



IGEL + Netskope One

Secure Managed Access for SaaS,
Web, and Private Applications



[READ THE REPORT →](#)

Table of Contents

Executive Summary	3
Integration Highlights	3
The Challenge	4
The Solution.....	4
Secure Endpoint Foundation	5
Cloud-Delivered Security and Access Control	6
High-Performance Global Access	6
Unified Architecture and Access Flow	7
Use Cases	7
Netskope One Enterprise Browser	8
Conclusion	8

Executive Summary

As organizations accelerate their transition to cloud, SaaS, and hybrid work models, the traditional perimeter-based security approach has become increasingly ineffective. Users now access applications from a wide range of locations and devices—many of which are unmanaged or outside of direct IT control. At the same time, data flows across multiple environments, including public cloud, private infrastructure, and web-based platforms. This shift has introduced new challenges around visibility, control, and risk management, particularly at the endpoint where user interaction begins.

The Netskope One platform addresses these challenges by delivering a converged security and networking architecture that provides consistent policy enforcement, real-time visibility, and high-performance access across all applications and environments. IGEL complements this approach by transforming the endpoint into a secure, immutable access layer that eliminates many of the risks traditionally associated with user devices. Together, IGEL and Netskope provide a comprehensive Zero Trust architecture that extends from the endpoint to the network and ultimately to the application and data layers, enabling organizations to securely support modern work without compromising performance or user experience.

Integration Highlights

End-to-End Zero Trust Security.

Netskope enforces **policy, visibility, and data protection** across web, SaaS, and private apps. IGEL ensures every session starts from a **trusted, immutable endpoint state**. Together, they eliminate implicit trust across the entire access chain.

Secure Access for Any Device.

Netskope One Enterprise Browser + SSE enables **secure, controlled access from unmanaged devices**. IGEL provides a **locked-down, no-data, read-only endpoint option** for high-security use cases. Expand access **without expanding risk**, which is critical for modern workforce models.

Reduce complexity with Better Performance.

The combined architecture simplifies while improving user experience. Netskope consolidates security into **one platform, one client, one policy engine**. IGEL eliminates endpoint sprawl and reduces OS-level overhead.

The Challenge

Modern enterprise environments are characterized by a high degree of distribution and variability.

Employees, contractors, and partners frequently access corporate resources from remote locations using a mix of managed and unmanaged devices. Applications are no longer centralized within the data center but instead reside across SaaS platforms, public cloud environments, and private infrastructure. This shift has significantly expanded the attack surface while making it more difficult to enforce consistent security policies.

Organizations are increasingly enabling access from unmanaged or bring-your-own devices to improve productivity and flexibility. However, this introduces substantial risk, as traditional endpoint controls are often absent or ineffective in these scenarios. At the same time, legacy security architectures rely on multiple disconnected tools that create operational complexity and inconsistent enforcement. Network backhauling and proxy-based models further degrade user experience, leading to latency and, in some cases, users bypassing security controls altogether.

The combination of these factors results in a fragmented security posture where organizations struggle to maintain visibility and control over user activity, application access, and data movement. The endpoint remains a critical point of vulnerability, as it is often the least controlled element in the access chain and the broadest attack surface.

The Solution

IGEL and Netskope together deliver a unified solution that addresses these challenges by securing both the endpoint and the access path to applications and data. This combined architecture enables organizations to enforce Zero Trust principles consistently, regardless of user location, device type, or application environment.

The Netskope One platform provides a cloud-native Security Service Edge (SSE) architecture that integrates capabilities such as secure web gateway, cloud access security broker, zero trust network access, and data loss prevention into a single, unified platform.





This approach allows organizations to apply context-aware security policies across all traffic, including web, SaaS, and private application access. The platform's Zero Trust Engine continuously evaluates user behavior, device posture, and data sensitivity to make real-time access decisions, ensuring that security is both adaptive and dynamic rather than static and binary.

Complementing this, IGEL delivers a purpose-built endpoint operating system designed specifically for secure access to centralized resources. Unlike traditional operating systems, IGEL OS is read-only and immutable, preventing unauthorized changes and eliminating the persistence mechanisms that malware and other threats rely on. By removing local data storage and restricting execution to trusted applications, IGEL significantly reduces the endpoint attack surface and ensures that each device operates in a known, controlled state.

Together, these capabilities create a seamless and secure access model in which the endpoint is inherently trusted, and all access to applications and data is governed by centralized, policy-driven controls.

Secure Endpoint Foundation

The IGEL Secure Endpoint OS Platform™ serves as the foundation for secure access by transforming user devices into controlled access points rather than general-purpose computing environments. Its immutable design ensures that the operating system cannot be altered by users or malicious actors, effectively eliminating configuration drift and reducing the risk of compromise. The absence of local data storage further enhances security by ensuring that sensitive information is never stored on the device, thereby minimizing the impact of potential endpoint breaches.

In addition to its architectural advantages, IGEL OS enforces a strict chain of trust from boot through runtime. Each component of the system is verified before execution, ensuring that only trusted code is allowed to run. This approach not only strengthens security but also simplifies endpoint management, as IT teams no longer need to continuously patch and monitor complex operating system environments. Instead, they can rely on a consistent, hardened endpoint posture across all devices.

Cloud-Delivered Security and Access Control

The Netskope One platform extends this secure foundation by delivering comprehensive security and access control capabilities through a globally distributed cloud infrastructure. Its Security Service Edge architecture enables organizations to inspect and control traffic across all application types without requiring backhauling to centralized data centers.

This results in improved performance and a more seamless user experience.

A key component of this architecture is the Netskope One Enterprise Browser, which provides a secure, managed browser environment for accessing applications and resources. Built on a hardened Chromium foundation, the browser enforces strict controls over user activity, including the ability to restrict actions such as copying, printing, or capturing screenshots. This is particularly valuable in scenarios involving unmanaged or BYOD devices, where traditional endpoint controls are not available.

The platform's data protection capabilities further enhance security by applying consistent policies across multiple channels, including web, SaaS, and cloud environments. By combining real-time inspection with advanced data loss prevention techniques, Netskope enables organizations to prevent unauthorized data movement while maintaining visibility into user activity and application usage.

High-Performance Global Access

Performance is a critical consideration in any modern access architecture, as users expect fast and reliable connectivity regardless of their location. The Netskope NewEdge network addresses this requirement by providing a high-performance, globally distributed infrastructure with presence in more than 80+ regions and 120+ data center regions. Each data center is equipped with full compute capabilities, allowing security services to be delivered directly at the edge without introducing latency.

When combined with the lightweight design of IGEL OS, this architecture ensures that users benefit from both high performance and strong security. By eliminating unnecessary processing overhead at the endpoint and optimizing traffic routing through the network, the solution delivers a consistent and responsive user experience that meets the demands of modern work environments.

Unified Architecture and Access Flow

The combined IGEL and Netskope architecture provides a seamless flow of secure access from the endpoint to applications and data. User devices running IGEL OS serve as secure access points, ensuring that each session originates from a trusted and controlled environment. From there, traffic is routed through the Netskope client or enterprise browser, where it is inspected and governed by the Zero Trust Engine. Policies are applied in real time based on context, and traffic is routed through the NewEdge network to the appropriate application or service.

This unified approach ensures that security is consistently enforced across all access points, while also providing full visibility into user activity and data movement. By integrating endpoint and network security into a single architecture, organizations can reduce complexity and improve their overall security posture.

Use Cases

This solution is particularly well-suited to a range of modern enterprise use cases. In environments with a distributed workforce, it enables secure access for remote employees, contractors, and partners without relying on traditional VPN infrastructure.

For organizations embracing BYOD, it provides a secure and controlled workspace that protects corporate data while allowing users to work from their preferred devices. In cloud-first environments, it ensures consistent policy enforcement across SaaS and web applications, while also supporting access to private applications and legacy systems.



Netskope One Enterprise Browser – SSE-native security built into the browser, centrally managed for IGEL-powered workspaces

Netskope One Enterprise Browser brings enterprise-grade Security Service Edge (SSE) protection directly into the browser – purpose-built for IT teams managing IGEL endpoints and hybrid work environments.

Security is embedded natively into a hardened, Chromium-based browser, giving IT centralized control over every web and SaaS session – no endpoint agents or VPN clients required.

For IT and security teams:

- Single policy engine from the Netskope One console governs workspace configuration, app access, DLP, extension governance, and browser settings
- Zero-trust adaptive access to web, SaaS, and private apps
- Full SSE stack via NewEdge Network: NG-SWG, CASB, DLP, and Threat Protection with extensive global coverage

For end users:

- Isolated corporate workspace with IT-defined app links for instant access
- High-performance global access with no speed-security tradeoff

Conclusion

As organizations continue to evolve toward cloud-first, distributed work models, the need for a unified and scalable approach to secure access has become increasingly critical. Traditional architectures that rely on implicit trust and fragmented controls are no longer sufficient to address the complexities of modern environments.

By combining the secure endpoint capabilities of IGEL with the cloud-delivered security and networking platform of Netskope, organizations can implement a comprehensive Zero Trust architecture that spans the entire access chain. This approach not only reduces risk but also simplifies operations and enhances the user experience, enabling businesses to securely support their workforce wherever and however they work.

IGEL and Netskope together enable secure, high-performance access by ensuring that every session begins from a trusted endpoint and is governed by intelligent, adaptive security controls.