HCLTech | zscaler

Supercharging Progress™

HCLTech's **Zero Trust** model for Secure Access

Modern, secure and seamless access to any application

With exponential increase in the cloud adoption models, enterprise borders have blurred leading to an increase in threat vectors. In a traditional "castle and moat" architecture, enterprises used to control complete access via their own data centers and all the users connecting from anywhere were backhauled through these data centers for the purpose of authentication and enforcing the security policies. However, currently enterprises across the globe need to access applications in hybrid and multi-cloud environments. Traditional network and security architecture thus need to transform to enable cloud, mobility, and work-from-anywhere models. This has led to cloud-delivered zero trust-based security framework, where not only the external users but even internal users are not given access without complete authentication.

*"By 2025, at least 70% of new remote access deployments will be served predominantly by Zero Trust Network Access (ZTNA) as opposed to VPN services, up from less than 10% at the end of 2021, according to Gartner."

Challenges with the traditional approach

01

Complexity due to widely distributed environment

Due to enterprise applications and resources spread across hybrid cloud (on-premise data centers, branches, and remote offices) and multi-cloud environments, traditional security solutions are incapable of handling this level of intricacies and thus can't enforce security policies in a standard manner across the enterprise environment.

02

Accessibility gap in legacy network security technology

VPNs used by organizations face numerous limitations in modern cloud-based world, as they expose the entire network to any authentic user thereby leading to chances of insider threats.
Point VPN devices are expensive to deploy and complex to manage.

03

Limited or no visibility into network, device health, and user activity

Remote Access VPNs are short of app-level controls and have no visibility into the users' movement once they have entered the private network, the traffic patterns, as well as the connecting devices' health status. This lack of visibility can compromise the whole network resulting in the risk of data theft or leakage

04

Inadequate performance and scalability of VPNs

Backhauling the entire traffic through the centralized data center via VPNs, even when it's destined for cloud or internet, adds to latency and poor user experience.
Also, VPNs are difficult to scale in the rapidly increasing remote workforce scenario.

05

Risk from third parties and advanced threats

Legacy perimeter-based security solutions tend to extend an organization's network to third parties thus exposing sensitive data to the third-party users. This results in a massive security hole for the organizations as they largely access applications using unmanaged devices.

Also, account compromise is a major threat from cybercriminals, where they can access and steal sensitive information by exploiting the blind spots in traditional network architectures.

The HCLTech approach

For the right security posture of an enterprise having a hybrid or a multi-cloud environment, HCLTech recommends deploying a Zero-Trust based Network Architecture for all kinds of user access to private, SaaS and other public cloud applications. All the security policies across an enterprise's data/ applications residing anywhere in the cloud (public and private) are applied based on a context that is further established through least-privileged access and stringent user authentication controls. A Zero-Trust based framework with a cloud led approach simplifies the network security architecture while providing better user experience and advanced threat defense.

At HCLTech, we believe that a comprehensive zero trust approach encompasses users, applications and data, and infrastructure so our ZTNA solution is based on the below principles and solutions-

Asset discovery and visibility

For providing the right access to the enterprise assets to the right people, discovery and classification of data, assets, applications, and services should be done to define their priority based on their criticality. Complete visibility across Shadow IT assets and the IoT environment should be available to the IT practitioners. HCLTech solution enables delivering continuous discovery and visibility of cloud resources, to identify gaps between an organization's desired baselines and current posture to mitigate any potential risks arising out of any existing vulnerability. HCLTech recommended Cloud Security Posture Management (CSPM) enables automatic discovery of all the deployed resources on cloud across compute, storage, user accounts, subnets, gateways, load balancers, etc.

Micro-segmented access for users

Least privilege access policies with strong authentication controls should be applied while users are given access to any critical/ non-critical application hosted on the cloud. The security posture of the device used should also be checked against the security policies for user device integrity. This can be enabled by deploying least privilege access controls on user's devices, enabling multi-factor-based authentication mechanism for additional user verification, and verification of non-corporate device through mobile device management solutions. HCLTech provided services can detect overly permissive access and suggest corrections to reach least-privilege entitlements. It also includes out-of-the-box policies that govern IAM best practices to help configure the correct level of privileges for enterprise cloud-native deployments. HCLTech ensures compliance to zero trust principles by helping implement per-user and per-app granular access policies for application access..

Application

In a zero-trust approach, applications shouldn't be published to the internet/ intranet and a user-to-app access should be provisioned based on the role-based access control policies. Identity and context-based access should be enabled for all enterprise and SaaS apps with continuous monitoring to verify and validate their behavior. Direct and secure user-to-app and app-to-app connections help eliminate the risk of lateral movement of a malware and prevent compromised devices from infecting other resources. It also keeps users and apps invisible to the internet, thereby reducing the threat attack surface.

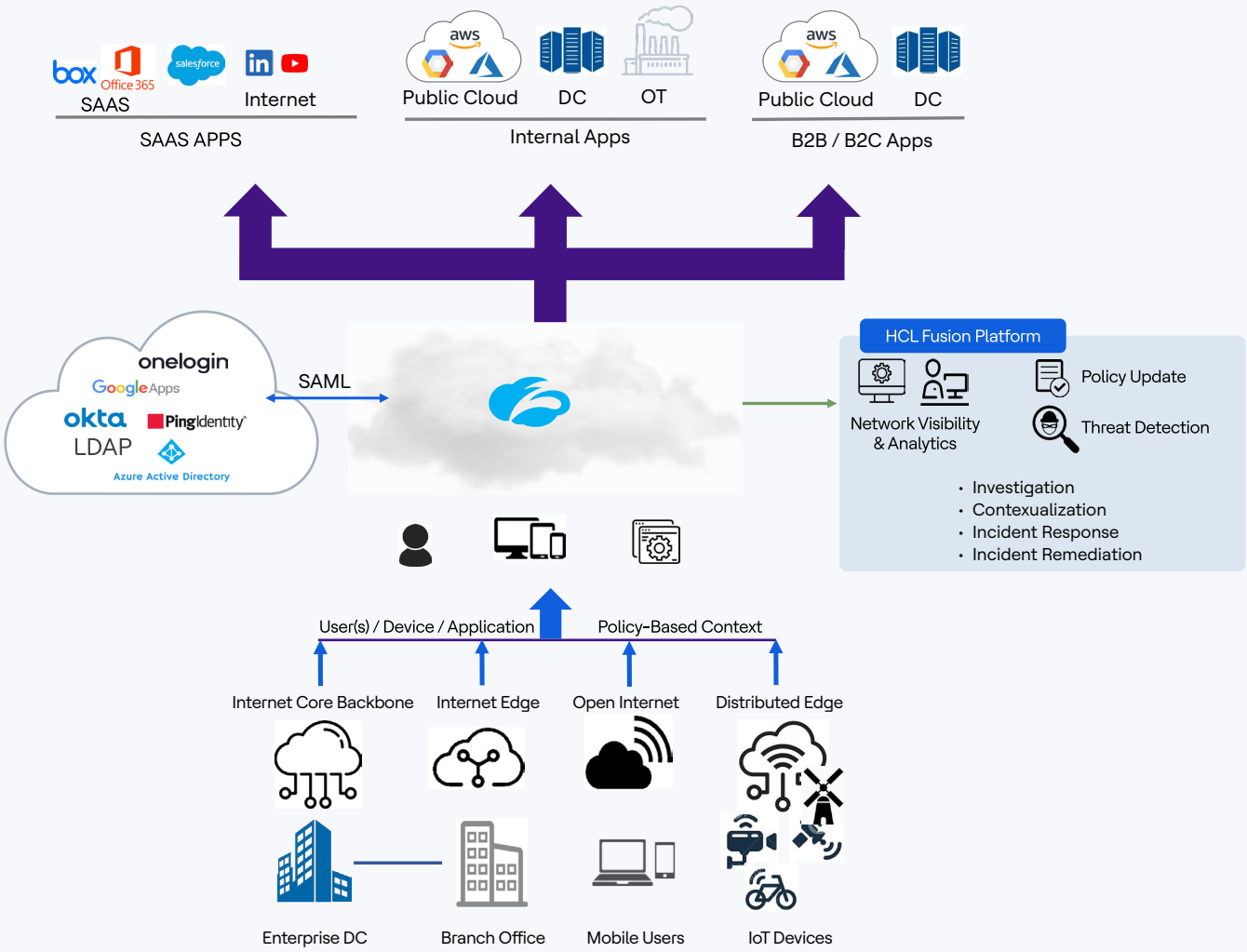
Infrastructure

The exponential use of microservices needs monitoring of east-west traffic passing through the workloads and allowing only the legitimate traffic to pass through based on the security policies. Micro-segmentation and Nano-segmentation techniques enable logical division of a private/ public cloud environment into distinct security segments up to individual workload level and then define the security policies and deliver services for each unique segment. Our services comprising of ZTNA and Workload Segmentation help provision in-depth application flow visibility, network visibility and threat detection and prevention capabilities. The solution enables instant protection against most file and web-based unknown threats—as well as zero-delay signatures for near-real time protection against newly seen threats.

Solution overview

HCLTech service is based on the facts that internet should be made available as a secure network without the need for traditional VPN, and corporate network should not be extended to remote users. In addition, internal applications should be invisible and not exposed to Internet where micro-segmented access from user to application is provided. Hence HCLTech recommends its clients to have a remote access solution based on Zero-Trust Network Architecture, where only authorized users are given access, and that to the applications and not the complete network. This makes the user experience better as they can swiftly and seamlessly access the respective applications irrespective of their location.

Such an access to internal applications is provided by a software-defined solution, powered by Zscaler Private Access. When an authorized user requests access to an internal application, the Zscaler policy engine enables a lightweight application layer-based tunnel through the Zscaler cloud. This tunnel is an encrypted channel and protects the application access from any kind of man-in-the middle attack or unauthorized access. HCLTech services provide complete protection of the traffic hitting the enterprise applications hosted in a private/ public/ multi-cloud environment ensuring users will get full protection from web and internet threats. Along with that, features like Cloud Sandboxing, Next-Generation Firewall, Data Loss Prevention, and Cloud Application Visibility and Control can also be utilized as per need basis. Backed by HCLTech Managed Services with respect to deployment and support, this approach will help customers to ensure security with enhanced user experience.



Key features of solution

Zero attack surface and data loss prevention
By using direct-to-cloud architecture to take traffic off the corporate network, applications become invisible to cyber threats reducing the risk of data loss. Threat actors cannot attack what they cannot see!

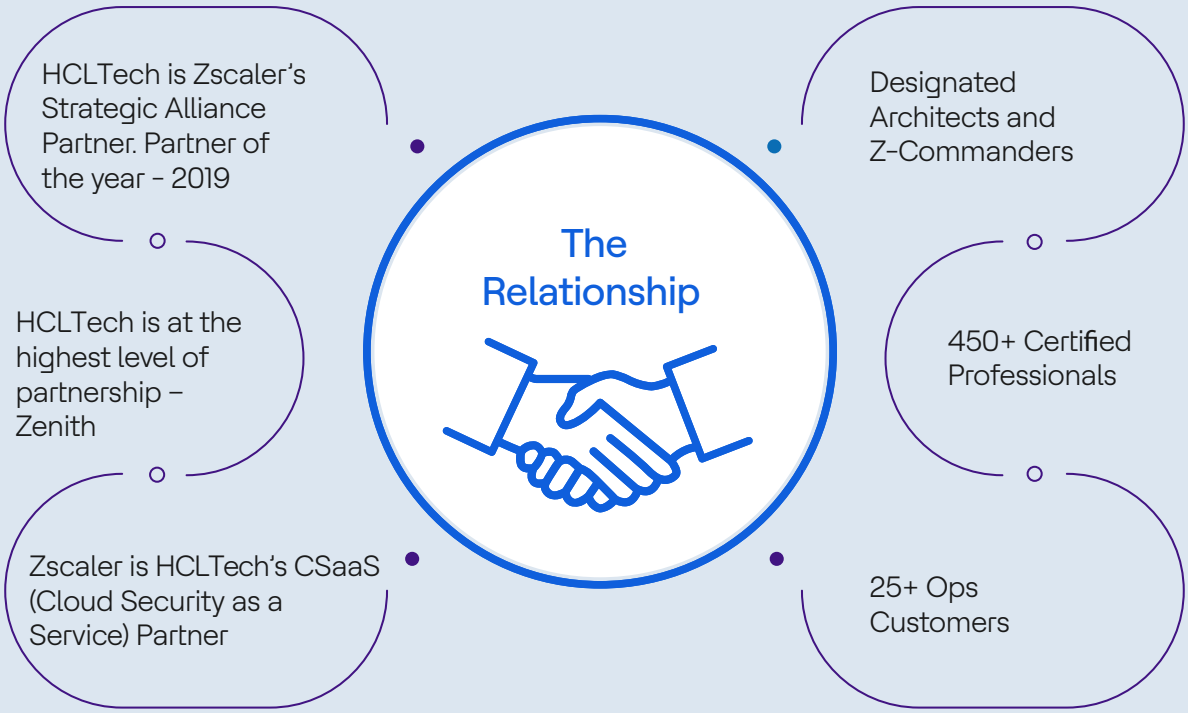
Simplified cloud connectivity
The Zero Trust architecture also avoids performance bottlenecks as IP overlap issues are removed, route distributions are no longer needed, and workloads are directly connected to the internet to other applications.

Superior application performance at scale
HCLTech services are built on a truly distributed architecture where every communication that reaches the service edge gets processed instantly for identity and context ensuring the shortest path between applications no matter where they are hosted, reducing latency and improving application performance.

Full visibility, end-to-end, with direct-to-cloud connectivity
With direct connectivity to the cloud, enterprises get full visibility and control over how workloads communicate. Logging is centralized and streamed in real time, and logs are exported to the HCLTech Cyber Security Fusion Platform for advanced analytics.

Real time detection
The comprehensive solution provides real time detection of compromised users and apps under attack. Full inspection provides a deep layer 7 visibility to contain top threat vectors.

HCLTech and Zscaler partnership



HCLTech – Zscaler capabilities

The transformation journery...

Phase 1 Consult, Plan & Design	Phase 2 Implement	Phase 3 Operations

• Infrastructure & Cloud Security Consulting
• CyberSecurity CoE
• Dedicated HCLTech SMEs
• Dedicated Zscaler Architects
• Joint specialized offerings on Zscaler Products
	• 20+ active deployments
	• 300,000+ users migration from legacy to cloud-based solutions
	• 3 Z Commanders
	• Deployments across verticals:
	  • RTCPG
	  • Healthcare
	  • BFSI
	  • Energy
	  • Manufacturing
		• 24*7 Monitoring & Management
		• Facilitating Reporting options
		• Run Book management
		• RACI execution

HCLTech | Supercharging Progress™

BE-112206AII734735745195-EN00GL

hcltech.com

HCLTech is a global technology company, home to 219,000+ people across 54 countries, delivering industry-leading capabilities centered around digital, engineering and cloud, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending September 2022 totaled $12.1 billion. To learn how we can supercharge progress for you, visit hcltech.com.