

# Secure Access Service Edge (SASE)

Secure, software-defined connectivity  
with next-gen solutions built on zero trust and AI



# Overview

Traditionally, the data center has been the cornerstone of enterprise network security. However, as businesses accelerate their digital transformation, the access demands of users, devices and applications have far outgrown the limits of a centralized model. Work is no longer tied to a physical office—it's an activity we carry out anywhere and everywhere. Whether remote employees, branch offices or IoT devices, today's workforce and systems need seamless access to the internet, SaaS platforms, cloud applications and internal resources to function effectively.

This proliferation of access points has brought about a new wave of secure access challenges that demand a holistic and future-proof solution. Secure Access Service Edge (SASE) offers a transformative architectural approach designed to unify and elevate network security in today's dynamic digital environment. Unlike traditional point-based security models, SASE streamlines essential networking and security services into a single, AI-driven, cloud-delivered platform. This convergence integrates technologies like SD-WAN, Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA). The result? Highly secure, consistent and scalable access—no matter where users, data or applications reside.

SASE empowers organizations to transform their networks and security capabilities into catalysts for growth and agility. By addressing critical challenges such as zero-trust access for remote employees, secure internet access for branch offices and seamless multicloud migration, SASE positions businesses to meet the future head-on. With its adaptability to diverse use cases, organizations can modernize securely while staying resilient in the face of ever-evolving IT complexities. Building on a foundation of flexibility and innovation, AI-enabled threat detection and response amplify SASE's ability to safeguard organizations' networks and applications. This advanced capability empowers businesses to stay ahead of threats, delivering proactive protection in an increasingly complex digital landscape.



# Challenges with the traditional approach



The digital era has reshaped how organizations operate, collaborate and innovate. Yet, traditional security models struggle to keep pace with this shift, creating roadblocks toward seamless and secure enterprise environments. Identifying these challenges isn't just about understanding the obstacles—it's about uncovering opportunities to build more innovative, resilient solutions.



## **Complexity in managing distributed environments:**

As enterprise applications expand across hybrid cloud infrastructures, including on-prem data centers, remote offices and multicloud ecosystems, businesses face unprecedented complexity. Traditional security architectures, built on rigid frameworks, falter under these demands, unable to enforce standardized policies and protect assets comprehensively.



## **Limited visibility into network, device health and user activity:**

Legacy solutions like remote access VPNs lack the granular, app-level controls needed to monitor and manage user behavior after they enter the network. Visibility gaps in traffic patterns, device health and user activity leave organizations exposed to risks that could compromise data integrity and asset protection.



## **Inadequate defense against advanced cyber threats:**

The age of 5th generation threats, marked by multi-vector mega attacks such as WannaCry and NotPetya, demands more than yesterday's defenses. These sophisticated attacks exploit the interconnected nature of enterprise ecosystems, targeting networks, cloud workloads, IoT devices and third-party systems. Traditional approaches often lack the agility and intelligence to counter these threats effectively. Meeting this challenge requires a bold, forward-looking security strategy that evolves faster than the threats themselves.



## **Poor user experience hampers productivity:**

Legacy hub-and-spoke architectures introduce latency by backhauling traffic from remote locations to centralized data centers. The result? Frustrated users, delayed access to cloud applications and diminished productivity. The digital future hinges on delivering fast, reliable connectivity to empower users and redefine what seamless experiences can mean for enterprises at scale.



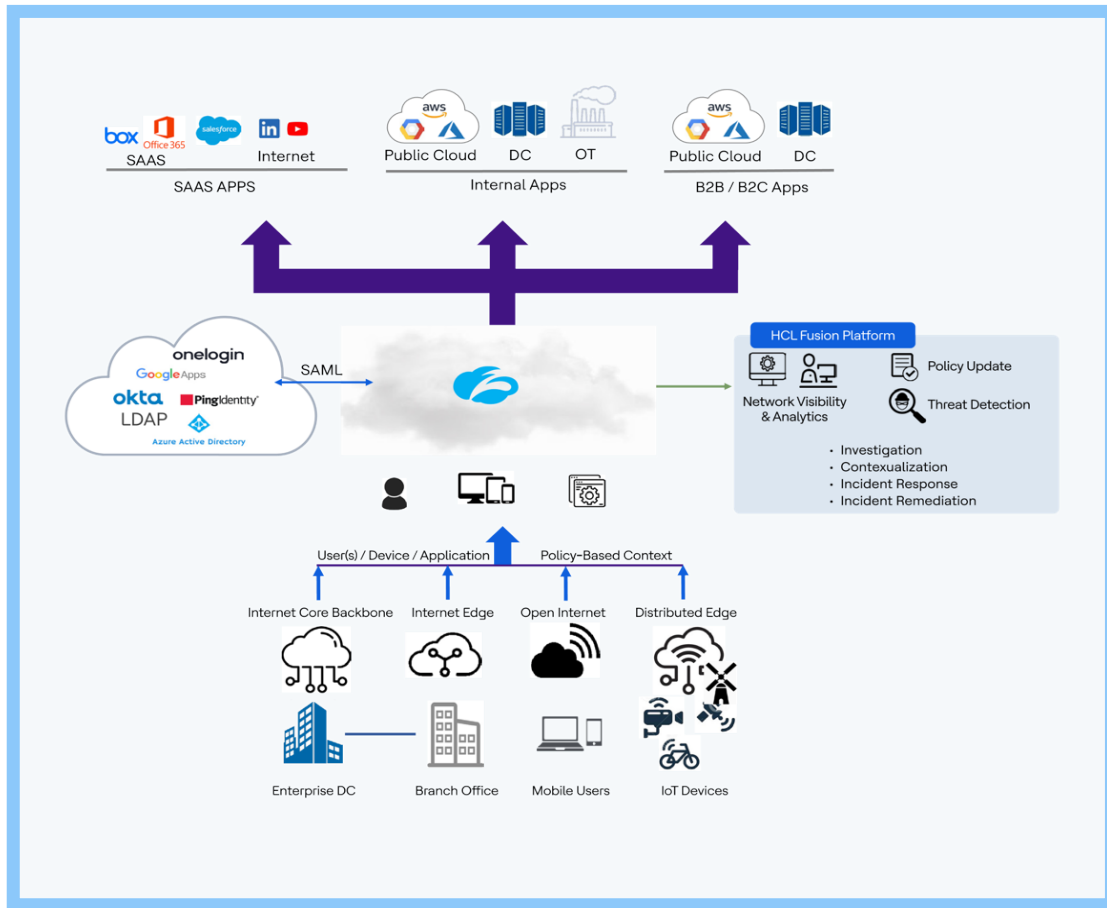
## **Visibility and compliance challenges in a dynamic landscape:**

End users are accessing critical applications and data from various locations, devices and networks, many of which are potentially risky. Organizations risk regulatory compliance failures and increased potential for data breaches without proper visibility and control. Addressing these vulnerabilities isn't just a matter of meeting standards—it's about building trust, protecting reputations and enabling fearless innovation in compliance-heavy industries.



# Our solution

HCLTech managed SASE combines comprehensive WAN capabilities with robust network security functions to support digital enterprises' dynamic, secure access needs. By harnessing the power of zero trust and AI, we enable organizations to strengthen and automate IT operations and security, reduce operational costs and simplify the complexity of managing a distributed workforce.



HCLTech Managed SASE integrates network security, SD-WAN and digital experience management into a unified, cloud-delivered service. This forward-thinking architecture revolutionizes how businesses securely connect users, devices and applications—delivering fast, reliable and flexible access to SaaS, enterprise applications and the internet from anywhere while ensuring an unparalleled user experience.

Legacy solutions often fall short in an interconnected world of hybrid workforces, edge computing and cloud migration. HCLTech reimagines the paradigm with a robust suite of next-generation capabilities:



**ZTNA**  
(Zero Trust  
Network Access)



**SWG**  
(Secure Web  
Gateway)



**FWaaS**  
(Firewall as a  
Service)



**CASB**  
(Cloud Access  
Security Broker)



**DLP**  
(Data Loss  
Prevention)



**DNS**  
security



**RBI**  
(Remote Browser  
Isolation)



**Digital**  
experience  
monitoring

Our Managed SASE services simplify and fortify enterprise security by:

**Connecting all users to all apps securely** using fine-grained access controls to reduce the attack surface significantly.

**Continuously verifying trust** based on behavior and context, ensuring that users and devices maintain the highest security posture.

**Delivering deep, automated traffic inspection** without sacrificing performance or user experience.

Offering end-to-end **visibility across endpoints, networks and applications**, enabling proactive issue detection and resolution.

**Safeguarding all types of applications**—whether premises-based, internet-based, legacy, SaaS or modern cloud-native—through a single, integrated platform.

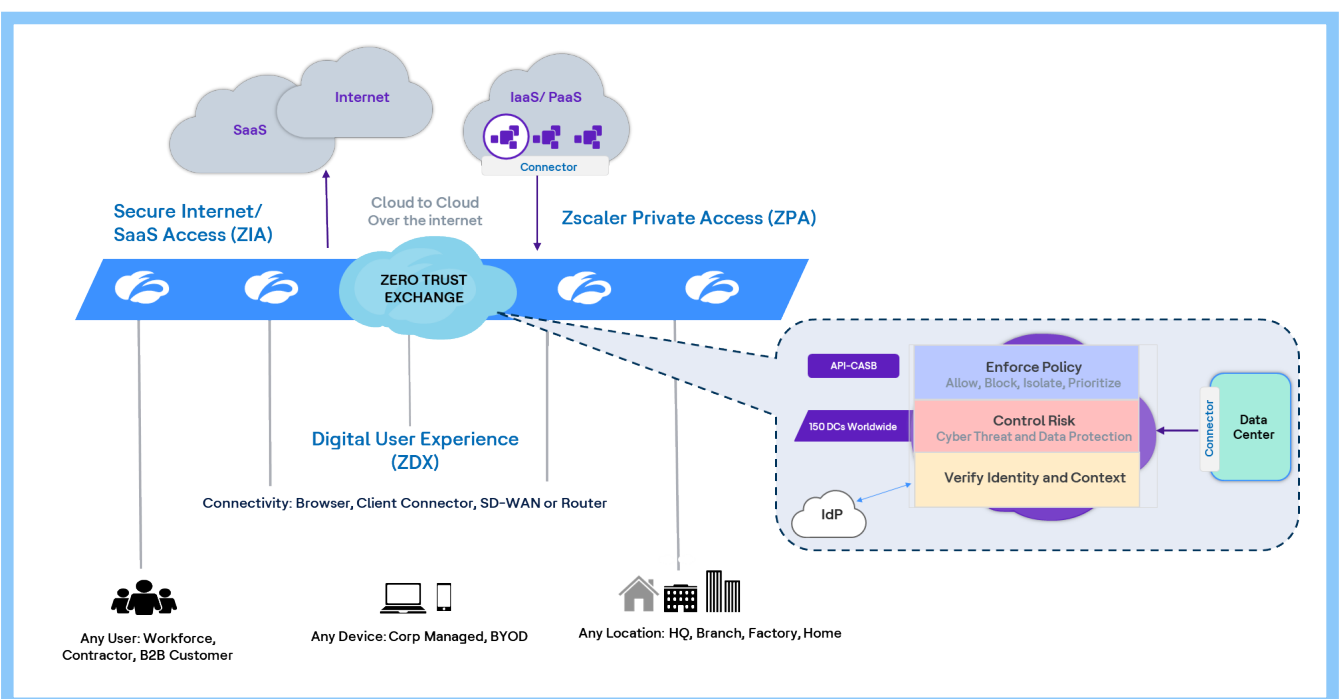
Supporting **multi-use case scenarios**, including secure access for branch offices, roaming employees, IoT devices and unmanaged endpoints.

HCLTech ensures organizations can adopt zero-trust application access for users and devices and secure outbound traffic to SaaS platforms or the Internet. Our SASE offering creates a seamless, secure connective fabric that spans physical locations, virtual sites, clouds and distributed networks. Our solution supports integrations with leading identity providers, including Okta, Azure AD and Ping Identity, to enhance user authentication.

To deliver unparalleled Managed SASE capabilities, HCLTech partners with Zscaler, uniting our expertise with Zscaler’s advanced Zero Trust SASE platform. The Zscaler architecture eliminates the inefficiencies and risks of legacy, network-based security models, offering:

- Least-privileged access for workforces, IoT, workloads and partners.
- A purpose-built, cloud-native platform that removes fragmentation and simplifies security.

HCLTech and Zscaler ensure businesses can step boldly into the future, bypassing traditional bottlenecks with seamless, AI-powered innovations.



# Solution features

HCLTech Managed SASE services, powered by Zscaler's cloud-native security platform, are a visionary service designed for agility, resilience and growth. Some of the key features include:

## **Cloud-first, zero trust architecture:**

Accelerates cloud adoption by removing network and security bottlenecks, consolidating IT services and eliminating the need for excessive device management.

## **HCLTech SPADE enterprise assessment framework:**

We identify areas of strategic importance to map out a customized SASE-centric transformation roadmap.

## **AI-powered risk engine:**

AI capabilities like security copilots, zero-day threat detection, malware identification, digital experience enhancement and CTEM ensure future-ready security and operational effectiveness.

## **Zero-trust networking:**

Zscaler's zero-trust SD-WAN connects branches, factories and data centers without routed overlays or inherent trust, delivering app-level access without exposing sensitive networks.

## **Zero attack surface:**

Our architecture protects businesses from being targets by obfuscating IP addresses and concealing the corporate network from external visibility, enabling seamless, secure connectivity.

# Comprehensive solution to drive success

HCLTech delivers a full suite of Managed SASE services to ensure a risk-prioritized, customized and scalable solution that evolves with your enterprise needs.

## Strategy and Consulting services

- **Assessment:** We analyze your security and network posture using in-depth visibility to create a risk-prioritized SASE adoption roadmap.
- **Roadmap design:** A tailored SASE implementation path, including clear timelines for transformation.

## Transformation and Integration Services

- Implementation of the right mix of network and security controls.
- Integration of remote users, branch offices, IAM solutions and threat detection and response platforms with SASE.
- Policy consolidation and streamlining for consistency and simplification.



## Managed services

- Continuous management, monitoring and optimization of the SASE platform.
- SASE policy updates to reflect organizational or threat landscape changes.
- 24/7 threat detection and monitoring for enterprise peace of mind.
- Incident response and migration services to ensure resilience in the face of evolving risks.

## Benefits of SASE adoption



Reduces complexity and costs due to numerous point solutions



Improves performance and eliminates latency



Enables new digital business scenarios



Offers secure access for a mobile workforce, branch users and protects from 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 operational efforts by providing a single management plane

## Key differentiators

HCLTech leverages its home-grown enterprise assessment framework, SPADE, to identify the areas of the most effective imperatives and delivers a transformation roadmap around SASE-centric architecture.

HCLTech offers the best-in-class managed SASE solutions, services and flexible consumption models

Our approach is based on an agile service delivery model, which enables enterprises to adapt, scale and innovate without compromise. We pair this agility with deep expertise and operational excellence to meet the dynamic demands of modern business environments.

Through trusted partnerships with industry-leading vendors, we deliver SASE solutions with 99.999% uptime, ensuring resilience, high availability and uninterrupted protection for your most critical workloads.

Our experienced consultants bring strategic and tactical expertise, empowering enterprises with tailored cybersecurity program evaluations and actionable strategies that work in the real world.

At the forefront of innovation, we've woven AI-driven intelligence into our zero-trust architecture. This means our security posture evolves dynamically to counter modern threats, leveraging AI-enhanced policies that proactively block even AI-enabled cyberattacks.

To learn more about the HCLTech and Zscaler partnership, [visit our partnership page](#)

**HCLTech** | Supercharging  
Progress™

[hcltech.com](https://hcltech.com)