

Lightweight Secure Service Edge (LWSSE)



Overview

Securing today's dynamic digital enterprise landscape has become increasingly challenging, particularly with the widespread adoption of cloud technologies and the browser emerging as the primary gateway to SaaS applications. This whitepaper underscores the necessity for a new security paradigm, addressing the inherent limitations of traditional perimeter-based models in a browser-centric enterprise environment. It examines how HCLTech's Lightweight Secure Service Edge (LWSSE) solution, powered by Palo Alto Networks Prisma Browser, revolutionizes secure SaaS access. Our approach delivers simple, scalable, seamless and context-aware protection, all while maintaining excellent end-user experience and operational agility.

Outdated security models in a borderless enterprise world

Enterprises across industries and geographies rapidly adopt cloud technologies to accelerate time-to-market, drive innovation and enable scalable growth. The post-COVID shift further expedited this transformation, where remote and hybrid work models have become the standard. As users and applications increasingly operate beyond traditional corporate boundaries, legacy security models, designed around centralized enterprise infrastructure, are proving insufficient. In today's enterprise environment, the browser has become the primary workspace for employees, enabling access to critical applications and supporting routine workflows. Yet, it remains one of the least defended vectors in the security stack, exposing significant vulnerabilities in outdated enterprise security frameworks. Key limitations of the legacy enterprise landscape include:

Overwhelming security requirements:

Complex security platform deployments burden SMBs, delaying adoption due to challenges with agent deployment, security device installation, integration and configuration.

High costs and complexity:

Significant investments in infrastructure, licensing and expertise reduce overall ROI and operational efficiency.

Delayed time-to-value:

Lengthy deployment cycles hinder real-time protection and responsiveness.

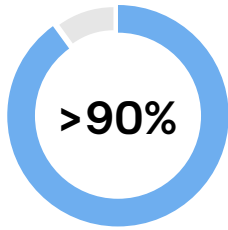
Unmanaged device risks:

Limited visibility and control over Bring Your Own Device (BYOD) and contractor environments create potential vulnerabilities.

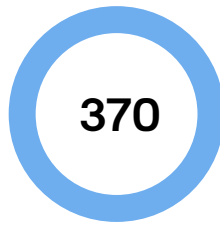
Visibility gaps:

Blind spots in SaaS applications and Shadow IT increase the risk of Data Loss Prevention (DLP) breaches and compliance violations.

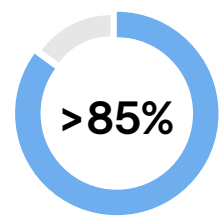




IT leaders rely on SaaS applications for daily operations



Average number of SaaS web apps in use, including Shadow IT



Work related tasks now taking place in a web browser, the primary hub of productivity

LWSSE: Redefining secure access in a browser-first world

HCLTech's Lightweight SSE (LWSSE), powered by Palo Alto Networks' Prisma Browser, is a cloud-delivered security platform designed for the modern, distributed workforce. It provides enterprise-grade protection directly at the browser level, offering agility, scalability and zero infrastructure overhead—ideally suited for today's cloud-first environments. LWSSE redefines secure access by addressing the needs of a browser-centric, decentralized enterprise, aligning security with the realities of a modern, digital workplace. Some of the key features of our solution are as follows:

Lightweight by design:

Our browser-based, cloud native architecture eliminates the need for endpoint agents or complex infrastructure. Our innovative solution enables rapid deployment, seamless scalability and operational agility across diverse environments. It especially benefits third-party users and contractors working from unmanaged devices, providing robust security without compromising convenience or performance.

Zero trust anywhere:

Adopts and extends Zero Trust principles by enforcing least privilege access across managed devices, unmanaged endpoints, BYOD and third-party users, including partners. This ensures secure, context-aware access regardless of device or location, while mitigating risks associated with shadow IT and unmanaged devices.

Unified visibility and control:

A centralized, integrated platform delivering granular access enforcement and real-time visibility into user behavior at the web session layer, application usage and data movement. This empowers IT and security teams with actionable insights to maintain governance, detect anomalies and prevent data loss effectively.

Built-in compliance:

The platform has over 1,000 pre-defined data classifiers, regulatory compliance profiles and advanced Data Loss Prevention (DLP) controls. This enables organizations to automatically detect and classify sensitive data, enforce compliance policies, prevent unauthorized data movement and easily streamline audit readiness.

AI-powered protection:

The LWSSE solution, integrated with Prisma Browser and Cloud Delivered Security Services (CDSS), provides AI-driven threat prevention. Leveraging advanced machine learning and behavioral analytics ensures real-time phishing defense, intelligent malware detection and prevention, context-aware threat analysis and access to integrated threat intelligence.

End-to-end delivery excellence:

From initial assessment and onboarding to policy design and ongoing managed operations, HCLTech ensures a consistent, high-quality delivery experience, accelerating time to value and simplifying ongoing security management.

Strategy, Advisory and Consulting	Transformation and Integration	Managed Services
<ul style="list-style-type: none"> • Strategic alignment with enterprise security goals and regulations • Identify high-priority use-cases to maximize ROI and ensure a strong start • Architect scalable and secure access models • Implement a unified policy framework across all users • Enterprise change management • Design Zero Trust architecture to enhance security 	<ul style="list-style-type: none"> • Implement Lightweight SSE strategy using appropriate controls • Apply Zero Trust principles through integration with CIE or corporate directory • Integrate the IAM platform with Strata Manager • Integrate with threat detection and response platform • Streamline policies across users and groups 	<ul style="list-style-type: none"> • Continuous platform management • Update SSE policies: <ul style="list-style-type: none"> - Access policies - Data exfiltration - Remote access - Identity policies • 24/7 monitoring and threat detection • Incident response and mitigation

Why LWSSE might be a smart choice for your enterprise



Faster deployment enabled by cloud-delivered security, eliminating the need for on-prem infrastructure. This approach ensures quick scalability and seamless onboarding for users across diverse locations.



Agentless security delivering enterprise-grade protection, powered by Prisma Browser, CDSS and precision AI for advanced and intelligent threat prevention.



Browser-centric workflows streamline secure access by utilizing native browser capabilities, minimizing reliance on traditional VPNs or endpoint software.



Provides **excellent user experience** with a chromium-based browser, offering fast Zero Trust access. Its intuitive, zero-learning-curve design ensures a frictionless experience, enhancing user productivity.



Cost-effective solution that leverages browser-native capabilities to deliver secure access, eliminating the need for complex security stacks and reducing operational burdens.



HCLTech cybersecurity COEs, powered by global delivery expertise, industry-leading accelerators and frameworks, deliver intelligent, scalable and resilient security outcomes.



Integrated service ecosystem that ensures seamless, scalable delivery of cybersecurity solutions across regions, backed by 24x7 support and compliance assurance.

About the HCLTech and Palo Alto Networks partnership

HCLTech and Palo Alto Networks partners to deliver advanced cybersecurity solutions, integrating world-class technology with deep industry expertise. Together, we ensure seamless transitions from legacy systems to cloud native platforms, enabling scalable, secure and resilient digital environments. This strategic collaboration empowers organizations to adopt zero trust, enhance cyber resilience and accelerate secure digital transformation through comprehensive consulting, transformation and managed services.

To learn more about the HCLTech and Palo Alto Networks partnership, visit our partnership page:
<https://www.hcltech.com/palo-alto-networks>

For more information, please write to us at cybersecurity-grc@hcltech.com



HCLTech | Supercharging
Progress™

hcltech.com