



Four pillars of secure innovation

A roadmap for transforming your network into a catalyst
for growth — powered by Palo Alto Networks and Accenture



The network isn't just infrastructure. It's your competitive edge.

The convergence of hybrid work, multi-cloud, and relentless AI adoption has permanently reshaped the enterprise landscape. Your network, once a behind-the-scenes enabler, is now either a competitive force — or a compounding risk.

Legacy architectures can't keep pace. Built for static perimeters and centralized apps, they now breed complexity, throttle innovation, and expose your business to escalating threats.

Palo Alto Networks and Accenture have joined forces to help enterprises move from fragmented, reactive environments to secure, simplified, and resilient infrastructure built for continuous transformation.

At the core is a unified Secure Access Service Edge (SASE) platform reinforced by four pillars: secure workforce, secure browser, OT security, and AI acceleration. Together, they empower faster threat detection and response, stronger business continuity post-breach, and a network built to adapt as fast as the threats do.

Equally important: a unified platform that eases the burden on IT teams. By eliminating the need to manage disparate point solutions, your teams are freed to focus on higher-value initiatives that drive the business forward.

This isn't just a shift in architecture — it's a shift in how your people, processes, and technology come together to fuel innovation.



The digital transformation gap

Only 25% of organizations say their digital infrastructure has been transformed, despite hybrid work being the new norm.¹



Cloud dominance

94% of U.S. infrastructure decision makers are using the cloud, with the majority being hybrid or multi-cloud.²



AI's relentless reach

78% of organizations say they use AI in at least one business function.³

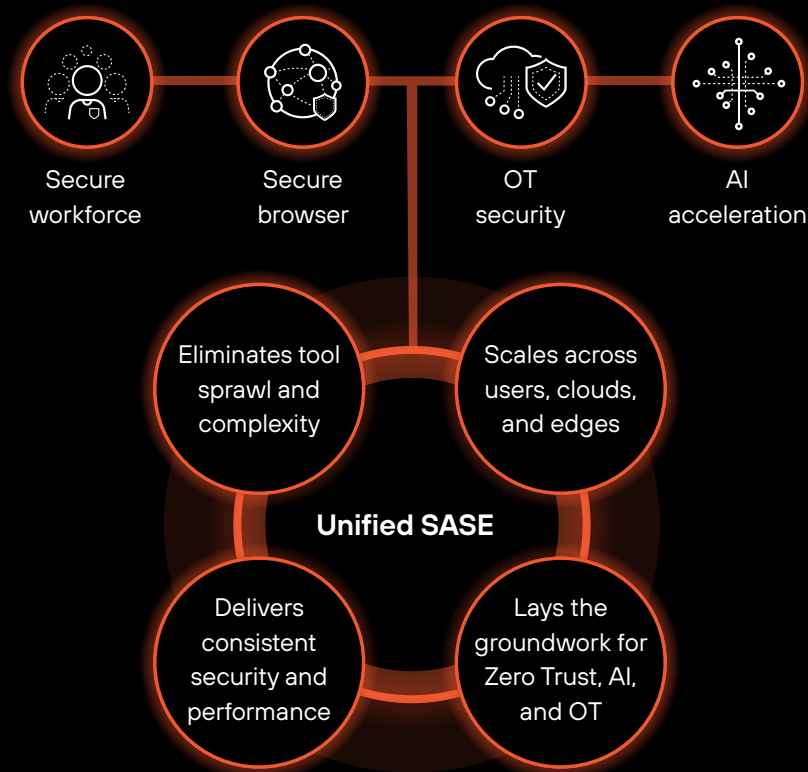
Unified SASE isn't the end goal. It's where transformation begins.

SASE is no longer just an IT initiative — it's a strategic accelerator. Unified SASE fuses networking and security into a single, cloud-delivered fabric that connects users and data with speed, simplicity, and confidence.

It reduces complexity, enhances user experience, builds resilience by design, and strengthens governance. With deeper visibility across your digital environment, SASE aids in maintaining data visibility and adhering to evolving regulatory requirements including GDPR, and new, sector-specific compliance mandates for IoT/OT.

But successful transformation doesn't happen ad hoc. It starts with a roadmap that aligns Zero Trust, cloud strategy, and business goals. Palo Alto Networks and Accenture provide both the platform and the strategic expertise to deliver.

SASE Considerations



THE FOUR PILLARS OF SECURE INNOVATION

From foundation to future: What you need to secure next.

To stay ahead, organizations need a roadmap that addresses the next wave of digital risk: web access, OT environments, and the AI acceleration. These aren't optional add-ons. They're essential pillars of secure innovation. Each requires a proactive approach, built on your existing SASE strategy, to protect what's next without slowing you down.

PILLAR ONE

Secure Workforce & Network Transformation

Smarter access. Stronger performance. Anywhere.

Enable hybrid workforces with cloud-native, AI-powered network security that adapts in real time. Prisma® SASE brings SD-WAN, ZTNA, ADEM, and Cloud SWG into one unified platform — boosting agility while cutting cost. Accenture delivers the strategy.



PILLAR TWO

Secure Browser

Your browser is the new endpoint. Secure it.

The browser has become the front door to enterprise apps — and a major attack vector. Prisma® Access Browser provides agentless, policy-driven protection across any device without disrupting workflows. Accenture ensures seamless integration and operationalization to keep your workforce secure and productive.

85%

of an employee's workday is spent using browsers, making secure enterprise browsers a non-negotiable layer of defense.⁴

PILLAR THREE

OT Security

At the edge of innovation lies real-world risk.

As IT and OT systems converge, industrial environments face increasing threat exposure with limited visibility. Palo Alto Networks offers agentless, real-time protection across the OT lifecycle, while Accenture tailors assessments, roadmaps, and managed services to harden your edge and elevate resilience.



PILLAR FOUR

AI Acceleration

Accelerate AI without compromising trust.

AI is now mission-critical, powering everything from productivity tools to core business processes. But it's also introducing unprecedented risk. Every model, prompt, and API request can become a potential threat vector. Prisma Access, with integrated ZTNA, SWG, CASB, and DLP, helps govern how AI is accessed and used — blocking data loss, controlling unauthorized use, and giving organizations visibility into shadow AI tools operating across the network. While Palo Alto Networks delivers the controls to secure AI at scale, Accenture brings the strategy, change management, and policy expertise to help organizations safely embrace AI, stay compliant, and scale responsibly.

24%

of ongoing GenAI projects
take security into consideration.⁵

Secure innovation isn't a technical win. It's a business mandate.

When executed strategically, secure innovation unlocks business-wide value:

- **Reduced complexity:** Streamline operations and refocus talent on growth.
- **Proactive security:** Anticipate threats with AI-powered defenses.
- **Faster innovation cycles:** Enable business units to rapidly adopt new technologies, launch new products or services, and enter new markets without security being a bottleneck.
- **Future-ready foundation:** Confidently support AI, OT, and next-gen applications.

According to Forrester, unified SASE accelerates transformation, reduces cost, and mitigates risk, making it a powerful foundation for business case justification.⁶ Organizations that move first gain the advantage. Those that wait risk more than delay — they risk falling behind in a world that's moving fast.

"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

From Risk to Resilience

270% ROI

Enterprises adopting Prisma® SASE can achieve up to **270% return on investment**, driven by reduced operational expenditure through automation, consolidation, and expert managed services from partners like Accenture.

Before

Unsecured browsers expose users to phishing, malware, and data loss

Fragmented network tools slow hybrid work and increase cost

OT systems lack visibility and are isolated from IT security practices

AI adoption outpaces security, risking model theft and misuse

After

Secure browser delivers agentless, protected access with policy-driven control

Unified, cloud-delivered access boosts agility and lowers total cost of ownership

The integrated approach, bolstered by real-time, agentless OT protection, provides immediate visibility into the compromised industrial environment, isolates the affected systems to prevent lateral movement to IT networks, and enables swift containment and remediation, maintaining operational continuity and resilience in the event of an OT breach

Secure AI ensures protection across the full lifecycle – from training to deployment

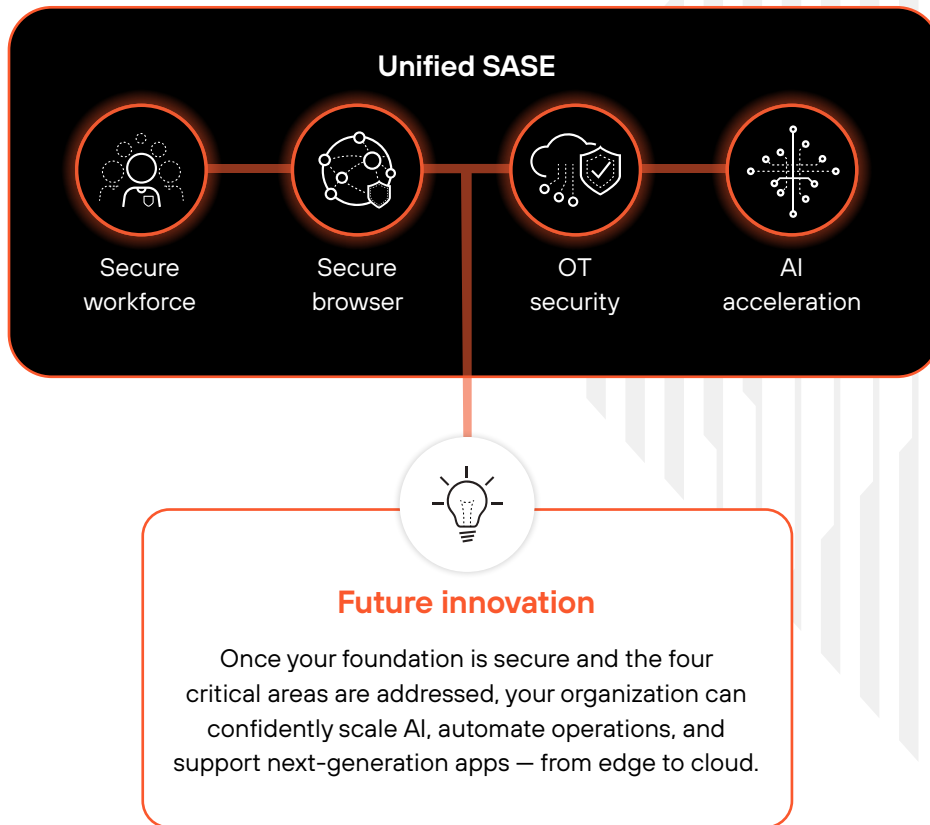
SUMMARY

Let's build for what's next.

Your infrastructure shouldn't be a barrier — it should be a springboard. Palo Alto Networks and Accenture unite best-in-class technology with deep transformation expertise to modernize your network, harden your defenses, and unleash what's next.

Whether you're refining SASE, securing your edge, or scaling AI, this is your moment to act.

Ready to get started? Get in touch at accenture@paloaltonetworks.com to start building your secure innovation roadmap.



SOURCES

1. 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-combatting-sophisticated-cyberattacks
2. <https://www.paloaltonetworks.com/resources/whitepapers/your-hybrid-infrastructure-is-under-attack.viewer.html>
3. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>
4. <https://start.paloaltonetworks.com/Gartner-innovation-insights-Secure-Enterprise-Browser>
5. <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/securing-generative-ai>
6. <https://www.paloaltonetworks.com/blog/sase/what-is-the-roi-of-sase/>



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.