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.

### Core & Extended Capability
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Zero Trust Network Access (ZTNA) & VPN
- Firewall (L3-L7)
- Data Loss Prevention
- Inline Encryption & Decryption
- DDOS Protection
- Granular Policy Mgmt.
- Advanced Threat Protection & Anti-Malware
- Simplify Branch Access
- Network Sandbox
- Simplify Branch Access

<table>
<thead>
<tr>
<th>Feature</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure Web Gateway</strong></td>
<td>URL filtering</td>
</tr>
<tr>
<td><strong>Cloud Access Security Broker (CASB)</strong></td>
<td>Protect sensitive data</td>
</tr>
<tr>
<td><strong>Zero Trust Network Access</strong></td>
<td>Identity-based</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>Deep packet inspection</td>
</tr>
<tr>
<td><strong>Data Loss Prevention</strong></td>
<td>Pattern and keyword matching</td>
</tr>
<tr>
<td><strong>Advanced Threat Protection &amp; Anti-Malware</strong></td>
<td>Real time visibility</td>
</tr>
<tr>
<td><strong>Inline Encryption</strong></td>
<td>Secure data in motion</td>
</tr>
<tr>
<td><strong>Granular Policy Management</strong></td>
<td>Location or device specific access control policies</td>
</tr>
</tbody>
</table>
**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 lightweight 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.
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).

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

• 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

• 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

• 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

Diagnose

Design

Deliver

Defend
Strategic Partnership
Technology, architecture, and global coverage are the key considerations for SASE adoption. We have a strong global strategic relationship with Zscaler, a leading SASE technology provider. 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.

Why Zscaler SASE?
In the SASE Zscaler Cloud Security Platform, the SASE service is built from the ground up for performance and scalability. As a globally distributed platform, users are always a short hop away to their applications, and through peering with hundreds of partners in major internet exchanges around the world, Zscaler ensures optimal performance and reliability for your users. Today, more than 400 of the Forbes Global 2000 organizations trust Zscaler to lead them into the digital era, securely. Because of its time in the market, Zscaler has proven its architecture was built to scale, currently processing up to 120B+ transactions at peak periods and performing 175K+ unique security updates each day. The Zscaler SASE architecture is delivered across 150+ data centers globally, ensuring that users get secure, fast, and local connections no matter where they connect.

Key Capabilities

A cloud-first architecture
The Zscaler SASE architecture helps accelerate cloud adoption by removing network and security friction through a consolidation and simplification of IT services. Without the need for device management and separate services, Zscaler offers a frictionless and transparent experience for users and standardization across locations for the IT team.

Full inline SSL inspection at scale
With majority of traffic encrypted today, you need a proxy-based architecture that can scale for effective threat protection and data loss prevention.

Application peering and optimization
Zscaler globally peers at the edge with leading application and service providers and optimizes traffic routing to provide the best user experience.

Zero Trust Network Access
Zscaler provides a user- and application-centric approach to application access. A fully cloud-delivered service, Zscaler provides native app segmentation by using business policies to connect an authenticated user to an authorized app without bringing the user on the network.

Zero attack surface
Adversaries can’t attack what they can’t see, which is why the Zscaler architecture hides source identities by obfuscating their IP addresses and avoids exposing the corporate network to the internet.
Zscaler SASE Benefits

- **Reduces IT cost and complexity**: Easy to deploy and manage as an automated, cloud-delivered service that scales.
- **Delivers a great user experience**: Brings security and policy close to the user to eliminate unnecessary backhaul.
- **Reduces risk**: Inline inspection of encrypted traffic at scale for threat protection and data loss prevention.

- **Multi-tenant Architecture**: Elastic scale, data privacy.
- **Zero Attack Surface**: IPs/Network not exposed to the internet.
- **Operational Excellence**: 10+ years running an inline cloud service.
- **Proxy Architecture**: SSL inspection at scale.
- **Zero Trust Network Access**: Native app segmentation.

Secure Access Service Edge
Compute at the edge – fast, peering.

Products / Services
Platform Services

External Document © 2022 Infosys Limited