

Secure your future

Why a Strategic SASE Approach is Non-Negotiable

Executive Summary

The convergence of hybrid work, widespread cloud adoption, and the undeniable rise of AI have permanently transformed the enterprise landscape. Your network, once a foundation, is now a critical differentiator — or significant liability.

With more users, devices, and data to manage, organizations that have historically used a patchwork of point solutions to solve security and networking challenges are facing unmanageable complexity, amplifying risk and impeding critical business transformation initiatives. This isn't just an IT challenge; it's a strategic bottleneck impacting innovation, operational efficiency, and your competitive posture.

In a rapidly evolving digital economy, speed to market and agility are paramount. Attempting to build and integrate this complex expertise internally can delay critical initiatives and erode competitive advantage.

The answer lies in a unified Secure Access Service Edge (SASE) architecture. Yet, merely adopting SASE technology isn't enough. True transformation demands a holistic, forward-thinking strategy — one that not only delivers immediate security and operational benefits but also proactively prepares your enterprise for the inevitable demands of AI, hyper-connected IoT/OT, and secure, high-performance global access.

Together, Palo Alto Networks and Accenture are helping enterprises de-risk their digital future and transform network security into a catalyst for innovation — maximizing efficiency, realizing substantial cost savings, and ensuring future-readiness for emerging technologies and threats.

In this whitepaper, you'll learn:



The strategic imperative for a unified SASE approach in the age of AI and hyper-connected environments



How a unified SASE strategy delivers measurable ROI, reduces complexity, and enhances your enterprise's security posture



Why a proven strategic partner is indispensable for building and executing a transformation roadmap that aligns SASE with your long-term business objectives

The Time for Secure Network Transformation Is Now

The way we work has undergone a fundamental shift — and the pace of change isn't showing signs of slowing. Hybrid work has turned every home into an extension of the enterprise network. Cloud adoption has erased the traditional perimeter. AI is accelerating decision-making and automation at an unprecedented pace. Yet many enterprise networks were built for a different era — designed for static workloads, centralized data, and predictable traffic. As organizations embrace multi-cloud environments, deploy AI-powered applications, and connect an array of IoT/OT devices, these legacy architectures become a critical vulnerability, incapable of supporting the dynamic, distributed, data-intensive workflows essential for modern business.

At the same time, cyber threats are evolving fast. Attackers are weaponizing AI, deploying sophisticated phishing, autonomous malware, and advanced evasion techniques to exploit systemic weaknesses faster than ever. A staggering 87% of security professionals report they encountered an AI-driven cyber attack in the last year, underscoring the urgent need for proactive, AI-powered defenses that legacy systems simply cannot provide.¹ This isn't just about data loss; it's about reputational damage, operational disruption, and significant financial penalties.

But Adoption Alone Doesn't Guarantee Success

While SASE adoption continues to rise — Gartner predicted that by 2025, 80% of enterprises would adopt a SASE/SSE architecture — implementation alone isn't enough.² Many SASE initiatives are derailed by a 'lift and shift' mentality, stitching together disparate point solutions. This creates fragmented architectures, introduces significant integration debt, fuels operational complexity, and creates inconsistent user experiences. And as AI-driven threats multiply and the attack surface expands to include vast IoT/OT environments, this piecemeal approach does more than amplify risk — it actively stalls innovation, hinders agility, and undermines your enterprise's competitive edge.

The Digital Transformation Gap:

25%

of organizations say their digital infrastructure has been transformed, despite hybrid work being the new norm.³

Cloud Dominance:

94%

of U.S. infrastructure decision makers are using the cloud, with the majority being hybrid or multi-cloud.⁴

AI's Relentless Reach:

78%

of organizations say they use AI in at least one business function.⁵

Forging a Future-Ready SASE Strategy: Beyond Point Solutions to Holistic Transformation

The core challenge isn't solely outdated infrastructure; it's the systemic issue of misaligned strategic priorities and disconnected operational approaches. To truly unlock the promise of secure network transformation, organizations require a holistic framework that tightly integrates people, processes, and technology around a singular, unified architecture.

The key components of a future-ready SASE strategy include:

Unified architecture by design:

Choosing a platform built for true convergence isn't just about reducing silos; it's about eliminating operational friction, enhancing real-time threat visibility, and ensuring policy consistency across your entire digital footprint. This is foundational for managing the complexity of AI-driven data flows and interconnected IoT/OT devices, and achieving this level of integration for AI and IoT/OT requires specialized knowledge that most internal teams lack or cannot scale to.

Consistent, high-performance user experience:

This directly impacts employee productivity, satisfaction, and your ability to attract and retain talent. For a global workforce interacting with AI applications and cloud resources, uncompromised speed and reliability are paramount to business continuity and innovation.

Built-in agility and scalability:

This ensures your network doesn't become a bottleneck for market expansion, new business models, or the exponential data demands of AI and IoT. It's about future-proofing your investments and enabling rapid adaptation to unforeseen technological shifts.

Zero Trust enforcement, everywhere:

Moving beyond perimeter-based security, Zero Trust is the imperative for protecting dynamic, distributed environments. It's about continuously verifying every user and device, safeguarding against internal and external threats, and securing sensitive data in the age of pervasive access and AI-driven data consumption. As AI-driven applications handle sensitive data and IoT devices become embedded in critical operations, the risk surface expands exponentially. Organizations must proactively address new compliance mandates (e.g., sector-specific IoT regulations) and build an adaptive security framework capable of defending against AI-generated attacks and securing the expanding IoT/OT perimeter.

Simplified operations and automation:

Leveraging AI-powered insights and unified policy management isn't just about reducing complexity; it's about optimizing your IT talent, reducing operational expenditure, and freeing up resources to focus on strategic initiatives rather than reactive fire-fighting. This is essential for managing the scale of future networks.

The Power of Strategic Partnership: Accelerating Your SASE Journey with Palo Alto Networks and Accenture

A compelling strategy, however, remains hypothetical without the right strategic partners to translate it into tangible, measurable outcomes. Executing a SASE transformation of this magnitude demands not just technology, but deep industry expertise, proven methodologies, and a shared vision for your future.

Together, Palo Alto Networks and Accenture are reimagining what secure network modernization really looks like.



An integrated solution

Palo Alto Networks Prisma SASE brings together cloud-delivered security and next-generation SD-WAN into a unified platform, ensuring all your applications and users are secured, regardless of their location. The solution consolidates disparate point products — including Zero Trust Network Access (ZTNA), Cloud Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and SD-WAN — while providing uncompromised performance backed by leading SLAs and the industry's only SASE-native ADEM to support an exceptional end user experience.⁶



Enhanced protection for future technologies

Beyond current threats, Prisma SASE proactively addresses the challenges of AI access, secure browsing for unmanaged devices, and critical IoT/OT implications. Capabilities like Prisma Access Browser provide secure, isolated web access, safeguarding sensitive data accessed from any device. This is vital as AI models interact with enterprise data, and as browser-based access becomes central to collaboration. Furthermore, Prisma SASE delivers advanced data security and granular visibility across expanding attack surfaces, ensuring that as AI-driven threats proliferate and IoT/OT deployments scale, your sensitive information remains secure without impeding the speed or flexibility your business demands.



**Industry recognition.
Real-world results.**

5x

faster than the
open internet⁷

2025

Gartner® Magic
Quadrant™ for
SASE Platforms

2025

Gartner® Magic
Quadrant™ for SSE

2024

Gartner® Magic
Quadrant™
for SD-WAN



AI-driven threat protection

AI brings new data privacy and security implications. IoT/OT introduces novel attack vectors and compliance challenges (e.g., industry-specific regulations). A strategic partner helps identify, mitigate, and navigate these emerging risks, ensuring continuous compliance and resilience. Leveraging Palo Alto Networks' Precision AI™ — built on over 15 years of AI expertise — your organization benefits from unparalleled defense, blocking an estimated 8.6 billion attacks daily.⁸ This proactive, intelligent defense is essential for countering the sophisticated, AI-generated cyber threats of today and tomorrow.



Support from proven partners

Network transformation isn't just about plugging in new tech. It involves deep network architecture changes, policy orchestration, data flow analysis, and potential impacts on operational continuity. Accenture brings the expertise to manage this complexity across diverse environments and provide end-to-end expertise — from initial diagnostics and architectural design to full operationalization and ongoing management services. Accenture's deep experience in large-scale enterprise transformations, combined with a profound understanding of Palo Alto Networks leading solutions, ensures a tailored success plan that addresses your unique challenges and accelerates time-to-value.

Palo Alto Networks and Accenture have partnered with Comcast Business, the nation's largest cable provider to small and mid-size businesses and recognized by leading industry associations as one of the fastest growing providers of Ethernet services, to implement Prisma SASE solutions to help protect their network assets across a dynamic workplace that spans office, remote and cloud environments. By providing a cloud-delivered security platform, Comcast Business is able to protect businesses applications from the branch office and extend that protection to users working from anywhere.

Collaborating to Secure the Future of Work

"Comcast Business is committed to leveraging a SASE framework to bring compelling network and security solutions to our customers — and our collaboration with Accenture and Palo Alto Networks expands our capability to do so. By providing a cloud-delivered security platform, Comcast Business is able to protect business applications from the branch office and extend that protection to users working from anywhere."

Shena Seneca Tharnish

*VP of Cybersecurity Products,
Comcast Business*

Strategic SASE: Unlocking Enterprise-Wide Business Outcomes and Future Resilience

A strategically implemented, unified SASE architecture, championed by the right partners, transcends mere security enhancements. It becomes a powerful catalyst for enterprise-wide business transformation, delivering significant ROI, and building unparalleled future resilience against evolving technological and threat landscapes.

Palo Alto Networks and Accenture can help deliver business benefits such as:

Reduced operational complexity:

By consolidating fragmented security and networking solutions onto a single platform, organizations can dramatically reduce IT overhead, simplify management, and redirect valuable resources from tactical maintenance to strategic innovation. This streamlined approach prepares your team to manage the expanding digital footprint of AI and IoT.

Stronger security posture:

Unified SASE delivers proactive, end-to-end threat prevention, addressing known and unknown threats. Crucially, with employees spending over 85% of their workdays using browsers, secure enterprise browsers become a non-negotiable layer of defense, ensuring secure work on any device while enhancing application performance – critical for safeguarding data accessed by AI systems and managing the risks of ubiquitous web access.⁹

Accelerated adoption with gen AI:

Unified SASE platforms inherently integrate generative AI and co-pilots, simplifying onboarding, accelerating policy deployment, and enabling IT teams to manage complex environments more intelligently. This is about augmenting your human capital and ensuring your SASE investment delivers faster, more impactful results.

Improved visibility:

A unified SASE strategy provides 360-degree operational insight by consolidating data from across your entire digital estate into a single view, eliminating blind spots and empowering proactive management of users, applications, and devices, including emerging AI and IoT/OT. This holistic visibility, coupled with AI-powered analytics, transforms raw data into actionable intelligence, allowing leaders to make informed, strategic decisions that optimize performance, mitigate risk, and accelerate innovation for a future-ready enterprise.

Smart talent and cost optimization:

For organizations facing critical talent shortages or seeking to reallocate resources, outsourcing network transformation to proven partners like Accenture allows you to overcome skill gaps, reduce operational costs through automation and global delivery models, and strategically re-focus your internal teams on core business priorities. Forrester Research indicates 270% ROI for Prisma SASE, underscoring the significant financial benefits of this strategic shift.¹⁰

Your Future-Proof Network Starts Here: Partnering for Strategic SASE Transformation

The digital landscape will continue to evolve, with new technologies constantly emerging. And the shift to a truly future-proof network architecture is not merely a technological upgrade; it's a fundamental strategic imperative. Navigating this complex transformation, especially in the context of developing AI and IoT/OT landscapes, and the demands of global secure access, requires more than just best-in-class SASE solutions. It demands the right strategy, coupled with the unparalleled support and proven expertise of a true strategic partner.

The Palo Alto Networks and Accenture partnership offers a clear, accelerated roadmap that anticipates future demands, ensuring your network remains agile, resilient, and prepared for whatever innovations come next. Our three integrated services — SASE Advisory, SASE Implementation, and SASE as a Service — are designed to guide your organization at every stage, ensuring a seamless transition and maximum value realization.¹¹

By combining the world's most advanced AI-powered security platforms with deep transformation expertise, we help enterprises modernize their networks and confidently scale for what's next.



Get in Touch — We're Here to Help

Don't let legacy infrastructure or a piecemeal SASE approach jeopardize your organization's future. Whether you're beginning your SASE journey with a focused initiative like securing AI access, optimizing SD-WAN for hybrid work, or implementing Zero Trust for ubiquitous connectivity, or if you require a comprehensive reassessment of your entire network strategy, our joint experts are ready to collaborate.

**Connect with us today
to schedule a strategic
discussion and begin
building your future-
proof network.**

[Start your journey](#)

Sources

1. <https://www.infosecurity-magazine.com/news/majority-of-orgs-hit-by-ai>
2. <https://www.paloaltonetworks.com/blog/2023/02/five-compelling-benefits-of-a-managed-sase-solution>
3. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/why-the-sase-approach-to-network-and-security-is-the-answer-to-combating-sophisticated-cyberattacks
4. <https://www.paloaltonetworks.com/resources/whitepapers/your-hybrid-infrastructure-is-under-attack.viewer.html>
5. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>
6. <https://www.paloaltonetworks.com/blog/2023/06/accenture-teams-with-palo-alto-networks/>
7. <https://www.paloaltonetworks.com/sase/app-acceleration>
8. <https://www.paloaltonetworks.ca/cyberpedia/what-is-precision-ai>
9. <https://start.paloaltonetworks.com/Gartner-innovation-insights-Secure-Enterprise-Browser>
10. <https://www.paloaltonetworks.com/blog/sase/what-is-the-roi-of-sase/>
11. https://www.paloaltonetworks.com/content/dam/pan/en_US/partners/nextwave-for-gsi/accenture/integrated-sase-solutions-delivered-by-accenture-and-panw.pdf



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.