforces consistent policies and advanced threat protection for all users – wherever they work. It consolidates critical security functions such as Cloud Access Security Broker (CASB), Cloud Firewall, Secure Web Gateway (SWG) and Zero Trust Network Access (ZTNA) moving from point solutions to an integrated platform solution.

Designed for today's distributed digital landscape, it places security controls closer to your users and resources, enabling straightforward management, lower costs and a dramatically improved security posture.

Secure your business across every device, user and location

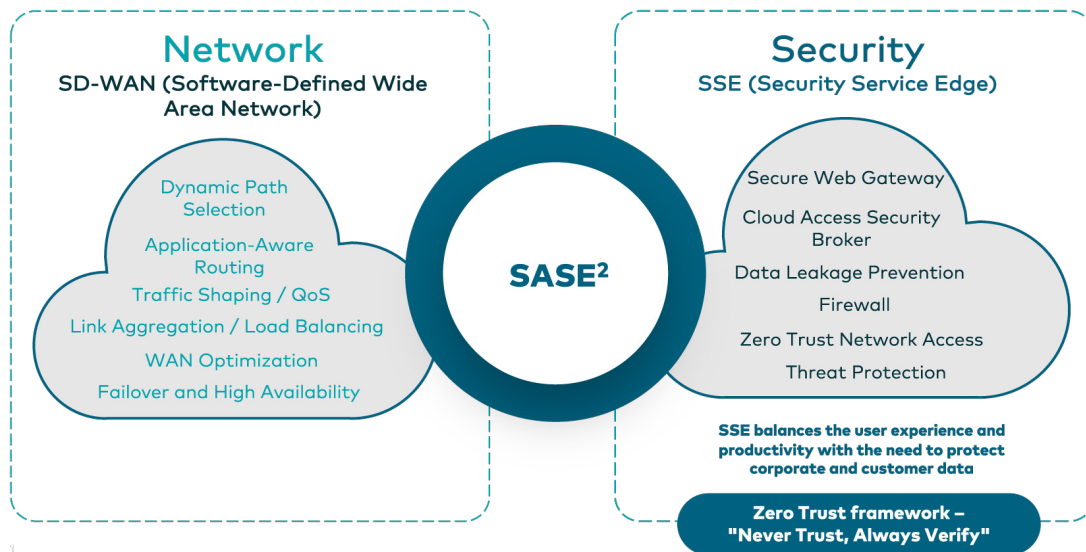
Optus Managed SSE balances the user experience and productivity with the need to protect your corporate and customer data. Importantly, it can also be unified with your SD-WAN in a Secure Access Service Edge (SASE) solution.

¹ Splunk 2023 State of Security report



What is SASE and how does SSE fit in?

Secure Access Service edge (SASE)² is a framework that unifies Network (SD-WAN) + Security (SSE)



What you get with Optus Managed SSE

Optus Managed SSE is engineered to address business challenges head-on, providing:

- ✓ **Enhanced security:** A unified security platform that integrates Cloud Access Security Broker (CASB), Cloud Firewall, Secure Web Gateway (SWG) and Zero Trust Network Access (ZTNA) into a single, fully managed solution — delivering consistent policy enforcement and reducing breach risk.
- ✓ **Scalable cloud delivery:** Adjust to changing needs (expanding sites, new users) without costly infrastructure upgrades, thanks to cloud-native elasticity.
- ✓ **Advanced threat protection:** Data loss prevention (DLP), intrusion prevention and malware detection help stop breaches before they impact your business.
- ✓ **Low-latency access and continuous authentication:** Ensure only authorised users and devices can access corporate resources.
- ✓ **Real-time visibility:** Centralised dashboards provide full control over activity and security posture.
- ✓ **Expert support and continuous improvement:** The managed model provides you with 24/7 monitoring, troubleshooting and policy optimisation by security professionals, ensuring rapid response to incidents and continuous enhancement of your security posture.

Optional extra

- ⊕ **Threat monitoring and response:** Optus Managed Threat Monitoring Service enables 24/7 detection, correlation and alerting across cloud, network and user activity, helping identify and respond to threats in real time.

² Secure Access Service Edge (SASE) is a Gartner term

How you will benefit

Optus Managed SSE delivers a comprehensive set of benefits that address the security, operational and financial needs of modern organisations. These benefits collectively enable you to operate confidently in a complex threat landscape, supporting secure digital transformation and business resilience.



Simplify your security:

One central point of contact to manage your security needs – maximise the value of your investment, save time and reduce complexity.



Reduced attack surfaces:

Future-proofed security architecture mitigates evolving cyber threats, reducing risks like lateral movement and data breaches.



Scale with confidence:

The cloud-based nature of the solution allows you to scale security controls as your needs evolve, supporting business growth and digital transformation.



Enhanced security for existing networks:

The solution strengthens the security of SD-WAN and remote access VPNs, ensuring that data and applications remain protected across distributed environments.



Protect your people and data:

Wherever your workforce is, you maintain control and visibility.



Improved compliance and risk reduction:

Enables the consistent and uniform enforcement of security policies, helping you maintain compliance with regulatory requirements and reducing the likelihood of cyber breaches through enforcing granular access controls and authenticating every access attempt.



Improved user experience:

Direct-to-cloud access reduces latency and boosts productivity.



Lower total cost of ownership:

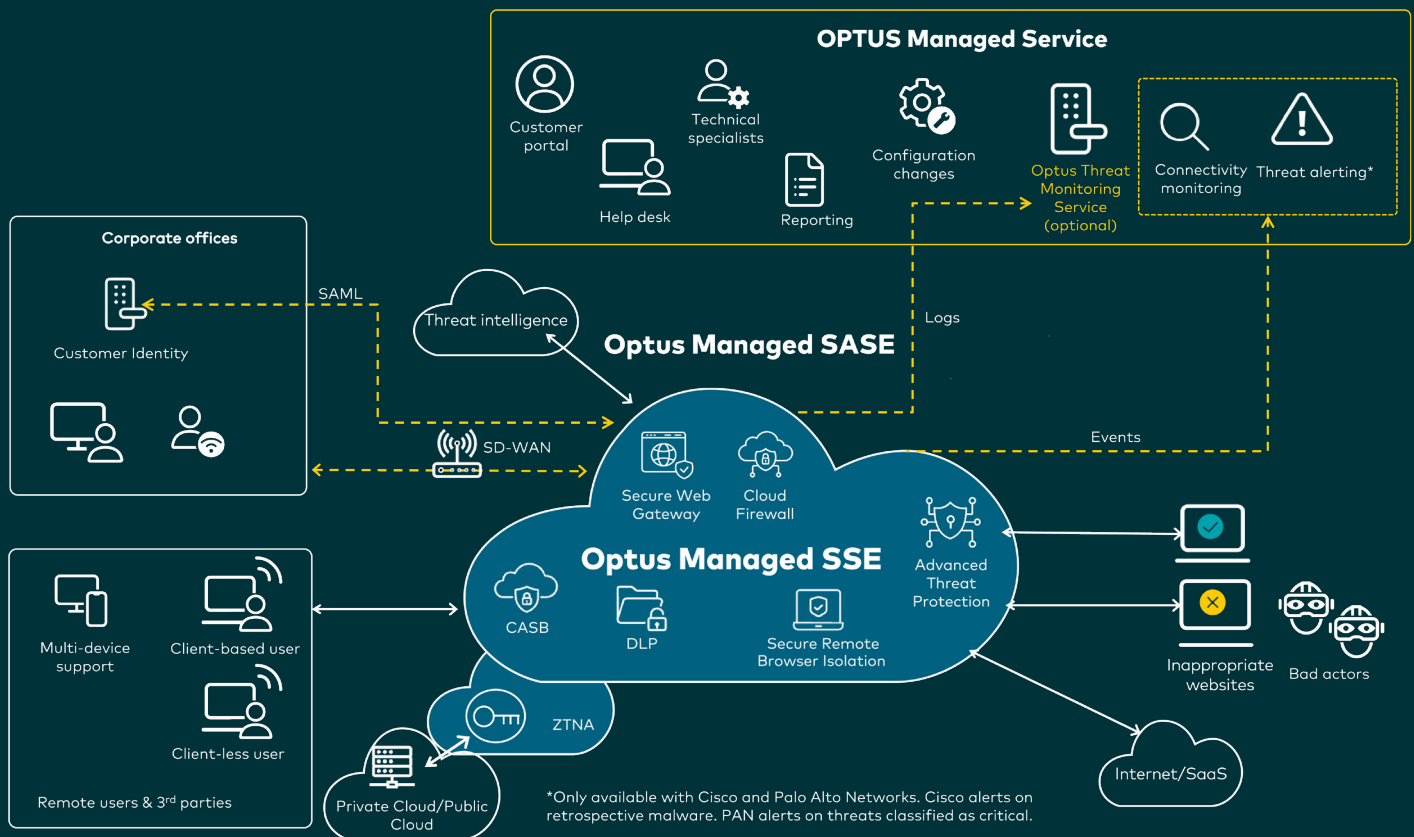
Through the elimination of hardware refresh cycles, patching efforts, disparate licensing and hiring of specialist security resources.



Respond faster to incidents:

Our Australian-based Security Operations Centre (SOC) provides the expertise and automation you need to detect, contain and recover.

How it works



Powered by industry-leading partners – expertly managed by Optus

Integrated into your organisation's networks and systems, Optus Managed SSE is delivered by globally recognised vendors such as Cisco (Secure Connect and Secure Access), Zscaler (ZPA & ZIA), and Palo Alto Networks (Prisma Access) – to deliver unparalleled security performance. And it is seamlessly managed by the expert Optus team who will support and optimise your solution end-to-end and allow your team to focus on other core activities.

Why Optus for Managed SSE



Optus Security Operations Capability

- 24/7 threat monitoring
- Incident, change, and problem management
- Governance, risk and compliance
- ServiceNow & Enterprise One integration
- Real-time feedback loop with customer



Platform Optimisation & Support

- Spot checks and health reports
- Feature enablement and optimisation
- Training and capability refresh
- Product lifecycle and updates



Why Optus

- Tier 1 managed security provider
- Deep operational expertise
- Australian-based support
- End-to-end service, simplified



Interested in Optus Managed Secure Service Edge?

Make security simpler and stronger, with one central point of contact to maximise your investment, save time and reduce complexity.

Request a call back at
optus.com.au/enterprise/contact-us

Visit the product page:
optus.com.au/enterprise/networking-security/security/secure-your-network/managed-security-service-edge

Follow us



yes OPTUS