Skyhigh Security

Skyhigh Security Hybrid Mesh Secure Service Edge (SSE)

Delivering data-first zero trust where work happens, protecting users, apps, agents, and data across cloud, on-premises, and private environments

BUSINESS VALUE

Local Security Costs Less: Security delivered through local gateways where users and AI access local resources costs less. With Skyhigh's unique location-aware licensing, customers only pay for cloud services their users need. Organizations with a meaningful number of in-office users can **save up to 50% of their web security and SSE OPEX**, by cutting license waste.

Zero Trust delivered Organization-Wide: Retire legacy VPNs and close the gap between "remote access zero trust" and zero trust for in-office/internal application reality. Reduced WAN utilization, better user experience and deliver data-aware microsegmentation and Zero Trust enforcement for local users and local applications.

Unlock the potential of AI: Unify data security, AI security, and zero trust under one platform. Enforce AI governance and reduce accidental and agent-driven data exposure.

Resilient by Design, Sovereign by Choice: Improve resilience and user experience by keeping local traffic local when policy, latency, or sovereignty requires it. Give auditors and regulators clearer proof of where controls are enforced and where data is processed.

Work is hybrid. Your security should be too.

Work now happens in more places than the security stack was designed for. Return to office mandates mean 74% of remote-capable employees are in the office at least some of the time[1], and more than 50% of multinationals globally are actively implementing a digital sovereignty strategy[2]. At the same time organizations are building custom AI applications, deploying private models on their own infrastructure, and repatriating workloads into local data centers for sovereignty and performance.

AI has turned this into a data problem. 1 in 6 prompts entered into AI tools contain proprietary data[3], so the interactions that matter most are increasingly the ones generated inside your own buildings.

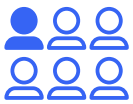
Securing this distributed architecture with traditional tools creates friction. Routing local office traffic and local AI workflows out to distant cloud Points of Presence (PoPs) with Cloud-only SSE technologies introduces latency, consumes WAN bandwidth, and incurs unnecessary cloud inspection costs. Conversely, maintaining separate on-premises SWG appliances alongside a cloud SSE stack forces teams to manage two consoles and two policy engines, causing configuration drift and coverage gaps.



74%
of remote-capable employees are in the office at least some of the time[1]



more than
50%
of multinationals globally are actively implementing a digital sovereignty strategy[2]



1 in 6
prompts entered into AI tools contain proprietary data[3]

Skyhigh Hybrid Mesh SSE closes these gaps. It decouples SSE policy inspection and enforcement from the deployment architecture and unifies the on-premises gateway and cloud security service edge under a single console and a single policy engine. Through a Policy-as-Code engine, you author policy once and enforce it anywhere, on premises with Secure Service Gateways (SSGs) or through global cloud PoPs based on user locality. With our location-aware licensing model, you only pay cloud-delivered SSE inspection rates when users actually need them, reducing web security and SSE OPEX by up to 50%.

1 Source: Gallup Hybrid Work Indicator, May 2026.
2 Source: Gartner, Forecast Analysis: Sovereign Cloud IaaS, Worldwide, 2025.
3 Source: Gartner, Cybersecurity Threat: AI Application Compromise, 2026.

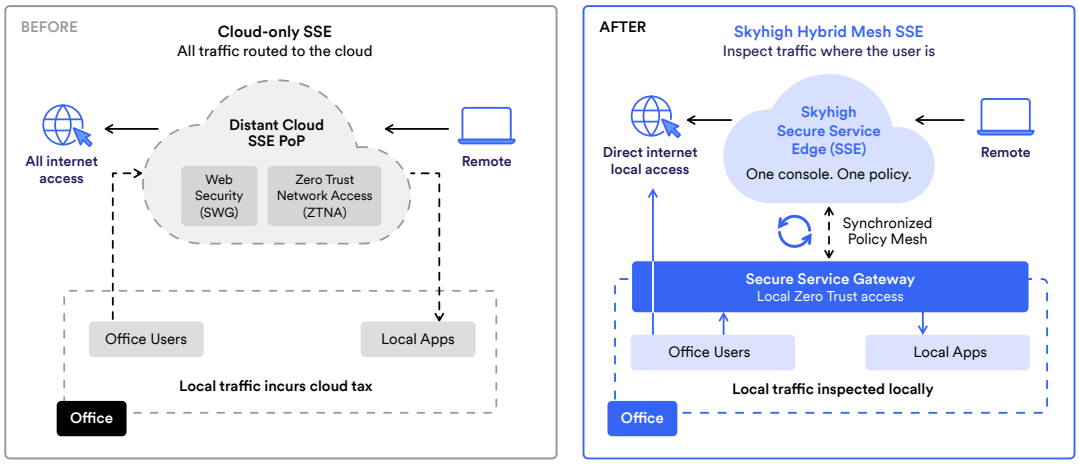


Figure 1. With Hybrid Mesh SSE, local traffic and data stays local, Zero Trust Access is enforced locally and customers only pay for the cloud services they need.

Cloud-only SSE architectures require every packet to be sent to a cloud point of presence, including traffic from an in-office user reaching a server or AI instance in the same building. That adds latency, consumes WAN bandwidth, and incurs cloud inspection costs for traffic that never needed to leave the site. Cloud-based Zero Trust Network Access (ZTNA) fails to protect local East/West traffic, and adds architectural friction for local users accessing these local resources.

For organizations that are protecting their hybrid working environment with on-premises gateways running alongside a separate cloud SSE subscription have to pay twice to protect their workers. The solution requires two consoles, two policy engines, rules are authored twice and reconciled by hand, so policy can often drift.

Security posture can vary depending on where the user connects rather than who they are. This dual stack approach incurs operation friction and cost.

Many high assurance organizations operating on-Premises Secure Web Gateways (SWG) are running on end of life hardware and software is essentially running in ‘maintenance mode’ as vendors favour a cloud-first R&D strategy. These appliances are struggling with performance and capacity, and not keeping up with the latest innovations seen in cloud SSE solutions. If organizations want to take advantage of newer capabilities like Zero Trust, they are forced to move to the cloud before they are ready and this impacts their risk to data sovereignty and resilience.

KEY ADVANTAGES

Adaptable Architecture for Fair, Flexible Economics
The right architecture protects better and spends smarter. Keep cloud where cloud makes sense, local where local is required, and use adaptive access plus Policy-as-Code flexibility to match controls and consumption to actual need, and pay fairly for it.

Zero Trust Where Work Happens:
The zero trust promise has to reach inside the organization and protect East/West traffic with microsegmentation, not stop at the cloud edge. In-office users, contractors, internal apps, and AI agents need controls close to the work.

Data-centric AI security:
AI changes who or what can access data and how fast it can move. The most defensible AI security story starts with discovering, classifying, controlling, and protecting sensitive data.

Local Control and Resilience:
Sovereignty is broader than geography. High-assurance organizations need control over where data is decrypted, inspected, governed, logged, and protected.

Skyhigh Hybrid Mesh SSE

Unified zero trust security across cloud and on-premises environments, under one policy engine

Skyhigh Security Hybrid Mesh SSE provides a unified security architecture that connects cloud and on-premises deployments across the data center, branch offices, and head office. Hybrid Mesh SSE decouples policy management from policy enforcement location, and a single policy-as-code engine governs local physical or virtual gateways and global cloud points of presence, with no manual reconciliation needed.

It centralizes policy management, analytics, reporting, and threat intelligence while delivering consistent SWG, ZTNA, threat protection, Data Loss Prevention (DLP), and Remote Browser Isolation (RBI) capabilities through a single platform.

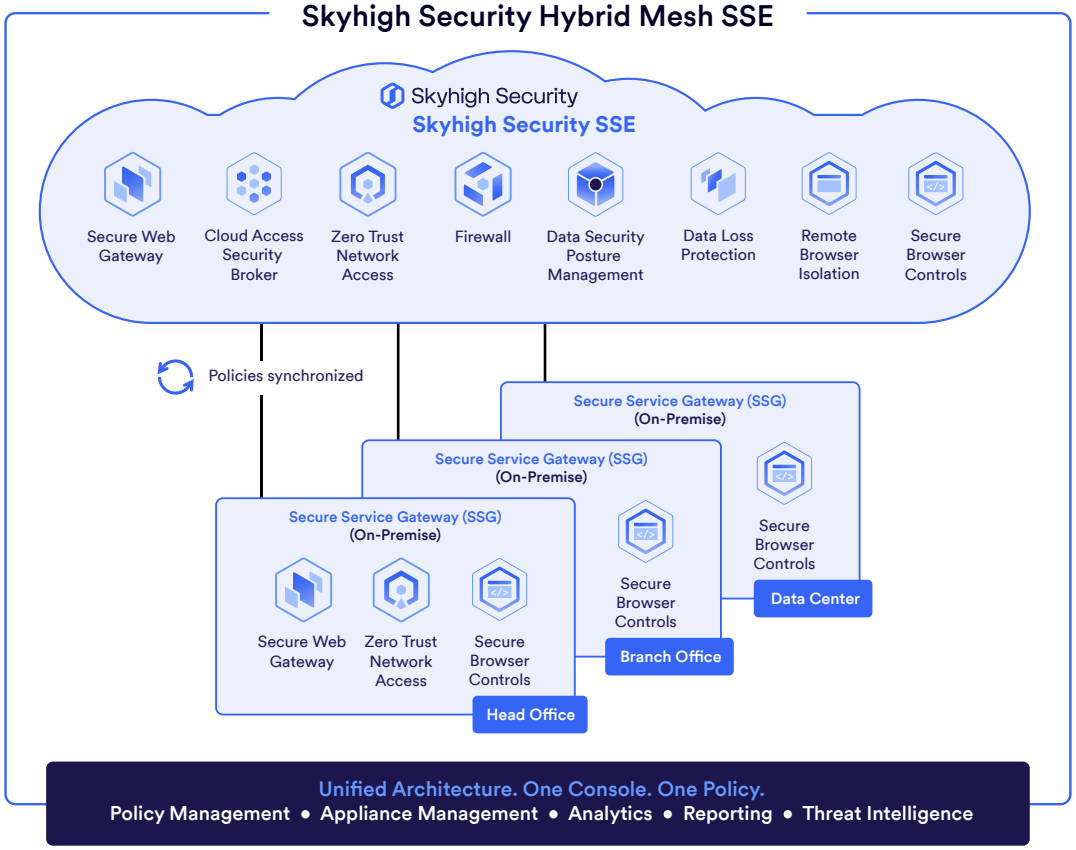


Figure 2. One policy framework across cloud points of presence and on-premises Secure Service Gateways.

One policy, managed centrally and applied everywhere.

With a single Cloud-based Policy-as Code Management plane, a single policy is synchronised across policy enforcement points in the hybrid environment; Skyhigh Cloud SSE Points of Presence (PoPs) for remote users and Cloud-delivered services and Secure Service Gateways (SSG) for locations with in-office workers and local applications and infrastructure.

Secure Service Gateways are managed compute nodes inside the same policy framework as the cloud nodes. The policy is authored once and governs every enforcement point simultaneously. There is no separate on-premises policy engine to maintain, and no second rule set to reconcile.

Log and telemetry data can reside on a local virtual machine, in your own AWS or Azure tenancy, or stream to a SIEM, so you control where your data lives.

Native local enforcement.

Secure Web Gateway, Zero Trust Access, and Secure Browser Controls run natively on the Secure Service Gateway (SSG) appliance. Local traffic inspection, policy enforcement and activity logging stay inside your perimeter. With local inspection and enforcement for in-office users, less traffic is forwarded to the cloud. Zero Trust can be enforced locally without hairpinning all access traffic and associated data to the cloud and back. In the unlikely event the cloud SSE instance is unavailable, local networks remain online and local users can access the Internet and local applications without service interruption.

Location-aware economics Saves up to 50% of web security & SSE OPEX.

With Skyhigh's unique Location-aware licensing, Customers only pay cloud processing costs when users need it. Inspecting local traffic on local appliances reduces cloud processing consumption, so the bill reflects where enforcement actually happens. 3rd party Cloud-Only SSE customers can save as much as 50% of their web security & SSE OPEX with Hybrid Mesh SSE.

Access to cloud-delivered advanced services.

Customers can seamlessly add advanced security services through their single Policy-as-Code framework to extend the protection of users, devices agents and data wherever work happens. Advanced Data Loss Prevention, AI security, Remote Browser Isolation, CASB and DSPM are available through Skyhigh's cloud SSE, under the same policy, with customer-controlled forwarding scope.

Integrated reporting and dashboards.

A single reporting console that unifies reporting across cloud and locally enforced security services as well as on-premises physical and virtual appliance management.

Modules

One platform, one policy engine, modules activated per location.

Module	Capability
Secure Web Gateway (SWG)	Enforced natively on the Secure Service Gateway appliance and in the cloud. Real-time URL and content-category filtering, ML cloud sandbox and anti-malware, MITRE ATT&CK mapping, full SSL and TLS inspection, phishing and credential-theft protection, global threat intelligence, SD-WAN via IPSec and GRE, and UEBA adaptive policy.
Zero Trust Network Access (ZTNA)	Enforced natively on the appliance and in the cloud. Identity-aware, least-privilege access to private applications, with per-session identity and device check, application micro-segmentation, east-west and in-office enforcement, posture-based access, and VPN replacement for remote users.
Application visibility and risk	Enforced natively on the appliance as part of web security. Discovery and risk scoring of sanctioned and unsanctioned application usage, with no cloud forwarding required.
Secure Browser Controls	Enforced natively on the appliance and in the cloud. In-session governance for managed and unmanaged endpoints, controlling clipboard actions, file uploads and downloads, printing, and applying digital watermarking to screenshots of sensitive browser content. Provides a compensating control where session content is not visible to the proxy.
Advanced Data Loss Prevention (DLP)	Applied through the Skyhigh cloud. A single DLP engine across web, cloud, and private access, with Exact Data Matching, Indexed Document Matching, OCR, and pre-built regulatory templates. On-premises users behind the appliance receive web DLP coverage through the Next-Hop Proxy.
Remote Browser Isolation (RBI)	Applied through the Skyhigh cloud. Containerized isolation for risky, newly registered, or uncategorized web sessions, with read-only rendering and category-driven auto-isolation.
AI Security	Applied through the Skyhigh cloud. Discovery of generative AI usage and risk scoring across 1,700+ AI applications, with access policy by user and service, and controls on sensitive data submission to external models.
Cloud Access Security Broker (CASB)	Applied through the Skyhigh cloud. Discovery and governance of sanctioned and unsanctioned SaaS, threat protection with data-centric visibility and control over your cloud apps, without compromising on security.
Data Security Posture Management (DSPM)	Available through the Skyhigh cloud. Continuously discover, classify, monitor, and remediate sensitive data — at rest and inline, in real time.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2026.
DS-EN-000067-01