INFOSYS SECURE ACCESS SERVICE EDGE AS-A-SERVICE POWERED BY PALO ALTO NETWORKS PRISMA® ACCESS

paloalto® NETWORKS

Infosys® Navigate your next

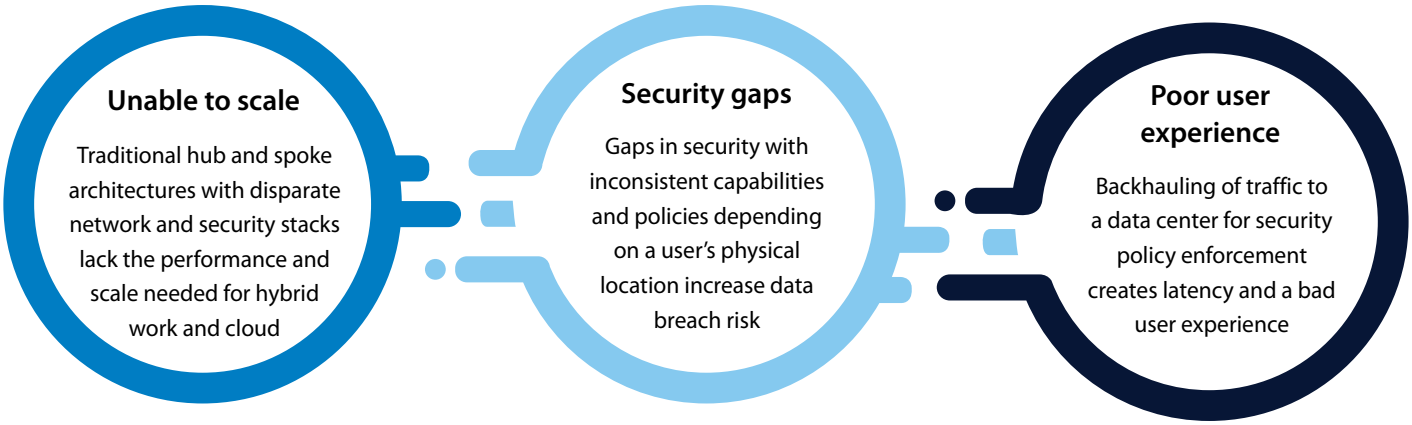
Cybersecurity redefined in the age of digital transformation

With hybrid and remote work becoming the norm, organizations must give employees secure access to the tools and resources required to perform their jobs wherever they choose to work. Modern work environments require a seamless and secure connectivity experience; however, legacy VPN and traditional technologies don't provide the level of security and access control organizations need to combat today's sophisticated and deliberate cyberattacks in the age of digital transformation.

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

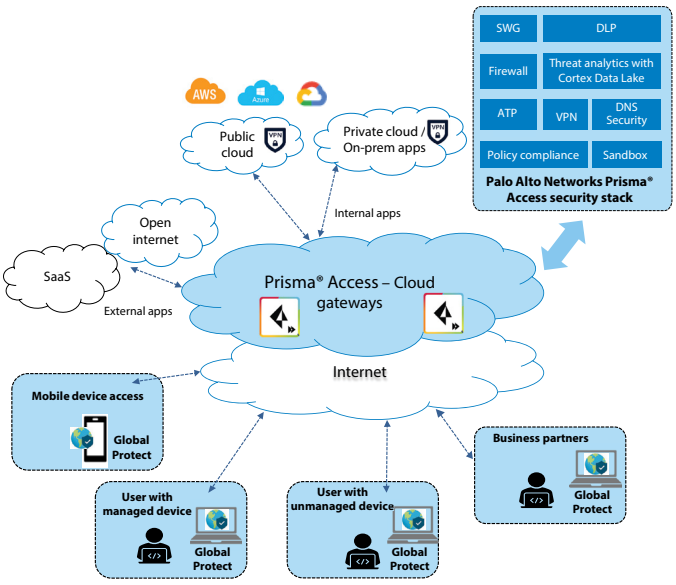
Challenges that exist in legacy networks and security approaches

Legacy network architectures no longer work in today's cloud-enabled world



Solution overview

Infosys Secure Access Secure Edge (SASE), powered By Palo Alto Networks Prisma® Access, is a robust solution for enterprise organizations. Prisma® Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma® Access protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach. With a common policy framework and single-pane-of-glass management, Prisma® Access secures today's hybrid workforce without compromising performance, backed by industry-leading SLAs to ensure exceptional user experiences.



Infosys' strategic alliance with Palo Alto Networks delivers Prisma® Access seamlessly to enable:

Superior ZTNA 2.0 Security

Consistently protect the hybrid workforce with the superior security of ZTNA 2.0

Security as-a-service model

Enables to scale the security controls and extend protection to users at all situations, eliminates any captive overloads bringing agility in the overall security posture

Standardized and simplified

Standardized and simplified security standards and policies enforced across the organization with unified interface and visualized through a single pane of glass with real-time telemetric view

External Document © 2022 Infosys Limited

Use cases

Prisma® Access enables employees from any location to operate seamlessly and securely across all applications

Hybrid work

With a Prisma SASE integration, employees may operate seamlessly across corporate offices, branch offices, at-home offices, and on the road as firms prepare to enable a hybrid/remote work mode

Secure SD-WAN

As more and more organizations start returning to branch offices, ensuring a powerful SD-WAN solution at the branch that is natively integrated with cloud-delivered security and deep application digital experience monitoring has become more critical than ever

Multi-cloud migrations

Direct-to-app access is offered to clients when they access their apps across any public cloud, SaaS, or private cloud provider, regardless of where the customer is located—at the branch, corporate office, or home

Service offerings to meet your needs

The Infosys approach to building a robust SASE solution is centered on a four-phase approach: Diagnose, Design, Deliver and Defend

Diagnose

- 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

Design

- Detailed technical design and acceptance test plan
- SASE foundation build and test for capabilities with sample users and sites
- Integration with Intrusion Detection and Prevention (IDP), Security Operations Center (SOC), policy management tools, and on-prem network gateway
- Policy configuration for cloud firewall proxy, Data Loss Prevention (DLP), Advanced Technological Education (ATE) traffic management, and other security tools
- Site and user migration to the SASE service

Deliver

- 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

Defend

- 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

External Document © 2022 Infosys Limited

Infosys and Palo Alto Networks joint value proposition

Infosys Technology and Palo Alto Networks work together to offer a complete, cloud-delivered security platform to assure robust security of enterprise network perimeters, workloads, workplaces, and cloud infrastructure, while constantly alleviating the customer's security posture and accelerating secured digital transformation.

What makes us different together?

Infosys technology offers best-in-class managed SASE solutions, services, and flexible consumption models wrapped around Palo Alto Networks SASE technology

Palo Alto Networks offers a next generation cloud-delivered security platform with a manageable architecture and SLA-backed performance

Our partnership offers an agile service delivery model, innovation, and scale to meet enterprise business needs

Infosys delivers scale with assurance. By driving an enterprise mindset towards Secure by Design at every stage of the business cycle, we minimize security risks while maximizing the visibility of the security threat, impact, and resolution.

Together, we support organizations as they adopt a Zero Trust architecture and use technology solutions such as SASE to become more risk-resilient and meet the challenge of securing today's hybrid workforce in a rapidly evolving cyber threat and security landscape.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2022 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.