For IT, Network and Security Leaders

From AI bottleneck to AI enabler: Build your case for Managed SASE



Telstra

AI agents are growing rapidly

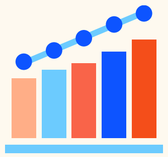
Your network and network security have to keep up



95%

of enterprises run at least one AI agent workflow in production, averaging 11 agents.

Agentic AI is already putting more pressure on enterprise networks and security.



80×

active AI agents are forecast to grow from 31 million to 2.5 billion by 2030.

Agentic AI will generate more dynamic traffic and expand network interactions as adoption grows.



37%

of organisations with network-related delays in AI projects say network security is the cause, ahead of automation and staffing.

Network security is already holding AI projects back.



70%

of enterprises cite increased network connectivity requirements as a top infrastructure impact of expanding agentic AI.

The network is becoming a bottleneck to scaling agentic AI.



37%

of organisations saw bandwidth grow by more than 50% in the past year.

AI workflows are creating more unpredictable demand and traffic across applications, clouds, and sites.

Source: IDC Analyst Brief Secure Enterprise Networking as AI Starts to Act: The Why and How of SASE, October 2026

Agentic AI exposes three gaps in networking and security architecture

IDC identifies three gaps that organisations need to close as agentic AI expands. Each one connects to a key priority for the CIO, CISO or Network Leaders, the key stakeholders who shape the business, security, and architecture decisions behind Managed SASE.



CIO | The visibility gap

Can we trace an AI workflow from start to finish?
Identity, network, application and security systems each hold only part of the record, making it harder to see and trace the complete AI workflow.



CISO | The identity gap

Who, or what, is acting, and on whose authority?
As AI agents interact with more applications, cloud services and data, organisations need consistent security controls and visibility across increasingly autonomous traffic.



Network Leaders | The traffic gap

How do we control new traffic paths without slowing them down?
AI workflows create new paths across clouds and services, making it harder to maintain consistent controls without compromising performance.

How SASE helps close the three gaps

SASE brings networking and security together, helping organisations apply policy consistently across distributed AI workflows while maintaining performance and accountability.

Visibility



Use identity and delegation context to find out who or what is acting on whose authority

Understand whether a person, machine or AI agent is acting, whose authority is being used, and for what purpose, to ensure the right policy can be applied.

Identity



Apply consistent controls across new traffic paths without slowing them down

Apply the same controls across cloud-to-cloud and agent-to-agent traffic without forcing everything through a central choke point.

Traffic



Connect identity, path and policy evidence to trace an AI workflow from start to finish

Link who initiated the activity, whose authority the agent used, which path it followed and which resources it accessed to track and trace the full AI agent sequence.

Why organisations are moving to a Managed SASE model

34%

of APAC organisations have implemented or are piloting an integrated SASE framework.

57%

of APAC organisations are planning to implement an integrated SASE framework through 2026–27.

40%

of APAC networking teams use five or more portals to manage network operations, resulting in a fragmented and incomplete view.

Source: IDC Analyst Brief Secure Enterprise Networking as AI Starts to Act: The Why and How of SASE, October 2026

What is holding organisations back:

- Legacy network and security stacks that do not share context easily
- Incomplete identity coverage for non-human actors
- Skills gaps in operating a converged environment



How a Managed-Service Partner accelerates your SASE progress

Tested assessment and migration playbooks
Bring repeatable methods across assessment, architecture, migration and deployment.

Integration of the existing environment
Integrate existing network and network security investments rather than starting again from scratch.

End-to-End operational responsibility
Manage enterprise network and network security infrastructure under a single managed-services model, reducing hand-offs and strengthening accountability for performance and policy enforcement.

Making the case for Managed SASE across three key stakeholders

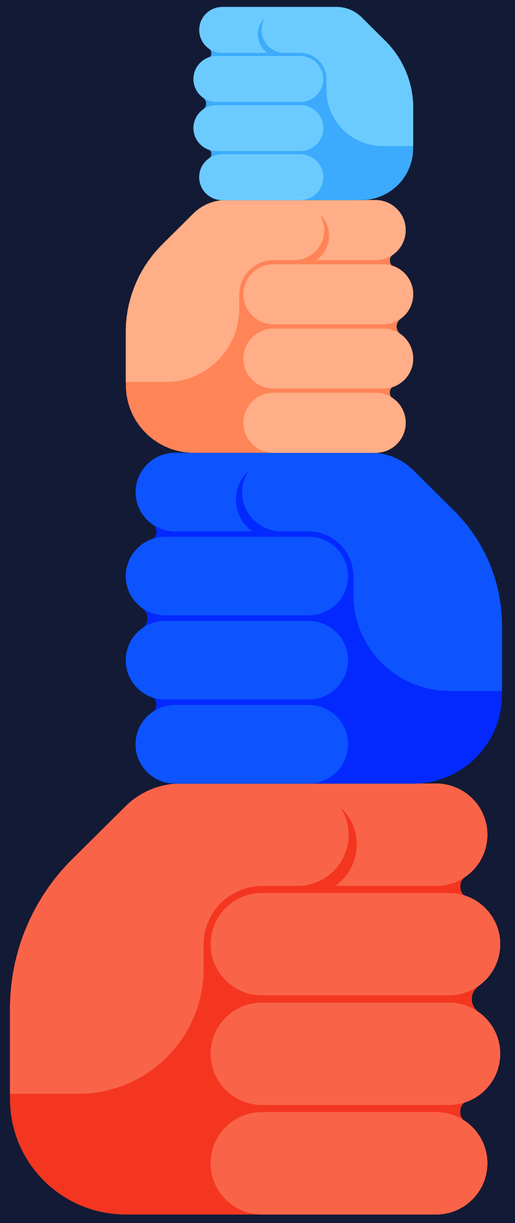
As Agentic AI scales, moving Managed SASE forward requires buy-in from the CIO, CISO and Network Leaders, each with different priorities and decision criteria. Explore the challenges that matter most to each, and how to position Managed SASE accordingly.

72%

of SSE and SASE buying decisions now involve both network and security teams

up from 57% in 2024.

Source: IDC Analyst Brief - Secure Enterprise Networking as AI Starts to Act: The Why and How of SASE, October 2026





The CIO POV

Three challenges CIOs face as AI scales

01

I’m scaling AI across an environment that’s already fragmented

AI workflows now span clouds, applications, sites and services. When network and security are still managed separately, every new AI use case increases complexity.

02

If our network slows down, so does our AI

AI depends on cloud-to-cloud traffic, repeated API calls and reliable, low-latency connectivity. When network performance suffers, AI performance suffers too.

03

My team can’t grow as fast as our AI workload

More agents, applications and policy changes mean more monitoring, incidents and providers to coordinate. The workload grows as AI expands.

Making the case for Managed SASE to the CIO

Talk to the CIO about what AI needs to scale

	 **Lead with cost and complexity**	 **Connect network performance to AI performance**	 **Position 24/7 operations as added capacity**
The problem	Every new AI use case adds to an environment that's already fragmented.	If the network slows down, so does AI.	My team can't grow as fast as our AI workload.
Say it like this	Every new AI use case adds more hand-offs between separate network and security providers. One managed service takes that coordination off our plate and visibility into costs we can plan around.	Our AI workloads depend on fast, reliable connections between clouds, apps and sites. Managed SASE sends each application down the best available path and keeps traffic moving if a link fails.	More agents means more alerts, more incidents and more providers to chase. A managed service watches the environment around the clock and gives us one team accountable for fixing issues, wherever they start.
Back it up with	One provider and one contract from underlay to SSE, with a standard SLA across network and security.	Application-aware routing, dynamic path selection, traffic prioritisation and WAN resiliency, with Digital Experience Monitoring to show it's working.	24/7 L1–L3 expert operations, defined L4 vendor escalation and a dedicated customer manager.



The CISO POV

Three challenges CISOs face as AI scales

01

AI agents are creating new access paths to applications and data

AI agents can connect to applications, services and data across cloud and private environments, creating more connections that security teams need to protect.

02

I need security controls to keep pace with AI agents

AI agents can interact with multiple systems at machine speed. Security policies need to be applied consistently as traffic moves between users, agents, applications and services.

03

Sensitive data is moving along more paths that I can effectively control

AI workflows can move data across SaaS platforms, AI providers, clouds and sites, including paths that may not pass through the organisation’s traditional web gateway or inspection controls.

Making the case for Managed SASE to the CISO

Show the CISO where control gets stronger

	Apply identity context to AI-driven connections	View and secure AI-driven traffic	Make it clear the CISO stays in charge
The problem	AI agents are creating more paths to applications and sensitive data, making access harder to control.	I need security controls to keep pace with AI-driven traffic.	As more network and security operations are managed for us, how do I retain control?
Say it like this	AI agents can connect across applications, cloud services and data. Managed SASE can use identity context from existing identity systems to apply security policies to those connections and traffic.	As AI agents interact across applications and services, Managed SASE brings network and security visibility together, helping security teams see traffic patterns and apply consistent controls.	You keep ownership of the business and risk decisions. The provider applies the policy you approve and reports back on how the service is performing.
Back it up with	SSE delivered alongside SD-WAN and underlay by one provider, under one operating framework.	One view across network and security, with real-time analytics and path metrics.	An SLA-backed service, with shared processes across network and security.



The Network Leader's POV

Three challenges Network Leaders face as AI scales

01

AI traffic no longer follows the network paths I designed

One workflow can generate many calls across applications, AI services, clouds and sites, creating more traffic and a wider range of paths for network teams to manage.

02

I'm having to choose between performance and consistent control

Backhauling traffic through a central firewall adds delay. Sending it directly shortens the path but applies a different set of controls, forcing a trade-off between performance and consistent enforcement.

03

Our existing network and security setup makes SASE migration more complex.

Most organisations already have SD-WAN, security platforms and connectivity in place. Moving to SASE means dealing with an installed mix of technologies, providers and policies, which can make migration complex.

Making the case for Managed SASE to Network Leaders

Show Network Leaders how to move forward without starting over

	 **Show how to stay in control of unpredictable traffic**	 **End the trade-off between performance and control**	 **Show how existing investments carry forward**
The problem	AI traffic no longer follows the network paths I designed.	I'm forced to trade performance for consistent control.	Our existing network and security setup makes SASE migration more complex.
Say it like this	We can't predict every path an AI workflow will take, but we can see them. Managed SASE gives us one view across the underlay, the SASE platform and the application, and lets us choose paths based on what each application and site needs.	We no longer have to backhaul traffic through a central firewall to keep controls consistent. The same security policy applies wherever traffic starts, so we can take the direct route without opening a gap.	We don't have to rip out what we've built. Our current SD-WAN and security can be brought into the SASE architecture using tested assessment and migration playbooks.
Back it up with	Real-time analytics, path metrics, Digital Experience Monitoring and application insights.	Underlay, SD-WAN and SSE from one provider, managed under one operating framework.	Lifecycle management, end-of-life tracking and refresh planning once the service is live.

6 reasons to choose Telstra Digital Infrastructure for Managed SASE



One provider, from underlay to SSE
Underlay, SD-WAN and SSE under one contract and one operating framework, with shared processes and a standard SLA across network and security.



One accountable team, measured on outcomes
A dedicated customer manager owns updates, escalations and outcomes, backed by SLAs and continuous service improvement.



24/7 operations and support
L1–L3 expert operations around the clock, with defined L4 vendor escalation, so your team isn't left coordinating providers when something breaks.



Future-proofed by design
Lifecycle management, end-of-life tracking, refresh planning and regular capability reviews keep your service current as your AI use grows.



Single pane of glass view of performance
Real-real analytics and Digital Experience Monitoring provide visibility into network and application performance.



Reach that matches your footprint
Australia's largest connectivity network, linking Australia to Asia Pacific and the world, with operations in over 19 countries.

Network and network security, managed as one, wherever you operate
Telstra Digital Infrastructure brings both together under one provider and one accountable team, with 24/7 expert operations behind it. As AI scales, your network keeps pace.

Ready to make the case for Managed SASE?

Bring your CIO, CISO and Network Leaders into one conversation with a Telstra Digital Infrastructure Managed SASE specialist.

Reach out to a Managed SASE specialist



Learn more about our Managed Network Services here.

About Telstra Digital Infrastructure
Telstra Digital Infrastructure is Telstra's integrated digital infrastructure business, delivering end-to-end digital infrastructure solutions across Australia and international markets. Through an extensive portfolio of fibre, duct, subsea cable, data centre, tower, satellite infrastructure and engineering services, we provide the connectivity, platforms and services that underpin business growth, digital transformation and the evolving demands of the AI economy.

Combining deep technical expertise, decades of operational experience and a long history of supporting customers across Australia, Asia-Pacific and beyond, we connect businesses, markets and communities through secure, reliable and high-performance digital infrastructure.

Telstra