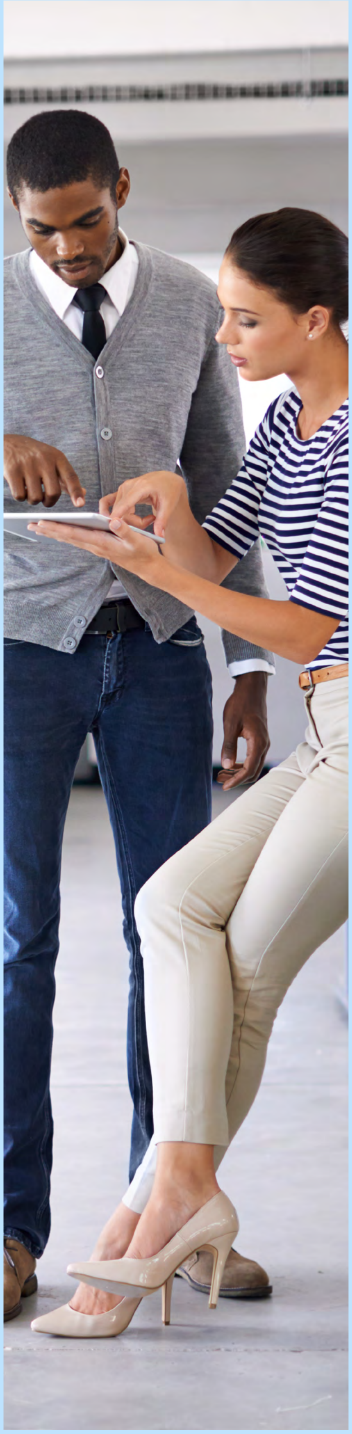
# SECURE ACCESS SERVICE EDGE (SASE)

## ACCELERATING DIGITAL TRANSFORMATION TO ENABLE A SECURE MODERN WORKFORCE



paloalto® NETWORKS

Infosys® Navigate your next

## Introduction

As more and more organizations ask their employees to return to the office, a hybrid work paradigm, sometimes referred to as “the new normal,” will continue to play an integral role in how business is conducted for the foreseeable future. Nowadays, work is no longer a place we go to but rather an activity we perform. The primary goal is to securely connect users that are now anywhere to the apps and services they need everywhere while mitigating the risks of cyber threats and malicious actors. As a result, organizations are now looking for ways to safeguard their users, applications, and data from evolving security threats while increasing cloud usage and ensuring optimal end-user experiences. However, the majority of businesses have discovered that this approach is easier said than done.

Many organizations still use traditional VPN solutions and legacy Zero Trust Network Access (ZTNA) solutions, both of which have inherent flaws in their architecture: they provide too broad of access to users - which goes against the core principles of a Zero Trust architecture - and they lack continuous trust verification as well as security inspection. To overcome these challenges and to converge disparate point products into a single solution, many organizations have started exploring Secure Access Service Edge - or SASE - solutions.

SASE is a new architectural approach. It converges essential networking and security services such as SD-WAN, Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA) into a single cloud-delivered service. SASE offers highly secure and consistent access no matter where users, applications, or data are located.

> Gartner®, “By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud services, and private application access using a SASE/SSE architecture, up from 20% in 2021.”

Organizations need a new security strategy plan to operate successfully and securely in this cloud-first environment that safeguards them from end to end.

## Existing challenges with traditional network and security

Legacy network architectures are no longer suited to address today’s digital cloud challenges for the following reasons:

1. **Poor performance:** Networks operating with a traditional nonintegrated model perform poorly and lack the agility needed for today’s workforce dynamics.

2. **Inability to scale:** Traditional hub-and-spoke architectures with disparate network and security stacks don’t scale to accommodate hybrid work and cloud.

3. **Security gaps:** Gaps in security with inconsistent capabilities and policies depending on a user’s physical location increase data breach risk.

4. **Poor user experience:** Backhauling of traffic to a data center for security policy enforcement creates latency and a bad user experience or no means of detecting the poor user experience.

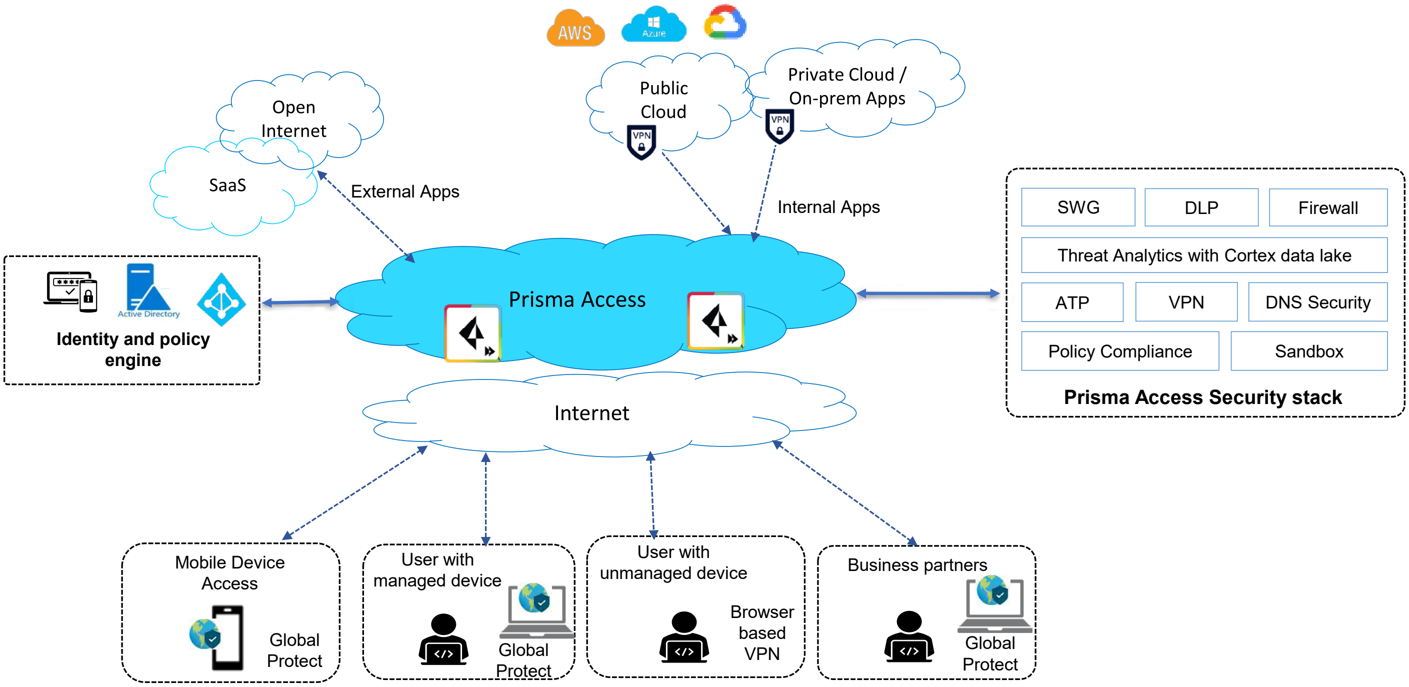
## Solutions Overview

Infosys managed SASE powered by Palo Alto Networks Prisma SASE, is a robust and comprehensive solution for enterprise organizations wishing to streamline their operations from a unified platform, reduce costs, and extend consistent security to their hybrid workforces. Prisma Access, the Security Service Edge (SSE) component of Prisma SASE, protects the hybrid workforce with ZTNA 2.0’ while providing optimal user experiences from a unified product that’s easy to manage. Purpose-built in the cloud to secure at scale, only Prisma Access protects all application traffic with best-in-class capabilities while securing both user access and sensitive data. With a common policy framework and single-pane-of-glass management, Prisma Access secures today’s hybrid workforce without compromising performance and is backed by industry-leading SLAs.

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

- **Superior ZTNA 2.0 security:** Consistently protects the hybrid workforce by combining fine-grained least-privileged access with deep and ongoing security inspection and enterprise Data Loss Prevention (DLP) to protect all users, devices, apps, and data from even the most sophisticated threats everywhere
- **A unified security product:** Comprehensive protection converged into a single unified product with single-pane-of-glass visibility and management, consistent policy, and shared data for all users and all apps to dramatically reduce the risk of a data breach

- **Security-as-a-service model:** Enables scaling the security controls and extending protection to users in all situations, eliminating any captive overloads and bringing agility in the overall security posture
- **Enhanced user experience:** A cloud-native architecture built to secure today’s digital enterprises at cloud scale and provides uncompromised performance backed by leading SLAs that deliver an exceptional user experience



## Use Cases

Three fundamental shifts are driving the need for network transformation in the workplace.

**Hybrid workforce** has become the new normal and a requirement for many organizations due to the pandemic. As a result, many organizations have planned to support a model where the of employees can work fluidly between corporate offices, branch offices, home offices, and on the road.

**Cloud and digital initiatives** are driving organizations to invest more in SaaS and other public cloud services. Cloud adoption enables companies to be more agile, efficient, and flexible—indicative of why 92% of all enterprises are now adopting a multi-cloud strategy. SASE brings protection closer to users, so traffic doesn't have to backhaul to headquarters to reach the cloud.

**Branch transformation** is well underway, driven by new hybrid work and digital transformation initiatives. Organizations are fundamentally changing the branch—leveraging branches as collaboration hubs rather than primary places of work—while retailers are transforming how they engage with customers. This trend is fueling the demand for WAN transformation from legacy Multiprotocol Labor Switching (MPLS) to SD-WAN and SASE.

## Service catalog:

The Infosys approach to building a robust managed SASE solution is centered on a four-phase approach:

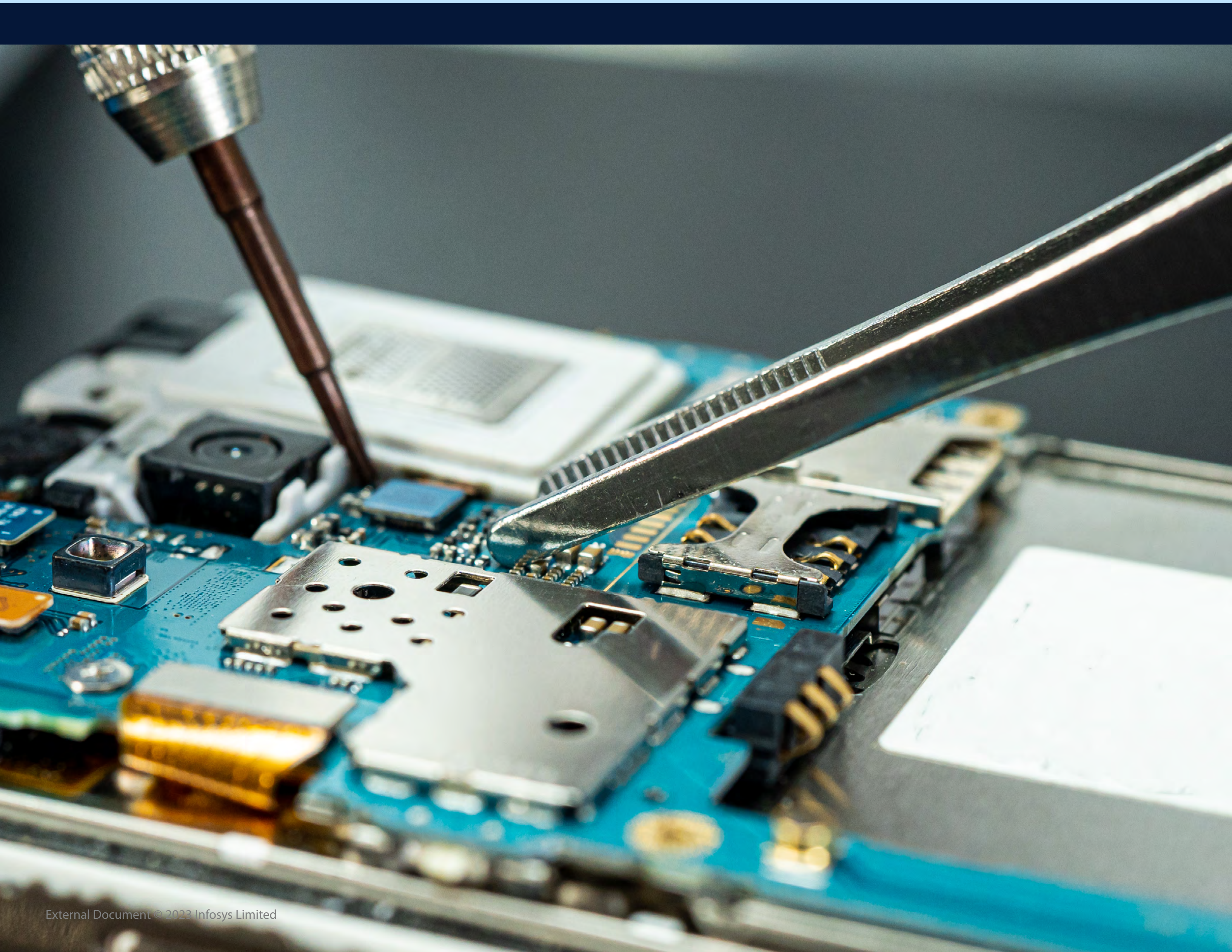
- **Diagnose:**
  - Assess current security controls and user profiles
  - Review current proxy, VPN, network topology, and IT resource access
  - Access gaps issues with reference ZTNA
  - Define requirements and use cases for secure access
  - Develop high-level SASE architecture, topology, and business case
- **Design:**
  - Design high-level SASE solution and security control
  - Design high-level business and user access scenarios
  - List application security policies and standards for enforcement through SASE
  - Define SASE success and acceptance criteria
  - Define a high-level plan implementation for 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 Intrusion Detection Prevention (IDP), Security Operations Center (SOC), policy management tools, and on-prem network gateway
  - Policy configuration for cloud firewall proxy, DLP Automatic Test Equipment (ATE) traffic management, and other security tools
  - Site and user migration to the SASE service
- **Defend:**
  - Monitoring of service availability and performance
  - Ongoing policy fine-tuning, URL block listing, and allow listing
  - Lifecycle management for new site/user/policy and capability management
  - Collaboration with Security Operation Center (SOC) teams for security incident resolution
  - Service assurance, governance, and continuous improvement

External Document © 2023 Infosys Limited

## Benefits of a SASE adoption

- Reduces complexity and costs with a unified networking and security solution
- Improves performance and eliminates latency
- Enables new digital business scenarios
- Offers secure access to a mobile workforce, branch users and protects unmanaged and IoT devices
- Provides ease of use and transparency for users and enhances user experience
- Moves inspection engines closer to the sessions
- Lowers operational overhead
- Enables zero-trust network access
- Delivers policy-based security services
- Eases operation efforts by providing a single management plane

An ROI of 270% with a Prisma SASE integration



## Key Differentiators

Infosys and Palo Alto Networks provide a comprehensive, cloud-delivered SASE architecture that ensures secure and ubiquitous access to all enterprise applications - whether in private data centers, in public cloud data centers, on the Internet, or in SaaS applications - while continuously strengthening the customer's security posture and accelerating their digital transformation journey.

IT leaders can depend on our joint offerings as it provides a more holistic approach to managing organizational threats and risks by improved threat detection and response, enhanced risk management, greater scalability and flexibility.

For a variety of reasons, we feel Infosys and Palo Alto Networks are regarded as a formidable team:

Palo Alto Networks— is the only vendor to be recognized as a leader in the 2023 Magic Quadrant™ for SSE and 2022 Magic Quadrant for SD-WAN by Gartner.

- Infosys provides best-in-class managed SASE solutions, services, and flexible consumption models wrapped around Palo Alto Networks SASE technology.
- Palo Alto Networks leverages powerful AI and ML capabilities to improve your security posture, network performance, and user experiences, all unified from the same data lake.
- Infosys delivers scale with assurance. By driving an enterprise mindset toward 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
- Palo Alto Networks provides an AI-Powered SASE solution, converging network security, SD-WAN, and Autonomous Digital Experience Management into a single cloud-delivered service.
- Infosys provides best-in-class managed SASE solutions, services, and flexible consumption models wrapped around Palo Alto Networks SASE technology.
- Infosys delivers scale with assurance. By driving an enterprise mindset toward 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
- Palo Alto Networks leverages powerful AI and ML capabilities to improve your security posture, network performance, and user experiences, all unified from the same data lake.
- Palo Alto Networks provides an AI-Powered SASE solution, converging network security, SD-WAN, and Autonomous Digital Experience Management into a single cloud-delivered service.

Together, Infosys and Palo Alto Networks support organizations as they adopt a Zero Trust architecture. By adopting secure access service edge technology, organizations become more risk-resilient and meet the challenge of securing today's hybrid workforce in a rapidly evolving threat landscape.

**Visit our website** to discover more about how our partnership enables organizations to take a fresh, more modernized approach to network and security

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner, Magic Quadrant for Security Service Edge, By Charlie Winckless, Aaron McQuaid, John Watts, Craig Lawson, Thomas Lintemuth, Dale Koeppen, 10 April 2023.

Gartner, Magic Quadrant for SD-WAN, Jonathan Forest, Naresh Singh, Andrew Lerner, Karen Brown, 12 September 2022.

Gartner, 2022 Strategic Roadmap for SASE Convergence, Neil MacDonald, Andrew Lerner, John Watts, 24 June 2022.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant is a registered trademarks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2023 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.