

HCLTech managed SSE solution in partnership with Cisco



Overview

HCLTech's managed SSE solution empowers organizations to navigate the rapidly evolving cybersecurity landscape through a robust and zero trust architecture designed to enhance security, streamline operations and reduce complexity. This solution integrates industry-leading technologies, ensuring expansive visibility, seamless access and effective protection against modern threats while driving digital transformation. Additionally, HCLTech provides ongoing management and optimization of security policies, enabling organizations to adapt swiftly to new threats and regulatory requirements, ensuring resilience in a dynamic digital environment.

Market Trends

65%



Enterprises are expected to consolidate their individual SSE components into one or two explicitly partnered SSE vendors by 2025, up from 15% in 2021, reflecting a trend towards streamlined vendor relationships and reduced operational complexity.

[Source](#)

80%



Enterprises will adopt a strategy to unify web, cloud services and private application access using a Security Service Edge (SSE) architecture by 2025, significantly increasing from just 20% in 2021, underscoring a pivotal shift towards integrated cybersecurity solutions.

[Source](#)

50%



SD-WAN purchases will be associated with a single vendor SSE offering by 2025, a sharp rise from less than 10% in 2021, indicating a growing preference for comprehensive vendor solutions that integrate multiple security functions.

[Source](#)

17.30%



The zero trust market is anticipated to grow at a CAGR of 17.30% between 2023 and 2028, demonstrating a rising recognition of the need for stringent security measures that adopt a "never trust, always verify" philosophy.

[Source](#)

\$25 billion



The global SSE market size is projected to grow at a compound annual growth rate (CAGR) of 29%, by 2027, highlighting the increasing investment and focus on advanced security frameworks as businesses adapt to digital transformation.

[Source](#)

45%



Organizations will prioritize advanced data security features for data protection at rest and in motion as a critical selection criterion for SSE solutions by 2026, signifying the enhanced demand for robust security mechanisms in an increasingly complex cyber threat landscape.

[Source](#)

Business drivers – Security for hybrid network



Cost takeout

- Customers need cost takeout options through consolidation of network security architecture, Optimization of resource type and volume



Increase in cloud based service consumption

- Increased consumption of PaaS and SaaS platforms require scalability in network and security architectures
- Adoption of cloud native apps need equally faster deployment of network security functions



Emerging business models-mergers and acquisitions

- In cases of mergers and acquisitions, onboarding of new employees in traditional ways is complex and less secure
- Access enablement to enterprise apps for new employees in traditional ways is a tedious task



Zero-trust based app access

- Due to work from anywhere policy, enterprises are adopting zero-trust based app access to all enterprise applications
- Visibility and control of B2B access (third party/ partner access)



Dynamic security and compliance requirements

- Enterprises need to keep the sensitive data in public cloud secure and prevent data loss/ theft to avoid hefty penalties in case of security breach



Visibility and optimization

- Provide broad traffic visibility and control
- Expose shadow IT and protect sensitive data

Challenges in traditional security



An architecture never designed for hybrid work

- Poor user experience and lower productivity
- Large sets of individual solutions and vendors
- Complexity of operations and costs
- Gaps in security posture born out of complexity and fragmentation



Diverse IT landscapes make secure connectivity hard

- Organizations aren't adequately prepared to handle cybersecurity threats
- Organizations report that high number of security tools is driving complexity
- IT leaders report that users bypass their current VPN sln



Lack of scalability

- Traditional appliance based architecture couldn't scale up with the increase of users
- Heavy investment needed to change architecture/ add user



Businesses unequipped to protect themselves from Gen5 attacks

- Mega attacks or 5th generation attacks are multi-vector in nature, can infiltrate swiftly and stealthily proliferate across enterprise network and infra (e.g. WannaCry attack, NotPetya)



Adoption of software defined perimeter

- Adoption of SD-WAN increased to improve QoS with increased site capacity, but deployment of perimeter security (FW, VPN, Proxy) at every branch location didn't provide true SDP



Complexities of having multiple point solutions

- Too many point solutions lead to increased CAPEX cost as well as operational costs
- Lack of interoperability between disparate network and security solutions makes data correlation difficult which lead to non-unified network security strategy



Chances of regulatory compliance violations

- Lack of visibility and controls across the below can lead to regulatory compliance violations:
 - Sensitive data flow across organization
 - App access of users/ employees
 - Network usage and device access



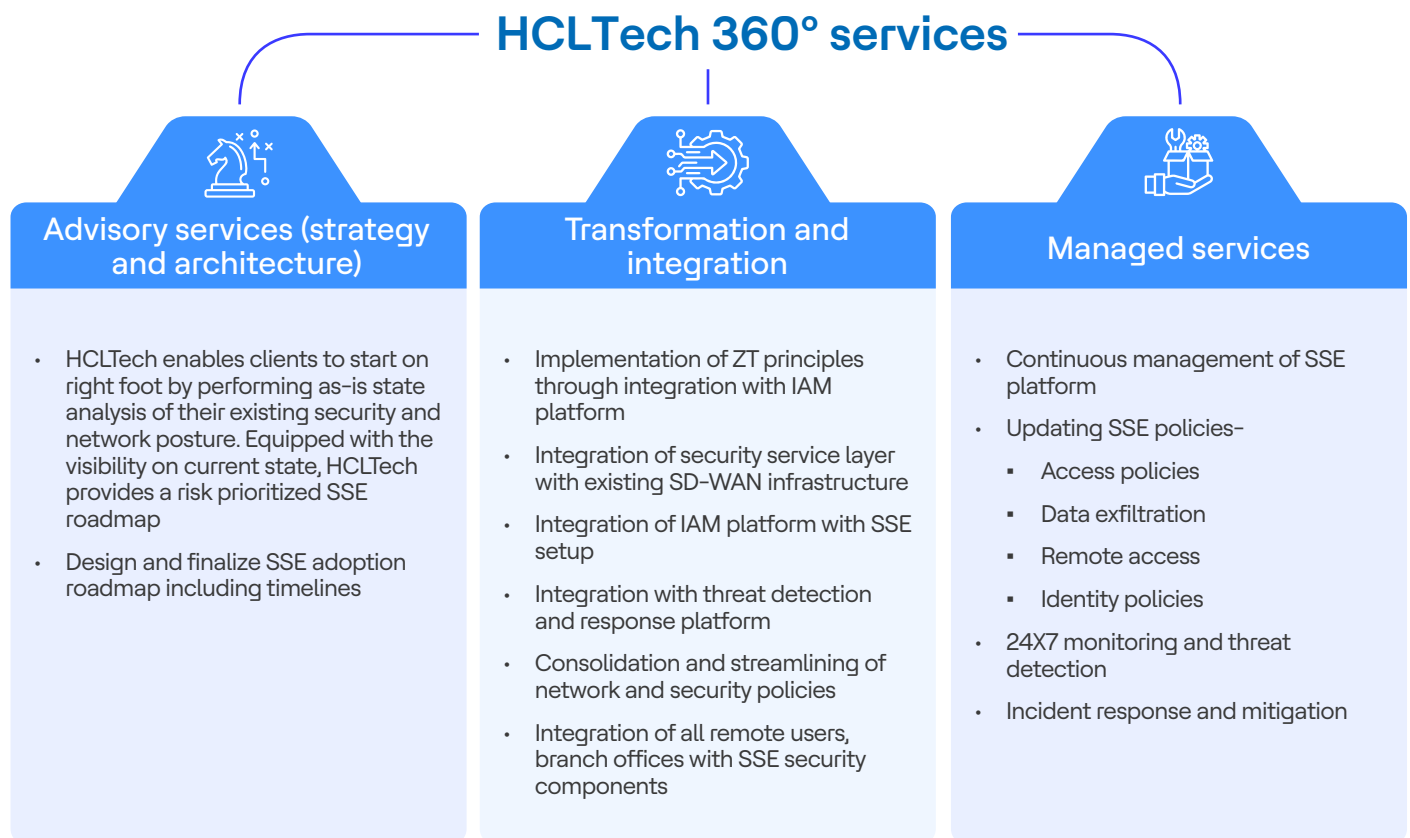
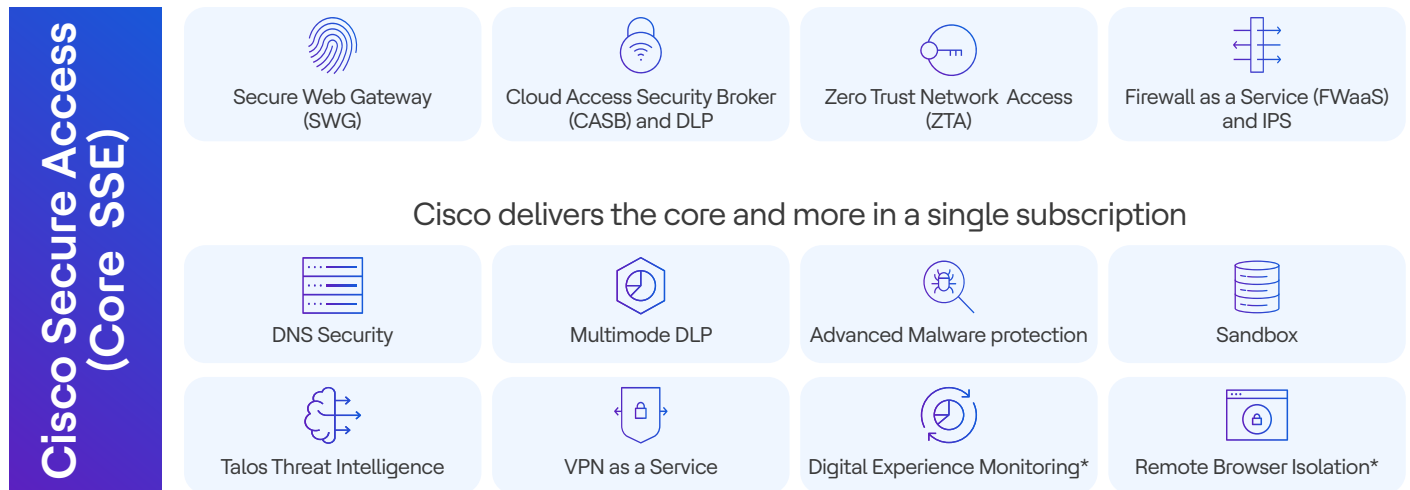
Inconsistency in policy push to edge

- Security policies pushed to edge are sometimes inconsistent with overall enterprise policies

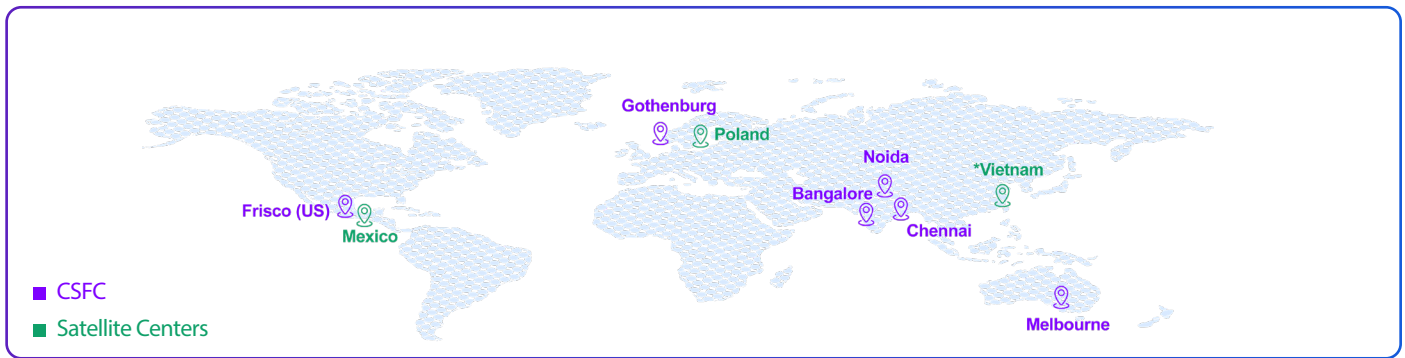
HCLTech services

Powered by cisco secure access (SSE solution)

Go beyond core Secure Service Edge (SSE) with the combined strength of Cisco and HCLTech. Cisco's advanced secure access technology, paired with HCLTech's 360 services, ensures enhanced connectivity and protection for your business



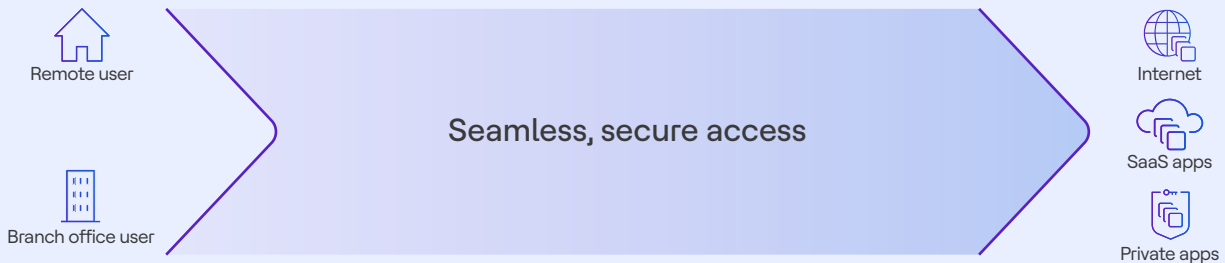
HCLTech CSFC delivery locations



Use cases

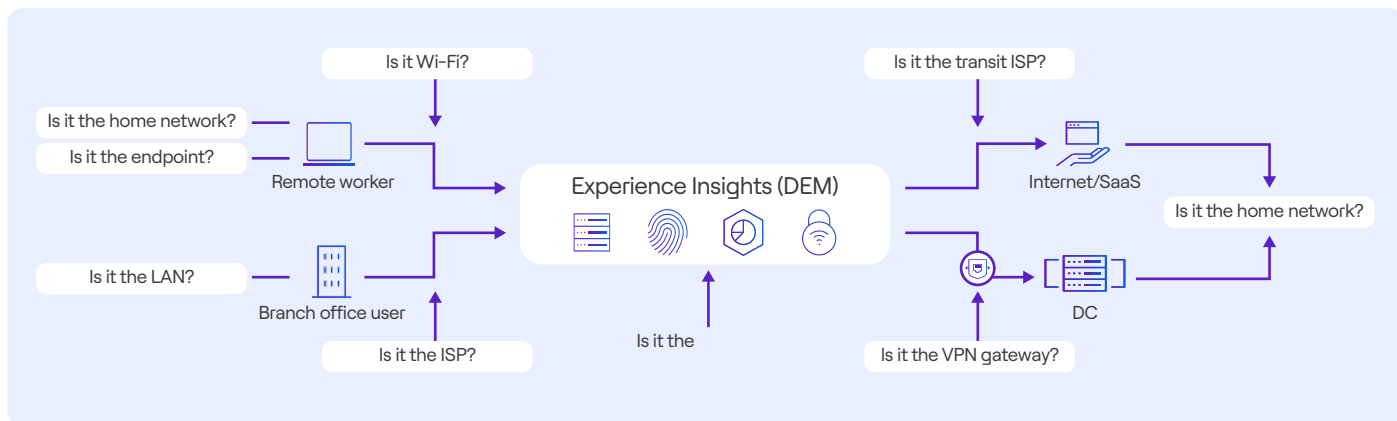
Enabling secure remote work

- Challenge** A company transitioning to a hybrid work model requires secure, remote access to internal and cloud resources for its employees.
- MSP Solution** Implement Cisco secure access to provide seamless and secure access through ZTNA and VPNaaS, enabling employees to securely connect to necessary applications and data from any location.
- Outcome** Enhanced productivity for remote and hybrid workers due to simplified and secure access to resources. The MSP helps the company reduce its attack surface and improve business resilience by implementing zero-trust security measures and multi-factor authentication.



Enhancing digital experiences with experience insights (DEM)

- Challenge** In a digital-first world, businesses face challenges in maintaining optimal performance across digital platforms and cloud applications, directly impacting user satisfaction and productivity.
- MSP Solution** By integrating Cisco secure access with ThousandEyes, MSPs offer a digital experience monitoring solution. This tiered service ranges from basic network monitoring to advanced, end-to-end visibility and predictive analytics. It includes setup, real-time performance alerts and actionable insights for continuous optimization.
- Outcome** Customers benefit from enhanced application performance and user experience, leading to improved productivity and employee satisfaction. Proactive issue resolution and informed IT decisions ensure a seamless digital experience, aligning IT performance with business goals.



Other use cases

- Secure web gateway
- Protect against ransomware and other sophisticated threats
- Quickly investigate and respond to incidents
- Detect and mitigate threats
- Protect sensitive information
- Protect branch offices with direct internet access
- Block risky apps while still ensuring user productivity
- Protect guest Wi-Fi access

HCLTech Solution

HCLTech's managed SSE solution is designed to elevate cybersecurity by fully harnessing the power of Cisco's advanced Secure Access technologies. This comprehensive offering integrates critical components such as Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and Firewall as a Service (FWaaS), creating a robust security framework tailored for the complexities of modern enterprises.

This solution employs Zero Trust Network Access (ZTNA) principles, ensuring that all access is authenticated and authorized, thereby minimizing potential vulnerabilities in the network. It also incorporates digital experience monitoring and remote browser isolation, enhancing the user experience while safeguarding against emerging threats.

At the heart of HCLTech's offering is a focus on streamlining integration and operational efficiency. A thorough as-is state analysis of the client's existing security posture informs the development of a risk-prioritized SSE roadmap, guiding organizations through the necessary transformations. This includes integrating security service layers with existing SD-WAN infrastructure and aligning identity management systems with security protocols.

HCLTech not only provides ongoing management of the SSE platform but also ensures continuous updating of essential security policies, including access, data exfiltration and identity policies. The solution supports 24/7 monitoring and incident response capabilities to swiftly address any potential threats.

By refining network security architectures and optimizing configurations, HCLTech's managed SSE solution enables enterprises to enhance their security posture effectively. This solution is backed by HCLTech's 360 Services, ensuring comprehensive support throughout the entire integration and operational process—aligning with business objectives while driving secure digital transformation efforts.

Why HCLTech?



The recognition as a "Cisco Gold Provider Worldwide" affirms our strong credibility in delivering comprehensive Security Service Edge (SSE) solutions utilizing Cisco's secure access technologies.



HCLTech has maintained a strategic, 360-degree partnership with Cisco for over 27 years, allowing us to leverage their cutting-edge technology for enhanced security and connectivity.



Our win of the "Americas Transformation Partner of the Year 2024" award from Cisco highlights our commitment to providing transformative security solutions designed to meet the evolving needs of businesses.



HCLTech also received the "Cisco CX Hero Award" for the exceptional implementation of Cisco WiFi technology, integrating advanced AI capabilities that boost our SSE services and enhance user experiences.



30+ years of network transformation experience

HCLTech possesses extensive expertise in designing, building, and delivering SSE solutions to global enterprises across various verticals and spanning over 60 countries.



Leadership across network assessments

Our recognized leadership in network assessments positions us as a trusted provider, as evidenced by our recognition from leading analyst firms like Gartner, ISG, Forrester and Everest group, affirming our strengths in weaving security into network frameworks effectively.

For more information visit our [page](#)

**Here's your partner of choice.
HCLTech means people and business.**

HCLTech | Supercharging
Progress™

hcltech.com