

Managed Security Service Edge (Palo Alto Networks)

We deliver robust protection for the hybrid workforce, ensuring superior user experience and safeguarding all application traffic with a next-generation security platform

The move to the cloud has exposed limitations in existing security controls. In the past, data was controlled mostly by IT and stored inside a protected perimeter. Remote access to the data was permission-based and almost always through a VPN. Threats were focused on the network and endpoints, with a defined perimeter that IT was able to tightly control access to.

Today, remote use is expected and happens outside of IT's control. The focus is on speed to market, collaboration, sharing, and business enablement, with security lagging behind. As a result, use cases have evolved beyond what legacy tools understand.

Powered by Palo Alto Networks, Telstra Managed Security Service Edge (SSE) with Prisma Access addresses these challenges by providing a cloud-native security solution that understands the new way of working and secure data in a borderless world.



How Can Telstra Managed SSE (Palo Alto Networks) Help to Secure Modern Hybrid Enterprise?



Deliver Great User Experiences

With increased numbers of staff working remotely, IT needs end users to easily and securely connect to wherever resources are located in a seamless manner anywhere, anytime, and at optimum speed.



Reduce Risk and Stay Compliant

Eliminate the attack surface, improve visibility, determine threats before they happen, and remain compliant.



Advanced Security

Telstra Managed SSE (Palo Alto Networks) incorporates advanced application layer inspection to help guard against security threats.



Elastic, Scalable Security

Telstra Managed SSE (Palo Alto Networks) is a scalable, reliable, agile, and cost-effective cloud security solution that offers high performance everywhere, anytime.

Benefits for Modern Hybrid Enterprises



Cost savings through security consolidation and efficiency gains



Increased visibility and control reduces risk of cloud delivered threats



Increased agility enables organisations to move to cloud apps more quickly



Removal of complex architectures and backhauling of traffic improves productivity

Telstra Managed SSE (Palo Alto Networks) Capabilities

Core Services



Secure Web Gateway (SWG)



Advanced URL Filtering



DNS Security



Advanced Threat Prevention



Advanced Wildfire



Zero Trust Network Access (ZTNA) Private App Access

Add-on Services



Cloud Access Security Broker (CASB)



Firewall-as-a-Service (FWaaS)



Email Data Loss Prevention (DLP)



ZTNA Connector



Colo Connect



Autonomous Digital Experience Management (ADEM)#



Enterprise Data Loss Prevention (DLP)



IoT Security^



Traffic Replication



Inline SaaS Security

#Requires Prisma SD-WAN license.
^Only available for remote networks.

We Provide Proactive Managed And Professional Services to Help You Stay Ahead Of Cyber Threats

Managed Services*

- Proactive Maintenance
- Technical Support
- Incident Investigation
- Service and Change Request
- Reporting
- Logging, Monitoring and Event Management

Threat Monitoring Services*

- Security Incident Detection & Response
- Network Security Monitoring
- Threat Intelligence
- Vulnerability Management

Advisory and Assurance Services+

- Security & Threat Assessment
- Regulatory Compliance
- Technical Security Assurance
- Target Operating Model
- Policies & Standards
- Incident Response Readiness
- Cloud Readiness & Security
- Crisis Management
- Security Training Services

*Service availability may vary. Please check with Telstra representative.

+We offer Professional Services as optional add-ons.

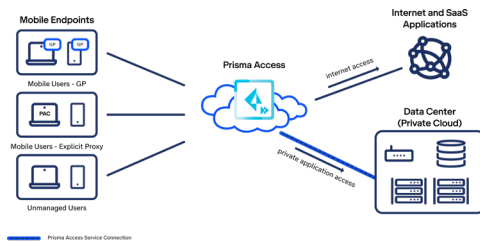
How does Telstra Managed SSE (Palo Alto Networks) Work?

Telstra Managed SSE (Palo Alto Networks) connects all users and apps with fine-grained access controls while providing behaviour-based continuous trust verification after users connect, to dramatically reduce the attack surface. It secures all apps with deep and ongoing security inspection to ensure all traffic is secure without compromising performance or user experience.

Telstra Managed SSE (Palo Alto Networks) Remote

Offers security services such as App-ID, URL filtering, DLP, and threat prevention for mobile users. It is ideal for cloud-first businesses with a remote or mobile workforce.

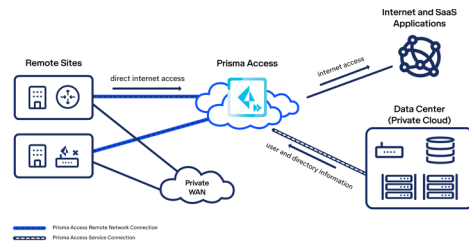
Mobile connection methods include Palo Alto GlobalProtect, Explicit Proxy, and Clientless VPN. Service connections use outbound tunnels to link customer data centers and private applications to Prisma Access.



Telstra Managed SSE (Palo Alto Networks) Cloud

Provides security services such as App-ID, URL filtering, and threat prevention for remote networks and branches, safely enabling commonly used applications and web access. It is ideal for branch-based solutions with or without SD-WAN.

Remote sites can connect to Prisma Access via an IPsec VPN-capable device or Prisma SD-WAN, while service connections use outbound tunnels to link customer data centers and private applications to Prisma Access.



Telstra Managed SSE (Palo Alto Networks) Uses Inline Machine Learning to Protect Against Up to 95% of Unknown Threats

Telstra Managed SSE (Palo Alto Networks) delivers AI-powered cloud Security Web Gateway (SWG) functionality, encompassing DNS Security, Advanced URL Filtering, advanced malware prevention, threat detection, SSL decryption, Data Loss Prevention (DLP), SaaS application control, and more. This next-generation security solution leverages an always-on cloud-native infrastructure, entirely managed by Palo Alto Networks, to operationalise security for today's dynamic business needs.



DNS Security

Machine learning based DNS security detects dynamic DNS-layer threats and blocks them in real-time.

Covers

40%

more DNS-based threats than other leading vendors



Advanced URL Filtering

Utilises inline deep learning to inspect live web traffic, preventing unknown, evasive, and targeted web attacks in real-time.

Detects

40%

more unknown and evasive threats



Advanced WildFire

Advanced WildFire processes over 50M files daily and has 180x faster signature delivery compared to other vendors.

More than

28x

larger than the industry standard threat intel service

*Based on Palo Alto Networks engineering test data and publicly available sources.

Our Approach to Safeguarding Your Business

Our proven consulting methodology has helped global customers to safeguard their business and achieve their desired business outcomes.

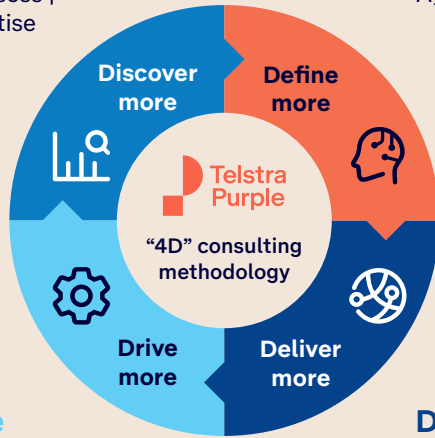
Discover more

Strategise | Assess | Identify | Prioritise

Define more

Agree | Architect | Design | Plan

What we'll do



Drive more

Transition | Manage | Review | Optimise

Deliver more

Build | Migrate | Modernise | Innovate



Logical and pragmatic approach to solution adoption and deployment, helping your business to navigate the complexities of security.



End-to-end solutioning that grows as your business does. Understand your security needs and design tailored services, managed by our experts.



Provide clear visibility of your solution functions and any risks we might encounter along the way.



Contextually-mapped and strategically-built around your specific threat profile to enable swift identification and resolution.

We are the right security partner for your success.

By partnering with Telstra, you gain access to our deep expertise and industry-leading cybersecurity technologies to help protect your business against advanced threats.

We take the complexity out and empower you to innovate, grow, and thrive. Focus on growth with confidence – We got your security covered.

Why Telstra International?

Expertise and Experience



Our deep experience and knowledge of security frameworks such as NIST, GDPR and SOC 2 enable us to design and implement robust and effective solutions that align with your industry, compliance requirements, and risk management objectives.

Strong Alliance Ecosystem



We bring together the strengths of our partner alliances with global technology leaders in our ecosystem to support you.

Proven Consulting Methodology



Our Telstra Purple "4D" Consulting Methodology has helped many global customers to strengthen their security posture.

ISO/IEC 27001 Certified



Our technology, delivery and support processes are certified to the ISO 27001 Information Security Management standard.

Discover how Telstra Managed SSE (Palo Alto Networks) can help you to secure your modern hybrid enterprise 24X7X365.

Contact your Telstra account representative for more details.

telstraenquiry@team.telstra.com

telstrainternational.com