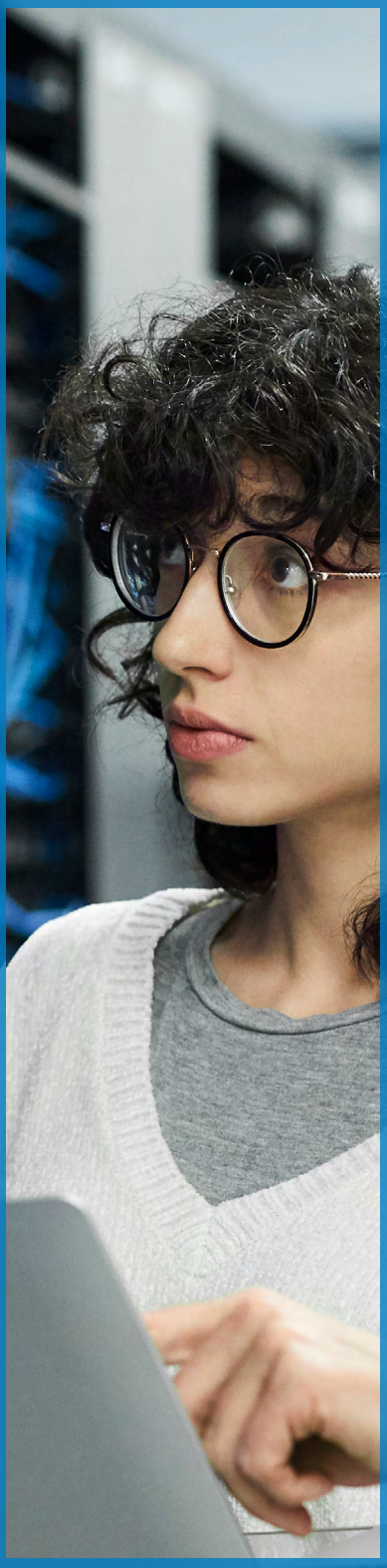
INFOSYS SECURE ACCESS SERVICE EDGE (SASE) OFFERING



Infosys®
Navigate your next

With enterprises transforming to cloud first, internet first and boundaryless architecture strategies, traditional on-prem security, limited internet breakout, and high-cost WAN/MPLS are proving to be constraints in realizing these strategies. Vibrant workplaces, cloudified applications and, digital transformation are demanding simplified and secured access from any device, any application and anywhere.

As internet has become the new enterprise transport, it is extremely difficult to manage user access to enterprise resources securely and efficiently. The traditional castle and moat approach to secure crown jewels is proving ineffective and expensive because most of the IT assets and people have moved outside of the IT perimeter. The perimeter as we knew doesn't exist anymore. Unprecedented events such as the pandemic has further accelerated the need for an effective, efficient, easy to administer, and user-friendly security control mechanism for users and machines allowing seamless connectivity from anywhere across the globe.

Need for Security on Edge

Moving workloads and applications on cloud (public or private) seems inevitable. Backhauling all the traffic to datacenter for security controls is not only adding latency but is also proving to be impractical and costly. Legacy security controls are inelastic and expensive to scale.

Standardization of security controls is critical to ensure the users are protected from advance threats and zero-day exploits. Users working from home, branch or any other location should have seamless experience and standard controls which are easy to deploy and manage by the security admin.

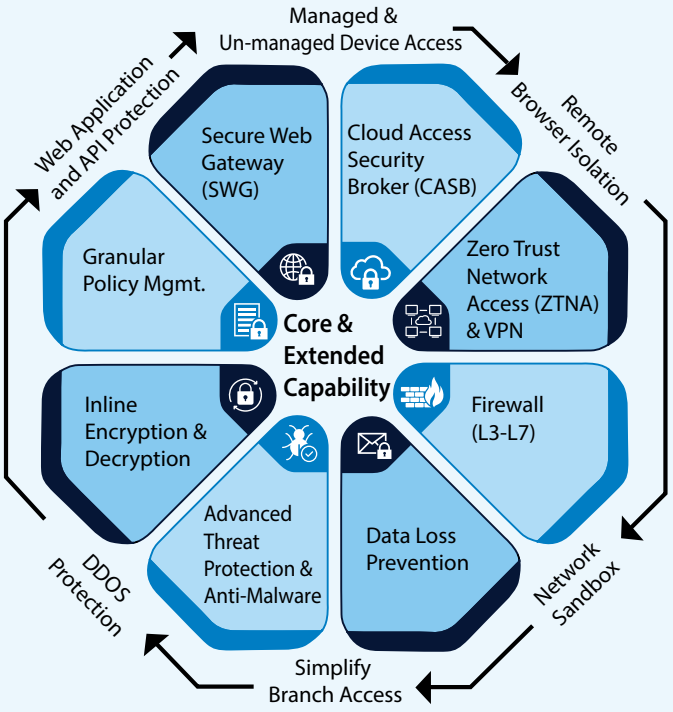
Building a Zero Trust Network Access (ZTNA) mechanism is the need for the hour. Built on least privilege access control policy, ZTNA is the key to secure user access. This can be provided over a secure internet edge avoiding heavy investments on appliances and gears at the datacenter.

Infosys SASE

Infosys offers Secure Access Service Edge (SASE) that provides Zero Trust based access by leveraging best of breed solutions and making it more contextual to bring specific use cases for our clients. It enables enterprise IT resources hosted on cloud and data center to be accessed securely from anywhere.

SASE Offering Features and Capabilities

Infosys SASE solution delivers comprehensive cloud security capabilities in addition to eliminating traditional and high cost on-prem solution components such as firewall, proxy and VPN gateway. With the Infosys SASE offering, we deliver end-to-end zero trust security, minimize threat posture and maximize user experience.



Secure Web Gateway
URL filtering| Enforce policy control | Application control I Remote browser Isolation

Cloud Access Security Broker (CASB)
Protect sensitive data | Threat protection | Greater visibility

Zero Trust Network Access
Identity-based | Micro segmentation | Posture validation

Firewall
Deep packet inspection | Intrusion prevention |App level

Data Loss Prevention
Pattern and keyword matching | Integrate with SIEM | Cloud-based

Advanced Threat Protection & Anti- Malware
Real time visibility | Context Aware | Data Awareness

Inline Encryption
Secure data in Motion | Enhanced User Experience

Granular Policy Management
Location or device specific access control policies | Cloud-based

Infosys SASE Offering Highlights

Zero Trust Network Access

Enhanced security capabilities with cloud centric security controls applied with Zero Trust Network Access (ZTNA) architecture that eliminates high cost and complex on-premise security solution controls/devices

Security as-a service model

Security as-a service model – Enables to scale the controls and extend security 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

Enhanced user experience

Enhanced user experience due to light weight agent on device, minimized network and security interventions, improved latency with optimized routing and granular policy implementation

Network simplification

Network simplification by reducing WAN/ MPLS complexity, backhauling and driving internet first culture

Strategic Partnership

Technology, architecture and global coverage are the key considerations for SASE adoption. We have built global strategic relationship with leading SASE technology providers - Zscaler, Palo Alto Networks and Cisco. As one size does not fit all, we adopt the client first approach to assess the current state, use cases and then propose a potential fit for purpose solutions.

Comprehensive Services Aligned to 4D Methodology

We have invested and built a large talent pool and ready to deliver, reusable assets in SASE solution which are aligned to our 4D approach – Diagnose (consulting), Design (HLD & LLD), Deliver (deployment & migration) and Defend (operation and optimize).

Diagnose

- Assess current security controls and user profiles
- Review current proxy, VPN, network topology and IT resource access
- Access gaps and issues with reference Zero Trust Network Access
- 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 (HDL)
- 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 for 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, ATP, 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

Assured Benefits

- Advanced threat protection with reduced threat posture
- Standardized, simplified and granular policy management
- Delivered as-a-service model
- Assured cost savings >30%
- Eliminated/minimized MPLS/WAN cost

To know more about Infosys SASE Service, scan the QR Code

For more information, contact askus@infosys.com

Infosys®
Navigate your next