INFOSYS SECURE ACCESS SERVICE EDGE POWERED BY PALO ALTO NETWORKS PRISMA CLOUD DEPLOYMENTS, GOVERNANCE AND ADMINISTRATION CAPABILITIES
Overview

With more user work performed remotely than on the enterprise network, workloads running on public cloud than on the enterprise data center, applications consumed via SaaS, sensitive data located outside the enterprise data center in cloud services, and user traffic destined for public cloud services than to the enterprise data center, organizations face a mammoth challenge of analyzing continuous threats and adhering to compliance across cloud and hybrid infrastructure.

To support the shift to an anywhere workforce, organizations need to adopt cloud, embrace mobility, and deliver a superior user experience—all while protecting their users and business against emerging security threats.

Infosys SASE with zero trust access, powered by Prisma Cloud, is a strong solution for enterprises. Prisma SASE is the industry’s most complete SASE solution, converging security, SD-WAN, and autonomous digital experience management into a single cloud-delivered service. Alleviate installation, deployment, monitoring, and troubleshoot challenges through automation. Cloud-hosted management platform that centralizes policy creation, distribution, and control. Easy to deploy and manage as an automated, cloud-delivered service.

With our strong strategic and technical partnership with Palo Alto Networks, we offer frictionless delivery of SASE with zero trust access solutions.
What We Do – Our Services

The Infosys approach to build a robust SASE solution

**Diagnose**
- Assess current security controls and user profiles
- Review current proxy, VPN, network topology and IT resource access
- Access gaps issues with reference ZTNA
- Define requirements and use cases for secure access
- Develop high level SASE architecture, topology and business case

**Design**
- High level SASE solution and security control design
- Design high level business and user access scenarios
- List application security policies and standards for enforcement through SASE
- Define SASE success and acceptance criteria
- High level plan implementation user adoption and operations readiness

**Deliver**
- Detailed technical design and acceptance test plan
- SASE foundation build and test for capabilities with sample users and sites
- Integration with IDP, SOC, policy management tools and on prem network gateway
- Policy configuration for cloud firewall, proxy, DLP, ATE traffic management etc
- Site and user migration to SASE service

**Defend**
- Service availability and performance monitoring
- Ongoing policy fine tuning, URL blacklisting whitelisting
- Lifecycle management for new site / user / policy and capability management
- Collaborate with SoC teams for security incident resolution
- Service assurance, governance and continuous improvement

Infosys – SASE Palo Alto Networks Prisma Solution – A Detailed View
Business Benefits –

Unified user experience and simplified access – The centralized monitoring and dashboards will give good visibility of endpoints. They bring security and policy close to the user across 200+ locations to eliminate unnecessary backhaul and provide optimal bandwidth and low latency.

Assured cost saving – By consolidating secure access services from a single provider, the overall number of vendors will be reduced, the number of physical and/or virtual appliances in a branch and the number of agents required on an end-user device will be reduced.

Zero trust network access enabled – Implementation of zero trust on principles such as verify explicitly, use least privileged access & assume breach is underway. Zero trust is also quite simple to deploy, implement and maintain using a simple five-step methodology of identify the protect surface, map the transaction flows, build a zero trust architecture, create zero trust policy, monitor and maintain. This guided process helps identify your current status and offers a future roadmap.