

Protecting sensitive healthcare data with SASE

As healthcare organizations transition to distributed workforce models, adopting a Zero Trust strategy is more critical than ever.

Inflexible network perimeters are no longer effective, and IT teams are navigating the complexity of securing their ever-expanding attack surface.



Network perimeter in healthcare is expanding at an exponential rate



The healthcare industry needs an alternative strategy to prevent insecure work habits



Cybercriminals frequently target the healthcare industry



How can healthcare organizations secure confidential data and their network infrastructure effectively and efficiently in the face of unrelenting threats on an attack surface that keeps growing?



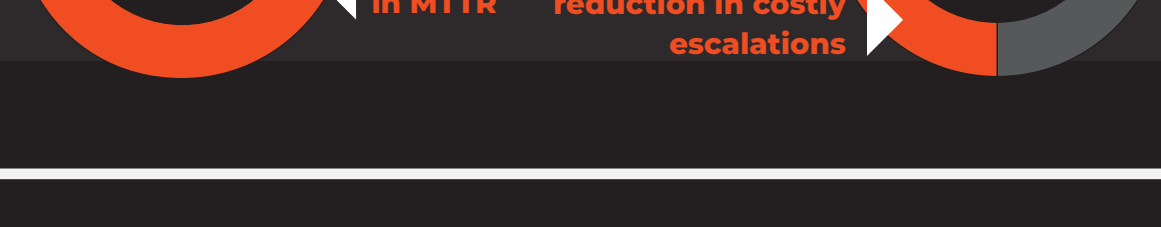
Think SASE: Revamp your cybersecurity strategy now

Secure Access Service Edge (**SASE**) is the convergence of wide-area networking (**SD-WAN**) and network security services like Cloud Access Security Broker (**CASB**), Firewall as a Service (**FWaaS**) and Zero Trust Network Access (**ZTNA**) into a single, cloud-delivered service model.

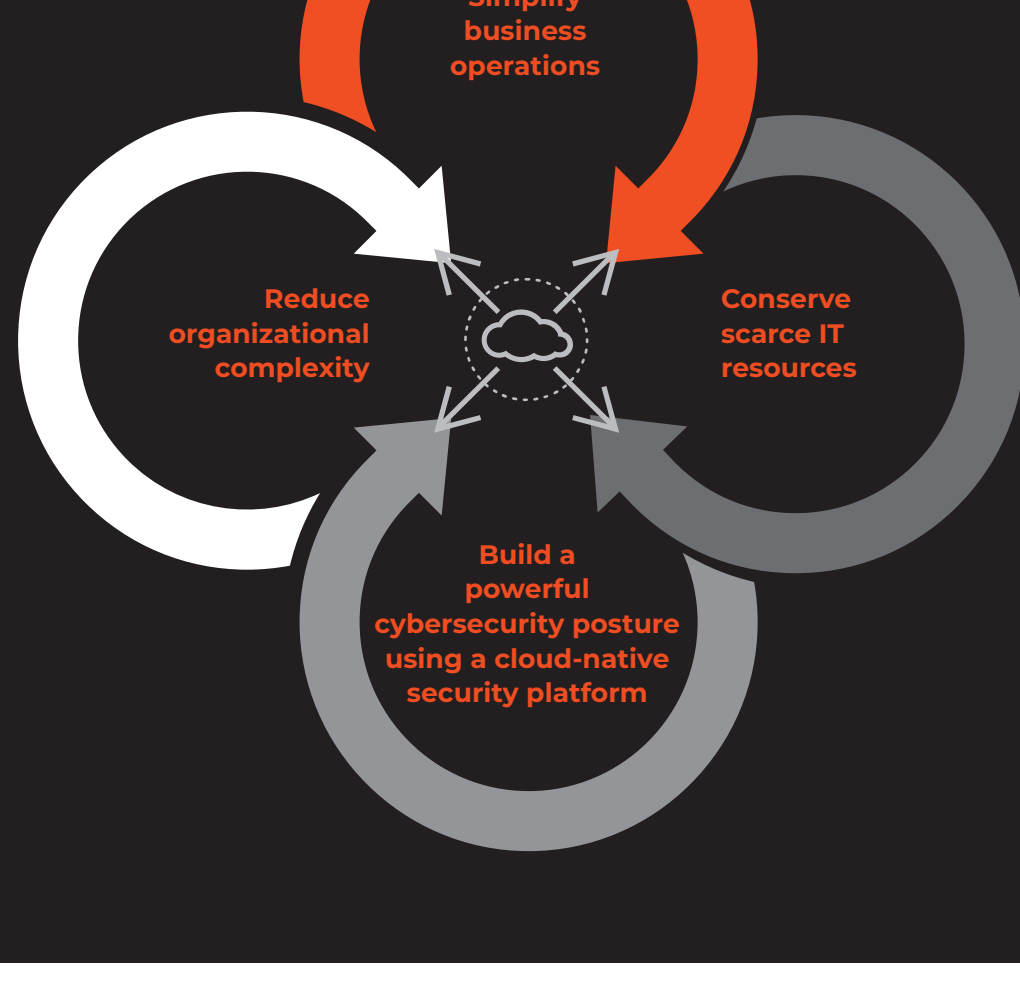
Palo Alto Networks **Prisma SASE** operates from a unified, single-vendor approach. This enables organizations to optimize security and operational outcomes while leveraging AI and ML across security, networking and user-experience management.

The power of ADEM

Built for Prisma SASE, AI-Powered ADEM enables IT teams to drive proactive IT operations and exceptional user experiences. The platform's **holistic observability** and **built-in AIOps** eliminate IT blind spots and automate complex IT operations, from incident detection through remediation, without installing additional software or hardware.



Providing healthcare organizations with the solutions to build a more robust, agile and predictive cybersecurity posture to:



The Infosys approach to building a robust managed SASE solution leverages the 4D framework:

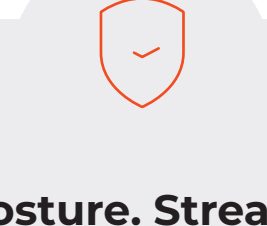
- 1 Diagnose**
 - Assess security controls
 - Review network architecture
 - Access gap issues with reference ZTNA
 - Develop high-level SASE architecture
- 2 Design**
 - Design SASE solution, high-level business and user access scenarios
 - List application security policies, standards for enforcement and success and acceptance criteria
 - Define a plan for implementation and user adoption
- 3 Deliver**
 - Detailed technical design and acceptance test plan
 - Test for capabilities
 - Test for integration with Intrusion Detection Prevention (IDP), Security Operations Center (SOC), policy management tools and on-prem network gateway
 - Test policy configuration for myriad security tools, site and user migration to the SASE service
- 4 Defend**
 - Monitor service availability and performance
 - Conduct ongoing policy fine-tuning
 - Review lifecycle management for new site/user/policy
 - Collaborate with SOC teams for incident resolution, service assurance, governance, and continuous improvement

Infosys Managed Services

- Rapid deployment with zero-touch provisioning and automated configuration
- Single pane of glass with telemetric view
- Enhanced UX with lightweight device agent, granular policies and improved latency
- Leverage 4D framework with reusable assets and best practices from across projects

Palo Alto Networks Prisma SASE

- Industry's most complete SASE
- Gartner Magic Quadrant™ Leader: 2022 SD-WAN & 2023 SASE**
- Gartner Peer Insights 2023 Customers' Choice for Security Service Edge**
- IDC's 2023 leader in **NESaaS** and **ZTNA** MarketScape Reports
- Organizations can expect an **ROI of 247%** with Prisma SASE integration



Bolster your security posture. Streamline your IT processes and tech stack. Prepare for whatever comes next with Infosys and Palo Alto Networks.

Contact us to **learn more.**

¹ McKinsey, "Americans are embracing flexible work—and they want more of it," 2022
² Proofpoint/Ponemon, "Cyber Insecurity in Healthcare, 2022"
³ Symplr, "Survey: CIOs Stressed in Managing Overabundance of Systems, Platforms, 2022"
⁴ The HIPAA Journal, "August 2023 Healthcare Data Breach Report"
⁵ Salesforce, "New Era in Data Stewardship, 2023"
⁶ Salesforce, "New Era in Data Stewardship, 2023"
⁷ SalesForce, "New Era in Data Stewardship, 2023"
⁸ TechTarget, "Healthcare breaches on the rise in 2022"
⁹ TechTarget, "Healthcare breaches on the rise in 2022"
¹⁰ Palo Alto Networks, "2023 Unit 42 Ransomware and Extortion Report"