Prepared for
Data#3

From Fragmented to Future Ready: The Managed SASE Advantage in Australia

June 2025 EMA White Paper
By Shamus McGillicuddy, Vice President of Research
Network Infrastructure and Operations

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Contents

Foreword: The smarter way to SASE

Richard Dornhart – National Practice Manager for Security, Data#3 Limited

At Data#3, we speak to security and IT leaders every day who are feeling the pressure of protecting a hybrid workforce, navigating tightening compliance standards, and managing fragmented technology environments. SASE (Secure Access Service Edge) provides a powerful framework to address these challenges, but as this EMA research shows, adopting SASE is often more complex than expected.

Many businesses face roadblocks: limited in-house skills, fragmented toolsets, and the burden of compliance. That's why more are choosing the **managed path to SASE** — not just to simplify deployment, but to reduce risk and accelerate value.

At Data#3, we've developed our **Managed Secure Edge Access service, powered by Cisco**, to do just that. With Cisco's global leadership in networking and security, combined with our mature, nationally scaled managed services operation, we help customers implement SASE right from day one. We handle the complexity, ensure local compliance, and deliver continuous performance and protection.

SASE is a powerful foundation for a more unified, adaptive, and secure future. We hope this paper helps guide your thinking and, more importantly, sparks the kind of conversations that move your security strategy forward.

Hybrid Work Forces Australian Companies to Address Cyber Risks

Today's Australian companies employ an increasingly hybrid and remote workforce, with 69% of Australian employers offering hybrid work arrangements[1] and 3.8 million Australians reporting that they usually work from home.[2] These companies are making significant technology investments to maintain productivity by providing remote employees a flexible and optimal digital experience regardless of location. At the same time, they must secure those digital experiences from malicious actors who have recognised remote work as an enticing attack vector.

With millions of Australians accessing their employers' digital assets from home, companies are facing an existential security risk. Hacking-as-a-service is experiencing rapid growth, and cybercriminals are leveraging artificial intelligence to enhance their attacks.

The potential cost of this threat environment is immense. In 2024, the average data breach in Australia cost A$4.26 million,[3] privacy laws are driving much of these costs. For egregious data breaches, Australian privacy laws now impose penalties that can exceed A$50 million. For less serious breaches of specific Australian Privacy Principles, penalties can reach A$300,000 for corporations and A$66,000 for individuals. Failure to comply with mandatory data breach notification requirements can also result in fines up to A$2.1 million for businesses and A$420,000 for each director. Moreover, reputational damage and loss of customer trust can cripple a company's efforts to recover from a breach.

[1] https://www.localdigital.com.au/blog/remote-work-statistics-in-australian-companies-for-2025

[2] https://www.abs.gov.au/statistics/labour/earnings-and-working-conditions/characteristics-employment-australia/aug-2024

[3] https://itbrief.com.au/story/australia-s-data-breach-costs-hit-record-aud-4-26m

To support a hybrid workforce, Australian companies need a unified security policy, zero trust access, comprehensive protection from emerging threats, and connectivity technology that delivers an optimal quality of experience. Many companies have reacted tactically to this shift to hybrid work by adopting multiple technologies from different vendors. This approach leads to increased costs and sprawling toolset complexity. Smaller Australian organisations often discover that they lack the engineers and architects needed to implement and manage these security tools effectively.

SASE Offers Australian Companies a Better Option

SASE is a smarter, all-in-one solution that helps businesses connect and protect their networks more effectively. It brings together tools that choose the best path for internet traffic (so things run faster and smoother), block dangerous websites, keep an eye on how cloud apps are being used, protect against online threats, control who can access what, and make sure no one gets in without proper checks. All of this is delivered through the cloud, making it easier to manage, more affordable, and more secure, especially for teams working from many different locations.

Business and technology leaders clearly recognise the opportunity to solve these challenges with SASE. Research shows that SASE adoption is growing rapidly in Australia today, and that growth will continue to be strong over the next six years.[4] However, despite the promise of this architecture, SASE implementation can be challenging.

[4] https://www.6wresearch.com/industry-report/australia-secure-access-service-edge-sase-market

The Complexity of SASE Adoption in Australia

While SASE holds great promise, many companies face challenges with adoption. Australia's unique data sovereignty and industry compliance requirements contribute to this delay. Off-the-shelf solutions from global SASE providers are built for broad use across geographies. Vendors don't necessarily tailor them to the compliance needs of Australian companies.

Despite SASE's ability to unify networking and security, implementing the technology is also complex. SASE combines multiple networking and security technologies that must be integrated into an existing architecture. Many IT infrastructure and operations personnel and cybersecurity personnel don't have the capacity or the necessary experience to take on this complexity. In fact, 37% of early SASE adopters say integrating SASE component technologies is a major challenge to their adoption of the technology.[5]

How Managed SASE Overcomes Challenges

Today, 66% of companies prefer a managed solution for SASE.[6] IT leaders tell EMA that they seek managed SASE services for many reasons. First, a managed SASE offering comes with a service level agreement (SLA) that provides assurances around resiliency and response times. Second, providers of managed services can offer deep Integration with the other managed services that a company is already consuming, ensuring a strong end-to-end networking and security architecture.

Cost is a major factor, too. Managed SASE solutions allow Australian companies to avoid large capital expenses for the SASE hardware and perpetual software licenses. Finally, buyers tell EMA that managed service providers remove deployment

[5] EMA, "WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success," April 2023.
[6] Ibid.

complexity. An Australian provider of SASE services will be especially valuable in helping a customer implement a solution that addresses the country's data sovereignty and compliance requirements.

Identifying the Ideal Managed Offering

To realise the full value of SASE, Australian CISOs and IT leaders should seek out managed services partners with capabilities tailored to local needs. Decision-makers should look for the following capabilities:

- **Regulatory readiness.** The SASE partner should have a deep understanding of Australian data sovereignty laws and compliance requirements.
- **Integrated, comprehensive technology platform.** Buyers should seek a SASE solution with robust capabilities. It begins with an SD-WAN foundation that delivers a high-performance network by leveraging features like WAN remediation, acceleration, and optimal path selection. This foundation should integrate with a full suite of security capabilities, including NGFW, SWG, CASB, DLP, and ZTNA, to ensure that SASE can protect companies from new and emerging threats.
- **Appropriate coverage.** The SASE technology must also ensure optimal user experience by delivering network and security services from true points of presence in every location where the company does business.
- **Cloud-native.** The SASE technology must support any WAN edge scenario with a platform that is truly multi-tenant and cloud scalable. This ensures that the managed services partner can customise a SASE solution that meets each customer's specific requirements.
- **Centralised management and policy control.** The SASE platform should offer a central, cloud-based management console that ensures efficient and effective management of networking and security. This central controller should leverage advanced analytics and observability to enable efficient and effective operations across SASE and legacy infrastructure.

- **The right partners.** Every company should evaluate the reputation of the managed services partner and the SASE vendor it works with. Buyers should seek vendors and partners that have a track record of delivering effective solutions with 24/7 support and the ability to scale as a business grows. The solution should offer best-of-breed technology across all elements of the SASE architecture, from the SD-WAN foundation to the multitude of security solutions integrated into the platform. And the managed services partner should have a track record of delivering solutions to Australian companies.

EMA Perspective

The long-term trend toward hybrid and remote work in Australia will force companies to modernise their networking and security solutions to ensure employees can securely access cloud applications with an optimal quality of experience. SASE technology can transform and optimise infrastructure for this new era, but many Australian companies are still navigating the best way to adopt this complex technology. EMA research shows that success hinges on partnering with experienced managed service providers rather than attempting DIY deployments.

Selecting the right managed SASE service is critical. Organisations should prioritise solutions built on a comprehensive, cloud-native platform from a trusted vendor—one that integrates networking and security seamlessly, offers strong policy enforcement, and provides deep visibility and analytics.

SASE is no longer optional; it’s a strategic necessity for securing the hybrid and distributed workforce. When you’re ready to advance your SASE journey, engage with your trusted managed services partner to ensure a smooth, secure, and future-proof transition.

About Data#3

Data#3 Limited (ASX: DTL) is Australia's leading IT services and solutions provider, delivering the technology, expertise, and managed services organisations need to modernise, secure, and thrive in a digital-first world.

Through a dedicated cybersecurity practice, Data#3 help customers protect their people, data, and operations with an integrated portfolio of solutions across Managed Security Services, Secure Edge Access (SASE), Extended Detection and Response (XDR), and Zero Trust strategies, all supported by a nationally scaled, ISO-certified service operations.

As a Cisco Gold Partner and Cisco APJC Customer Experience Partner of the Year for 2023 and 2024, Data#3 is a trusted partner for organisations seeking secure networking solutions. Data#3 managed services are relied on by organisations across all industries, including government, education, health, and commercial sectors, to reduce complexity, improve visibility, and maintain a strong security posture in a rapidly evolving threat landscape.

With over four decades of experience and a strong track record of delivery, Data#3 combines global technology leadership with deep local expertise to help customers get the most from their IT investments, now and into the future.

Learn more at **data3.com**.

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.