Mastering SASE: Secure, Agile and Scalable Networking for the Future

How to get the most out of SASE with managed services.

Telstra

Unlock the true value of SASE with managed services

What do you get when you add one + one?

When it comes to SD-WAN and SSE, the answer is: Much more than two. Together, they form Secure Access Service Edge (SASE)—a transformative architecture that streamlines and enhances network and security operations.

SASE offers a broad range of advantages to both business and technology teams. Here's how one Forrester study quantified some of the benefits of SASE.

SASE savings

$12.2 million
from improved end-user productivity

$3 million
from reduced Data breach risk

$2.3 million
from increased security and it operations efficiency

$846,000
from security solution consolidation

Source: Forrester. Based on a composite organisation using Forrester's Total Economic Impact™ framework.

Given these substantial benefits, it's no surprise that SASE adoption is accelerating. Gartner projects the SASE market to grow to $25 billion by 2027, with a compound annual growth rate (CAGR) of 29%.

But while the benefits of SASE are clear, the path to realising them is not without challenges. Implementing and managing a SASE solution demands specialised expertise across its lifecycle—deployment, maintenance, and optimisation.

Without expert management, enterprises risk complex deployments, security gaps, and wasted investments. Partnering with a managed service provider (MSP) ensures SASE solutions operate at peak performance and adapt to evolving business needs. These advantages make MSPs an essential partner for enterprises—so much so that 62% of large enterprises and 66% of mid-sized businesses engage MSPs to manage their SASE solutions, according to Frost and Sullivan.

In the following sections, we'll explore the specific challenges enterprises face when managing SASE independently and how MSPs transform these challenges into opportunities for innovation, growth, and resilience.

> **"While SASE promises tremendous technical and business benefits, it is useful to consider a managed SASE services option that has the right technology, process, and expertise. An experienced managed SASE services provider helps to keep companies aware and on top of their performance and business metrics."**
>
> Cathy Huang, Research Director, Worldwide Security Services, IDC
>
> Source: IDC

39%
of organisations have deployed or will deploy SASE in the next 24 months.
Source: Gartner

Overcome resource and expertise constraints

The challenge

Managing a SASE solution requires specialised expertise in both networking and security—a level of skill many in-house teams struggle to maintain amid rising attrition rates and fierce competition for talent. Without the right resources, enterprises face a slew of challenges, including:

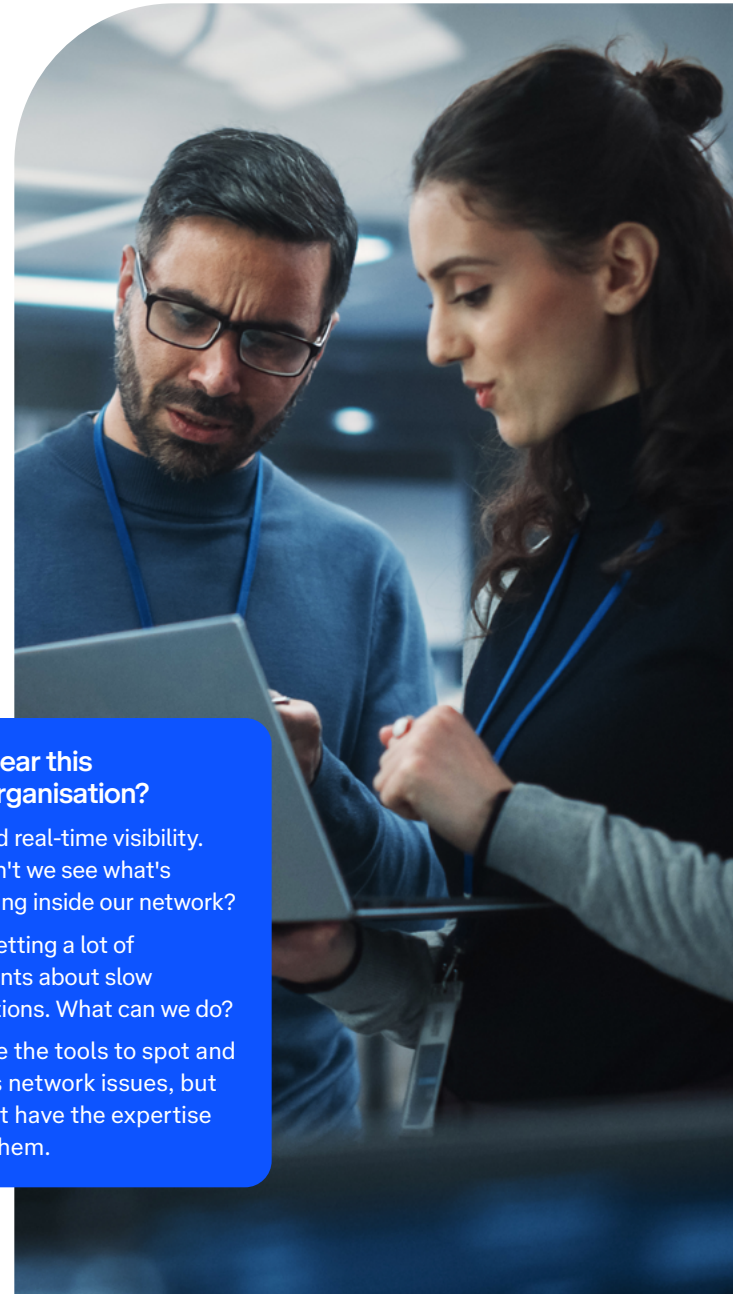
- **Prolonged deployment:** Limited in-house expertise delays the design, integration, and rollout of SASE solutions, which can hamper business agility.
- **Alert fatigue:** A lack of best practices results in poor incident triaging and prioritisation, which overwhelms SecOps teams and increases the risk of missed threats and delayed response.
- **Delayed incident detection and response:** Inadequate staffing and manual workflows impact a SecOps teams' ability to detect and contain threats.
- **Network degradation:** A scarcity of expertise can lead to misaligned network policies, unoptimised bandwidth allocation, and routing misconfigurations, which can result in poor application performance.

Real risks

- **Low ROI:** Poor configuration and oversight prevent enterprises from fully realising the benefits of SASE.
- **Overburdened teams:** Increased workloads lead to burnout and higher attrition. This can make organisation less attractive to top IT talent.
- **Stalled digital transformation:** Insufficient expertise slows multi-cloud adoption, remote workforce enablement, and business and IT automation.
- **Audit failures:** Inconsistent policy results in failed security and compliance audits, which can expose organisations to fines and reputational damage.
- **Missed strategic opportunities:** Poorly managed SASE limits an enterprise's ability to adapt to market changes and seize growth opportunities.

With Telstra managed SASE solution, your organisation can achieve

- Expertise on-demand
- 24/7 Monitoring and incident management
- Proactive resource management
- Streamlined operations with automation
- Continuous improvement with strategic partnership



Do you hear this in your organisation?

- We need real-time visibility. Why can't we see what's happening inside our network?
- We're getting a lot of complaints about slow applications. What can we do?
- We have the tools to spot and address network issues, but we don't have the expertise to use them.

Achieve threat detection and response in real time

The challenge

Enterprises find it difficult to detect and respond to cyber threats in real time, as attacks become faster, more evasive, and increasingly automated. Without the real-time threat monitoring, AI and analytics, and automated response capabilities that managed SASE solutions deliver, enterprises are exposed to significant risks, including:

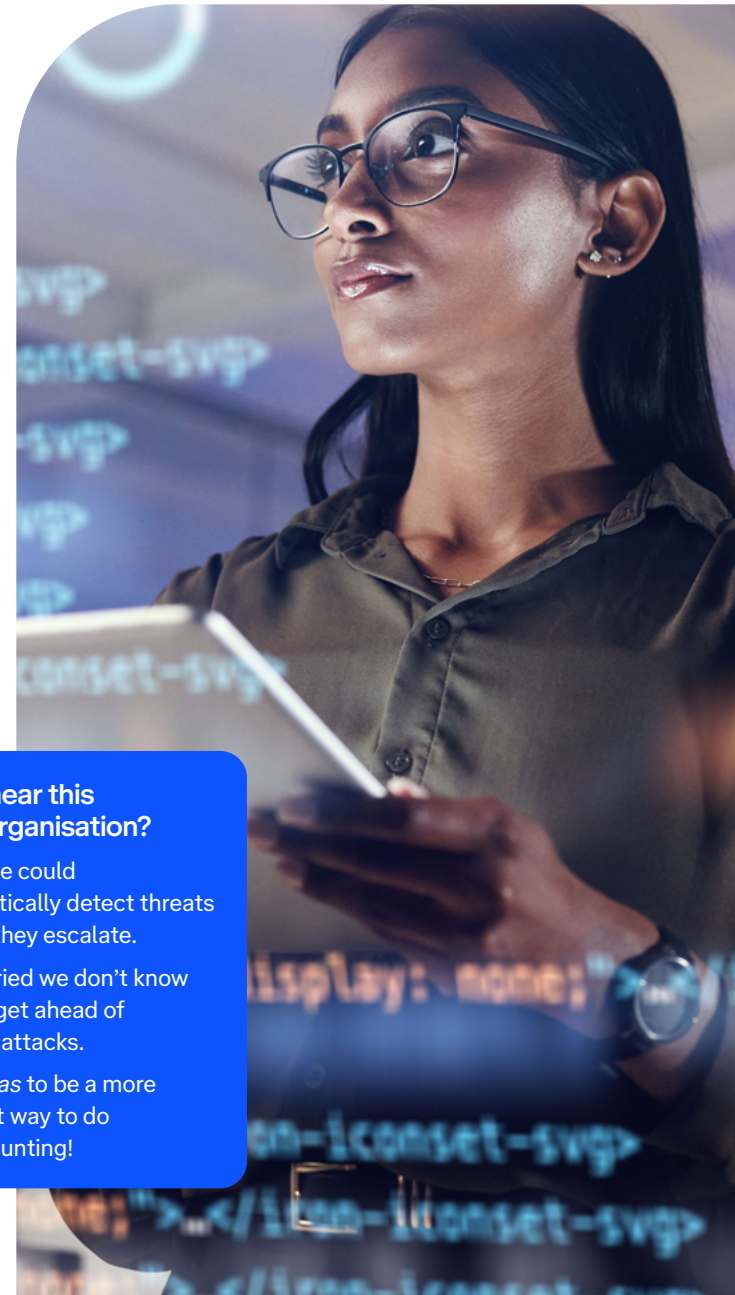
- **Alert overload:** High alert volumes, manual triaging, and the challenge of distinguishing true threats from false positives overwhelm SecOps teams, which leads to missed threats.
- **Visibility gaps:** Siloed security tools and fragmented telemetry prevent threat correlation across cloud, network, and remote environments.
- **Undetected threats:** Gaps in real-time correlation and attack signal analysis fail to detect zero-day exploits—such as those enabled by the Log4j (an open source Java logging framework) vulnerability.
- **Delayed investigations:** Manual log and IOC (indicators of compromise) correlation hinder threat hunting and lead to slow responses.
- **Slow threat containment:** A lack of automation delays mitigation efforts, which increases the risk of lateral movement—as seen in the NotPetya attack—and facilitates the spread of ransomware.
- **Encrypted threats:** Attackers use TLS (Transport Layer Security) encryption, fileless malware, and obfuscation techniques to evade detection.

Real risks

- **High recovery costs:** Ransomware attacks incur significant recovery costs and force organisations to invest heavily in system restoration and data recovery.
- **Reputational damage:** Data breaches and compliance failures erode customer trust and brand credibility.
- **Regulatory penalties:** Non-compliance with regulations result in fines and lawsuits.
- **Intellectual property theft:** Cyber espionage and data exfiltration expose trade secrets and sensitive business information.
- **Operational disruptions:** Cyber incidents, such as DDoS and phishing attacks, can lead to significant downtime and lost productivity.

With Telstra managed SASE solution, your organisation can achieve

- 24/7 Managed security operations
- Unified security analytics and telemetry correlation
- AI-driven threat intelligence
- Automated threat hunting and incident response
- Full TLS decryption and encrypted traffic analysis



Do you hear this in your organisation?

- I wish we could automatically detect threats before they escalate.
- I'm worried we don't know how to get ahead of evasive attacks.
- There *has* to be a more efficient way to do threat hunting!

Ensure consistent Zero Trust security across the enterprise

The challenge

Zero Trust security demands constant validation of user, device, and workloads across cloud, on-premises, and hybrid environments. However, traditional security models rely on static access policies, rather than continuous, risk-based authentication and least-privilege enforcement. Without a well-managed Zero Trust approach, security teams face:

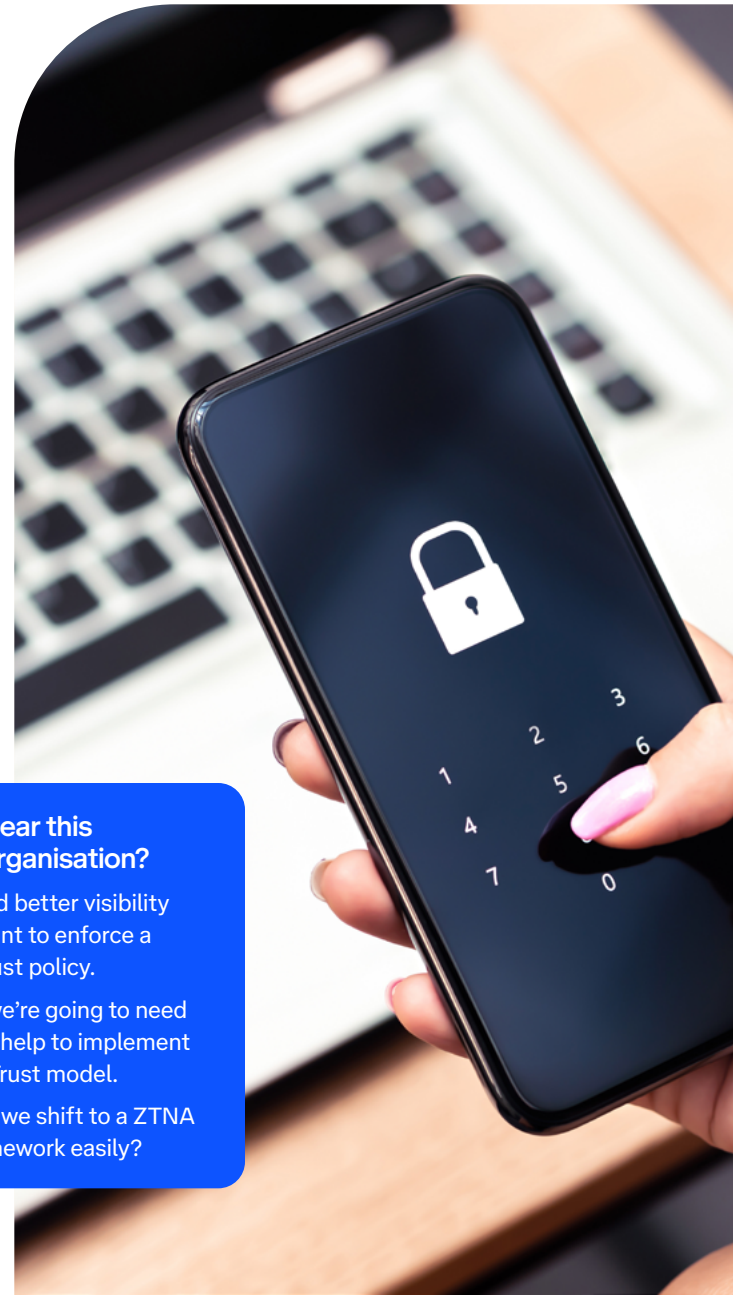
- **Gaps in continuous verification:** Static authentication grants persistent access, even if a user or device is compromised, which allows attackers to escalate privileges.
- **Failure to prevent lateral movement:** Without microsegmentation, attackers leverage static access policies to move laterally and compromise sensitive systems.
- **Lack of adaptive access controls:** A failure to adjust to risk in real time increases exposure to account takeovers and privilege abuse.
- **Visibility gaps:** Fragmented data across SaaS, private applications, and workloads, compounded by static access policies, make it hard for SecOps teams to detect anomalous activities.
- **Operational complexity:** Without automation and centralised orchestration, managing Zero Trust policies across users, networks, and applications burdens SecOps teams.

Real risks

- **Data exposure:** Attackers can steal data and move laterally, which leads to financial losses and regulatory penalties.
- **High cyber insurance costs:** Increased breach risk raises cyber insurance premiums and limits coverage options.
- **Customer churn and opportunity costs:** Security-sensitive industries require Zero Trust compliance. Poor enforcement leads to lost contracts, customer churn, and failure to enter regulated markets.
- **Risks to leadership team:** In some countries, enterprise leaders risk civil penalties or even criminal charges if Zero Trust failures cause breaches.

With Telstra managed SASE solution, your organisation can achieve

- Identity-centric access control and continuous authentication
- Least-privilege access and adaptive policy enforcement
- Cloud-delivered microsegmentation and traffic inspection
- Automated policy orchestration and centralised enforcement
- Real-time threat prevention and inline security controls
- Unified security analytics and telemetry correlation



Do you hear this in your organisation?

- We need better visibility if we want to enforce a Zero Trust policy.
- I think we're going to need outside help to implement a Zero Trust model.
- How do we shift to a ZTNA 2.0 framework easily?

Leverage automation for faster, more accurate operations

The challenge

Manual SecOps and NetOps workflows introduce delays, human errors and operational inefficiencies. This increases security risks and compliance challenges and impacts network performance and business agility. Without the AI and automation expertise a managed provider offers, enterprises struggle with:

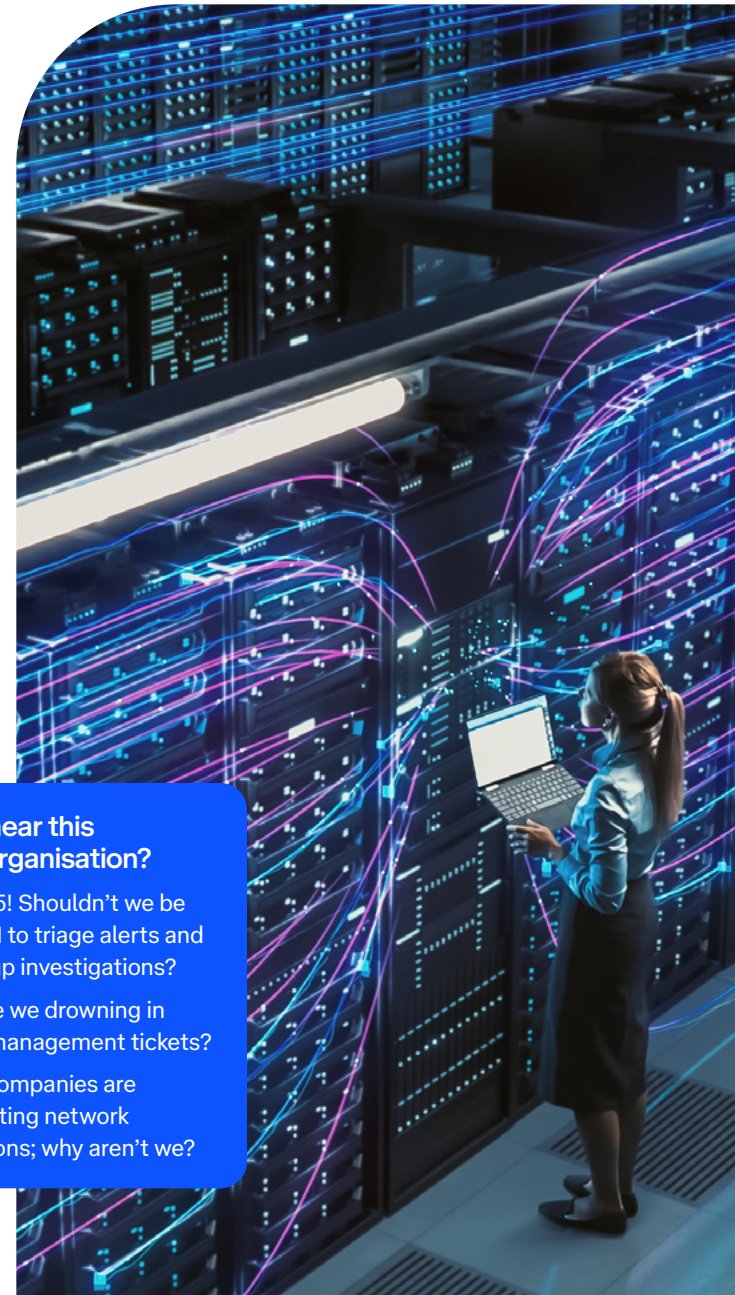
- **Policy enforcement gaps:** Manually configuring network and security policies leads to delays, inconsistencies, and misconfigurations. As organisations grow, manual policy management creates policy drift and a poor ability to scale branches, workloads and users swiftly.
- **High MTTD and MTTR:** Manual incident triaging, event correlation, investigations, and response workflows extend MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond). This allows threats to go undetected, persist longer, spread laterally, and burden SecOps and NetOps teams.
- **Network performance degradation:** Manually configuring traffic routing, bandwidth allocation, and security policies results in operational overhead, inefficient resource utilisation, latency, and poor SaaS performance.

Real risks

- **Increased security risks:** Inconsistent policies, misconfigurations, and inefficient security operations expose enterprises to cyberattacks and insider threats. Longer containment times increase breach impact, which raises financial and recovery costs.
- **Loss of competitive advantage:** Organisations that leverage AI and automation can adapt to changing business conditions faster and scale more efficiently. This gives them an edge over enterprises reliant on manual NetOps and SecOps.
- **User dissatisfaction:** Security blind spots and network inefficiencies lead to poor customer experience, lower employee productivity, and a loss of partner trust.
- **Rising costs:** Manual workflows increase IT overhead, delay troubleshooting, lead to inefficient resource allocation, downtime, and latency, and undermine business profitability.

With Telstra managed SASE solution, your organisation can achieve

- Automated network and security policy orchestration
- AI-powered network optimisation
- Accelerated incident resolution with ai-driven playbooks
- Faster, more efficient onboarding and scaling of users, branches, and workloads
- AI-enabled and automated threat detection, investigation, and response



Do you hear this in your organisation?

- It's 2025! Shouldn't we be using AI to triage alerts and speed up investigations?
- Why are we drowning in policy management tickets?
- Other companies are automating network operations; why aren't we?

Anchored in success

How Telstra delivered reliable and scalable connectivity and security to a market-leading shipbroker.

Rough seas

As one of the world's leading shipbrokers, this London-headquartered enterprise facilitates the chartering of ships and freight contract negotiations, which makes it critical to global supply chains.

But cracks in its network infrastructure slowed it down. Less-than-optimal connectivity led to frustrating user experiences, while an aging firewall estate left it increasingly vulnerable to security threats.

It urgently needed a future-proof solution to ensure reliable global connectivity and strengthen its security posture.

Charting a new course

Telstra delivered a full-stack single-vendor managed SASE solution. It combined its professional expertise and managed services to address immediate challenges and long-term objectives.
Core components included:

- Deploying a cloud-managed SD-WAN solution to deliver reliable, high-speed connectivity across all 15 global offices.
- Implementing a cloud-delivered SSE platform to give employees secure, anytime access to critical cloud applications and resources.
- Introducing a digital experience monitoring solution to identify potential network issues early and optimise traffic flows, which significantly improved user experience.

Smooth sailing

With Telstra's expertise and robust managed SASE solution, the shipbroker achieved:

- Greater productivity from reliable connectivity, which shrank disruptions and network degradations and ensured application uptime and uninterrupted data transfers.
- Enhanced security powered by a unified framework that defends against sophisticated cyber threats and supports secure, remote work from any location.
- Improved efficiency through proactive monitoring and real-time insights.
- Faster time-to-value by seamlessly integrating the solution with existing WiFi infrastructure, LANs, and data centres.
- Future-ready scalability that empowers the shipbroker to support growth and maintain peak network and security performance.

Telstra Managed SASE: Security, Agility, Simplicity, Expertise

Telstra's comprehensive consulting and managed SASE solution combine the latest technology, deep expertise, proven best practices, and global infrastructure to help enterprises deploy, run and optimise SASE architecture.

Scalable expertise
Telstra's team of certified specialists, located globally, provides 24x7x365 support with committed SLA. They deliver real-time anomaly detection, proactive incident resolution, hands-on management, and continuous optimisation of SASE deployments.

Global reach
Telstra's extensive global presence ensures seamless, high-performance connectivity wherever businesses operate. With one of the largest subsea cable networks in the Asia-Pacific region and robust data centre partnerships worldwide, Telstra delivers consistent service quality and reliability across the globe.

Flexible, tailored solutions
Telstra offers the flexibility to choose between single-vendor and dual-vendor SASE solutions, with options for fully managed or co-managed models.

Critical incident management
Telstra's High Priority Impact Management Team specialises in addressing unplanned emergency outages. Backed by over a decade of experience, the team delivers swift resolutions or effective workarounds, which minimises downtime and ensures business continuity.

Strategic partnerships
Telstra's extensive ecosystem of partners includes global technology leaders across networking, security, and cloud services. From Palo Alto Networks to VMware by Broadcom, Cisco, Netskope, and more, Telstra incorporates advanced technologies to deliver SASE solutions that are innovative, scalable, and aligned with business goals.

Telstra offers both single-vendor and dual-vendor managed SASE solutions

- **Single-vendor managed SASE:**
  Our single-vendor approach offers a pre-integrated SD-WAN and security solution from a single technology provider, ensuring seamless compatibility, simplified management, and consistent security policies. With a single interface and centralised control, enterprises can reduce complexity and streamline operations. Ideal for enterprises seeking a turnkey solution with maximum compatibility across different SASE components.
- **Dual-vendor managed SASE:**
  Our dual-vendor approach allows enterprises to combine best-of-breed SD-WAN and SSE technologies from different vendors, allowing them to avoid vendor lock-in. This solution is suited for businesses that want the ability to choose specialised solutions for networking and security.

Reimagine what your network can do

Your network is more than infrastructure—it's the foundation of innovation, agility, and growth. Telstra's Managed SASE solution combines unmatched expertise, global reach, and advanced technologies to optimise operations, secure data, and scale for the future.

Whether you are addressing today's challenges or planning tomorrow's opportunities, Telstra is here to partner with you.

Discover how you can secure your enterprise 24x7x365 with Telstra.

Explore Now

Let's build a secure future. Schedule a free managed SASE consultation today.

Request a Callback

Telstra