Wipro Managed SASE with Palo Alto Networks

Modernize Your Enterprise for Security, Speed, Growth, and Cost Reduction with Secure Access Service Edge

In the last decade, three fundamental transformations changed the way applications are deployed and managed:

The adoption of cloud and online collaboration

The automation of infrastructure to keep pace with agile business demands

The availability of cost effective, high performance wide area network (WAN) connectivity, such as broadband and 4G/5G.

Many enterprise organizations are moving their workloads to the cloud and cloud-based architectures, considering the lower cost, higher performance, enhanced user experience, and improved agility.

Today, companies collect and process massive amounts of information, ranging from confidential business and customer data, to sensitive intellectual property, to everyday data. They're also storing this data in more places than ever: data centers, public and private clouds, software-as-a-service (SaaS) applications, mobile devices, and more. As a result, many organizations struggle to put in place the right security controls for their data or the right access controls for their applications. Moreover, they struggle with configuring the tools they use to distinguish sensitive data from normal, shareable data.

As more and more enterprise organizations migrate data for enterprise resource planning (ERP) applications to the cloud, it becomes more and more important to address security concerns that pertain to the use of public clouds.

Traditional network approaches and technologies no longer provide the levels of security and access control that digital organizations need.

Secure access service edge (SASE) is a service model that provides the right path for organizations to modernize their enterprise for security, speed, growth, and cost reduction.

Some of the unique challenges that organizations face include:

1. **Legacy architectures:** Networks operating with a traditional non-integrated model lack the performance and agility that's needed for today's workforce dynamics. Enterprises must be able to deliver uninterrupted access for their users worldwide without sacrificing cybersecurity.

2. **Application visibility:** As applications move to cloud-based architectures, organizations need more visibility into application flows, unified policies, and security risks and threats— especially for data at rest, in transit, and in the cloud. As more users connect remotely (e.g., work from home), it becomes more cumbersome to track and enforce security policies and controls. This demands deeper visibility into applications and security controls.

3. **Lowering costs:** With multiple tools for networking and security, enterprises typically struggle against increasing costs. Moreover, it becomes increasingly difficult to maintain multiple disparate point solutions.

Companies often turn to multiple point products to secure web gateways, support application firewalls, secure virtual private network (VPN) remote access, and more. Since these products come with their own policy management protocols, interfaces, and logs, this can create unwieldy administrative issues, increase costs and complexity, and lead to gaps in a company's security posture.

Traditional network approaches and technologies simply no longer provide the levels of security and access control the digital organizations need. These organizations demand immediate, uninterrupted access for their users, no matter where they are located. With an increase in remote users and SaaS applications, data moving from the data centers to cloud services, and more traffic going to public cloud services and branch offices than back to the data centers, the need for a new approach to network security has risen dramatically.

This approach starts with a strong foundation. Secure access service edge (SASE) is a service model that provides the right path for many organizations to modernize their enterprise for security, speed, growth, and cost reduction.

The SASE approach

SASE is the convergence of wide area networking (WAN) with network security services like secure web gateway (SWG), cloud access security broker (CASB), firewall as a service (FWaaS), and Zero Trust Network Access (ZTNA) into a single, cloud-delivered service model. According to Gartner
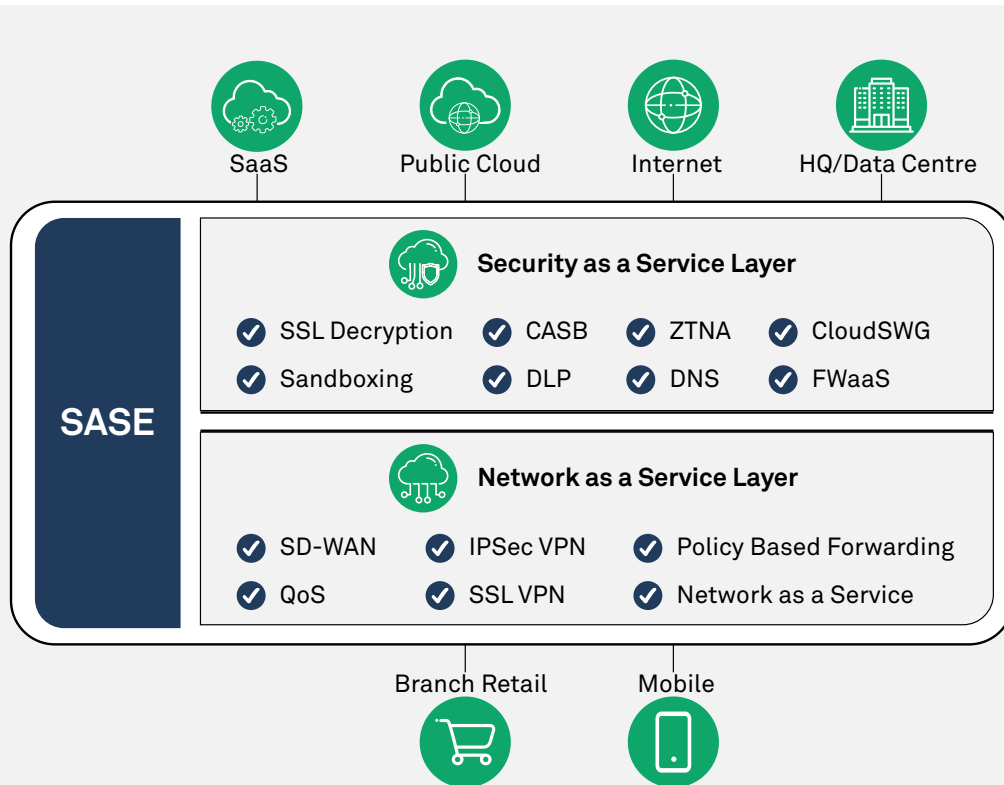

Figure 1: SASE—advanced network and security capabilities in a converged cloud-delivered solution

SASE combines WAN capabilities with comprehensive security functions such as SWG, CASB, FWaaS, and ZTNA to facilitate secure network access in cloud and mobile environments.

How SASE solutions work

A SASE solution provides mobile users, branch offices, and retail locations with secure connectivity and consistent security wherever they are in the world. It does this by offering companies a single, centralized view of their entire network, enabling them to quickly identify users, devices, and endpoints; apply their networking access and security policies; and securely connect users to their applications and data in a cloud or mobile environment, all while ensuring multi-branch and multi-cloud network security.

Different from any legacy system, SASE focuses on the user experiences and helps companies become:

- **Cloud-based,** embedding the agile, adaptive, secure capabilities of the cloud without the need to maintain on-premises architecture. This also allows for the implementation and delivery of security services (e.g., threat prevention, sandboxing, data loss prevention).

- **Identity-driven,** employing a least-privileged access methodology. SASE enables interactions to be controlled within all resources, making security pervasive.

- **Streamlined,** , as SASE includes the delivery of networking and security services with faster provisioning of new services.

- **Global,** as SASE enables global work and remote productivity through low-latency service to all enterprise network edges.

Benefits of SASE

A SASE model can help your organization in several ways.

Rapid Transformation

SASE eliminates the need for appliances to support separate security and networking stacks, simplifying management of the infrastructure. With cloud-based services from diverse geographical locations accessed through a SASE SD-WAN, secure network access will improve dramatically. As a result, users can work securely, accessing the tools and information they need without compromising on performance. This brings the flexibility of cloud-based infrastructure to deliver security and networking.

Enhanced Security

To improve enterprise security, organizations must increase end-to-end visibility. SASE's simplicity enhances security by providing visibility across the entire environment, delivering fully integrated, high-performance, all-in-one security policies that eliminate gaps and redundancies. This approach ensures Zero Trust security and removes trust assumptions when users, devices, and applications connect. SASE provides complete session protection, whether a user is on or off the corporate network. This enables threat prevention with full content inspection integrated into a SASE solution, allowing organizations to benefit from more security and visibility into their network. It improves user experiences by allowing users to immediately gain secure access to a company's network, wherever they are and on whatever device they use.

Immediate and Continuous Savings

Reducing the number of vendors, tools, and technology stacks means SASE can save organizations on their WAN budgets, greatly reducing capital costs as well as overhead expenses typically associated with deploying security and networking at scale. More importantly, it speeds up deployment time and reduces the time to deliver protection by eliminating the need to set up traditional IT infrastructure. It also provides significant return on investment (ROI) through lower operational costs and incident avoidance, along with the flexibility to easily scale up or down remote offices/branches, aligning technology and security with business cycles.

The Palo Alto Networks SASE

Palo Alto Networks brings together Prisma® SD-WAN and Prisma Access to deliver hybrid applications over any network while providing consistent, cloud-delivered security. Prisma Access, the industry's most complete cloud-delivered security platform, protects all application traffic so organizations can safely enable secure remote workforces. It consolidates the best-of-breed security capabilities—including SWG, CASB, FWaaS, ZTNA, and more—into a consistent global service edge that delivers more security coverage than any other solution. Built upon a massively scalable network with ultra-low latency and backed by industry-leading SLAs, Prisma Access ensures a great digital experience for end-users.

Prisma SD-WAN, the industry's first next-generation SD-WAN solution, was built upon an application-defined foundation, using an application session-based approach. This approach provides deep application visibility, with Layer 7 intelligence for network policy creation and traffic engineering, ensuring an exceptional user experience by enabling network teams to deliver SLAs for all apps, including cloud, SaaS, and unified communications as a service (UCaaS). With an app-defined approach, policy, and path-steering decision-making intelligence expands to include Layer 7 information. Prisma SD-WAN makes the secure cloud-delivered branch possible, ensuring exceptional user experience with app-defined policies, simplifying network and security operations using machine learning (ML) and automation, and delivering an **ROI of up to 243%.**

When Prisma Access is combined with Prisma SD-WAN, Palo Alto Networks offers customers the most complete SASE offering, enabling organizations to transform their networking and security infrastructure while realizing market-leading ROI. This SASE solution combines a global high-performance network with next-gen SD-WAN to simplify the delivery of consistent security at scale while ensuring an optimal work-from-anywhere experience.

This SASE service model provides the right path for many organizations to modernize their enterprise for security, speed, growth, and cost reduction, all while increasing application performance, improving the user experience, and reducing complexity. Partnering with Palo Alto Networks for network security and SD-WAN results in significant financial and

organizational benefits, including a **247% ROI over three years.** These benefits are spread across nine different categories, including efficiency gains for IT, security, and end-users; cost savings from sunsetting legacy technology; and the reduced risk of a data breach.

Wipro Managed SASE Services

Wipro #WANFreedom and Lifecycle Services

Wipro's industry-leading **SD-WAN solution** stands head and shoulders above others in the market. #WANFreedom is Wipro's managed SD-WAN offering, powered by Palo Alto Networks' Prisma SD-WAN. **#WANFreedom** goes beyond the distinctions of legacy network architecture and enriches businesses by embracing technologies such as SaaS, cloud, and modern software architecture.

The foundation of #WANFreedom is rich, and actionable analytics gleaned over applications and WAN links. Each application flow is examined for key performance indicators (KPIs) to determine the user experience. Each WAN link is examined to determine availability, utilization, congestion, and service quality to understand how it is performing. This data is visualized in an easy to use cloud management portal—giving you instant visibility into how your applications, sites, and WAN links are performing—and serves as a foundation for the powerful ML algorithms that Prisma SD-WAN Instant-On Network (ION) devices use to determine how application traffic traverses your network. The self-healing characteristics of SD-WAN enable immediate decision making, according to the business policies you define, to give your users the best experience with the least amount of interruption possible.

This SD-WAN solution is backed by Wipro's comprehensive lifecycle services, covering consulting, planning and design, product procurement, implementation, and managed network services.
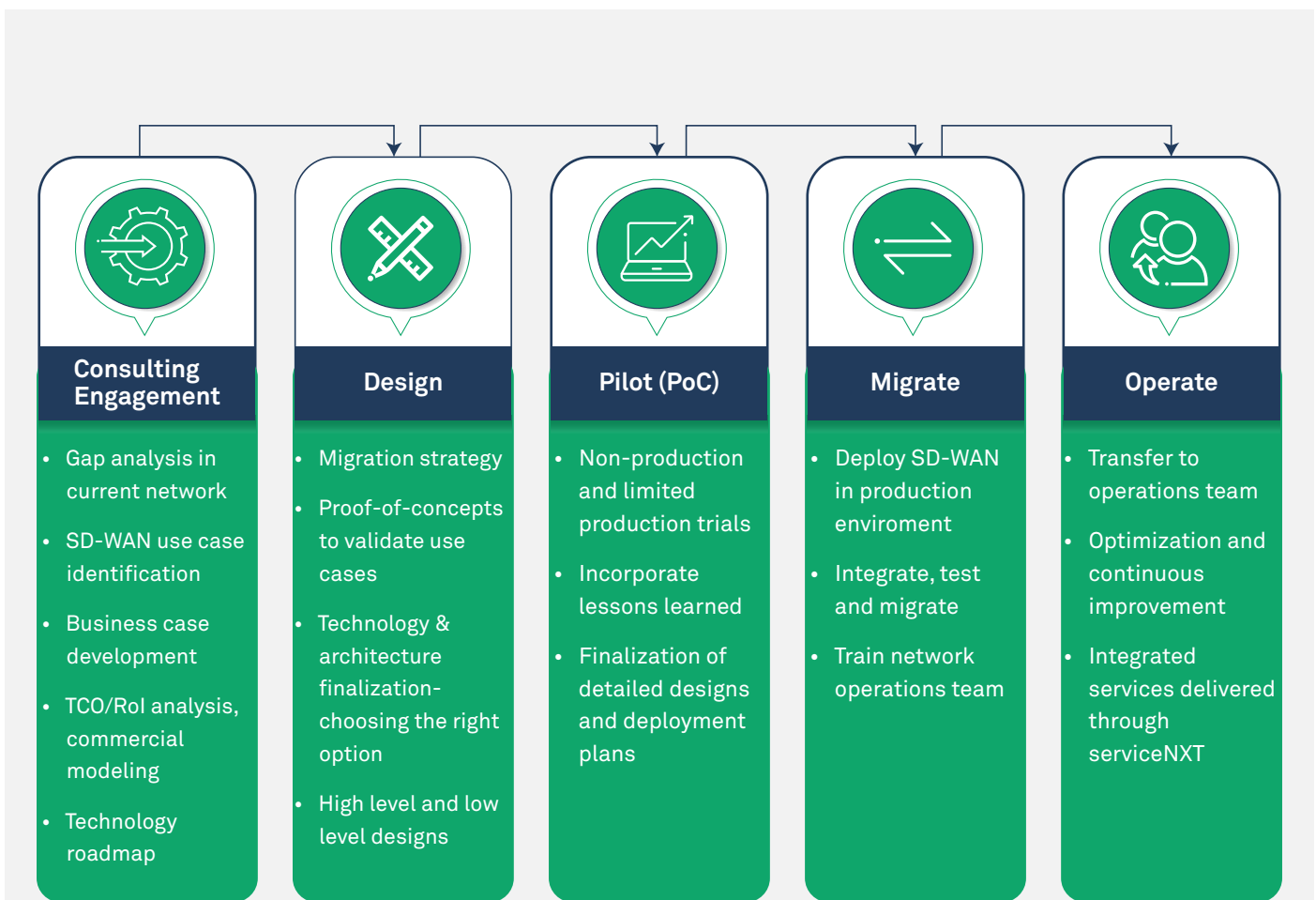
Consulting Engagement	Design	Pilot (PoC)	Migrate	Operate
• Gap analysis in current network	• Migration strategy	• Non-production and limited production trials	• Deploy SD-WAN in production enviroment	• Transfer to operations team
• SD-WAN use case identification	• Proof-of-concepts to validate use cases	• Incorporate lessons learned	• Integrate, test and migrate	• Optimization and continuous improvement
• Business case development	• Technology & architecture finalization-choosing the right option	• Finalization of detailed designs and deployment plans	• Train network operations team	• Integrated services delivered through serviceNXT
• TCO/RoI analysis, commercial modeling	• High level and low level designs			
• Technology roadmap				

Figure 2: SD-WAN lifecycle services

Wipro Integrated Secure Internet Access Services with #WANFreedom

Wipro provides comprehensive Secure Internet Access (SIA) services integrated with #WANFreedom SD-WAN to enable complete SASE services with Palo Alto Networks:
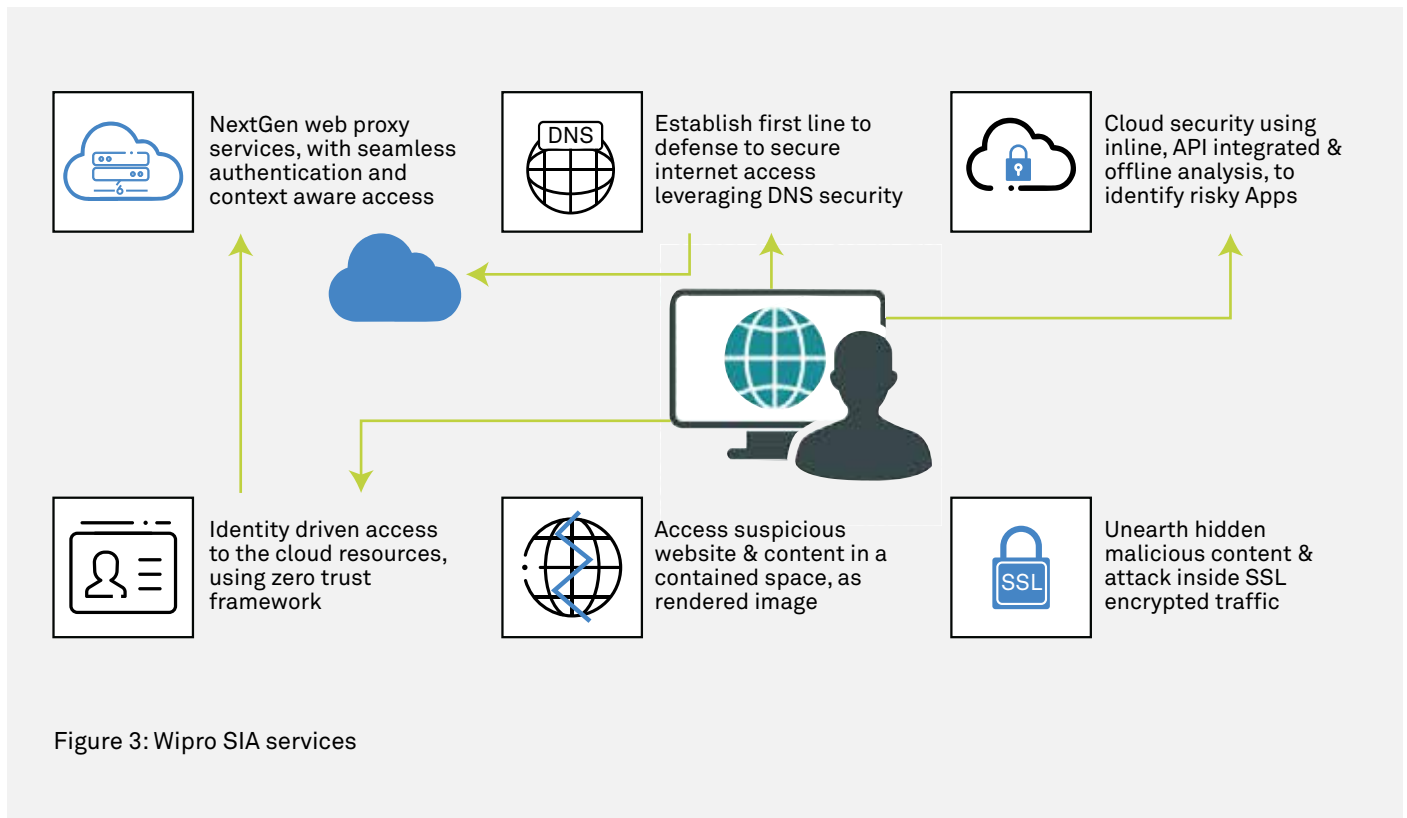
Secure web proxy services: Enable users to access the internet from the cloud, which is scalable, protected from web-based threats, and integrated with SD-WAN.

CASB and reverse proxy services: Secure cloud access and mitigate threats in cloud infrastructure. Enforce identity-driven access to corporate resources.

Threat isolation services: Allow access to uncategorized internet content while preventing endpoint compromises by isolating threats and malware attacks.

NextGen web proxy services, with seamless authentication and context aware access

Establish first line to defense to secure internet access leveraging DNS security

Cloud security using inline, API integrated & offline analysis, to identify risky Apps

Identity driven access to the cloud resources, using zero trust framework

Access suspicious website & content in a contained space, as rendered image

Unearth hidden malicious content & attack inside SSL encrypted traffic

Figure 3: Wipro SIA services

Additional automation with these services enable multiple use cases:

Automated analysis for threats in suspicious websites.

Simulate web access of users using BOT.

Endpoint and web security service monitoring and remediation BOT.

Rerouting of traffic based on proxy auto-config (PAC) file.

Uncategorized website resolution analysis and user access restriction.

Analysis of web traffic for non-productive access.

Identification of non-productive and malicious website access.

Summary

Migrating data and applications to the cloud provides clear benefits, such as lower costs, improved performance, and enhanced agility, but it also presents a set of unique challenges. Legacy architectures slow down the businesses, threat visibility becomes limited, and complex ecosystems of security can be overwhelming and costly to manage. SASE is a model thatprovides the right path for many organizations to modernize their enterprise for security, speed, growth, and cost reduction.

Wipro and Palo Alto Networks have defined a managed service delivered through #WANFreedom and Secure Internet Access services to enable organizations to embrace digital transformation and deliver cybersecurity success with SASE.

If you are interested in learning how Wipro is helping our clients achieve their vision of a modernized enterprise, we should talk.

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 200,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**

IND/BRD/AUG2021-JUL2022