Prisma Access Browser and IGEL

Browse Bravely on Any Device—Built to Support the Ways People Connect, Communicate, and Collaborate in Hybrid Work

Key Benefits

- Enable secure access to applications from any IGEL OS-powered endpoint.
- Quickly onboard and offboard on all IGEL OS-powered endpoints in minutes.
- Improve the end-user experience by delivering a familiar browsing experience with zero learning curve.
- Defend against AI-powered phishing attacks and advanced malware on any IGEL OS-powered endpoint.
- Identify and protect sensitive information with LLM-augmented data classification.
- Streamline deployment and management of secure browsing across all endpoints adhering to regulations.

The Challenge

Enterprises across healthcare, finance, manufacturing, and retail face the challenge of securing access and information in applications across a distributed workforce while maintaining endpoint security, simplifying IT management, and optimizing the user experience. Traditional browsers can expose sensitive data to security risks, and managing access policies across diverse environments can be complex and costly. Organizations need a solution that secures access, work, and the endpoint while delivering delightful user experiences, simplifying operations, and lowering costs. The solution needs to secure the endpoint and access to data and applications, simplify operations, and lower costs, while also improving the user experience.

The Solution

In a browser-first workspace, where 85% of work takes place in the browser,[1] simplifying endpoint management and securing work are made possible through the fast, easy deployment of the secure browser. The secure browser protects against security risks originating from compromised devices, against advanced web threats with AI-powered Advanced URL Filtering and malware protection, and against malicious extensions. Last-mile data controls and built-in enterprise-grade data loss prevention (DLP) capabilities protect sensitive data from accidental and intentional data loss. All of these capabilities are accessible through the IGEL OS app store.

IGEL OS

IGEL is a transformative secure endpoint OS platform designed for software-as-a-service (SaaS), desktop-as-a-service (DaaS), virtual desktop infrastructure (VDI), and secure browser environments. It significantly reduces endpoint total cost of ownership (TCO) and the endpoint attack surface. With the move to a cloud-first strategy, organizations have increasingly moved applications away from the endpoint and into private and public clouds using SaaS, DaaS, VDI, and secure enterprise browsers. This gives organizations an opportunity to rethink the enterprise endpoint. IGEL OS helps organizations:

- Improve endpoint security through a Preventative Security Model™ versus the ineffective monitor, detect, and remediate model.
- Move to Windows 11 in the cloud, utilizing existing endpoints.
- Decrease endpoint TCO by as much as 75%.
- Accelerate endpoint recovery and analysis of a breached device running Windows locally.
- Contribute to IT sustainability goals by reducing e-waste.

1. *The State of Workforce Security: Key Insights for IT and Security Leaders*, Omdia, January 2025.

Palo Alto Networks Prisma Access Browser

Prisma® Access Browser is the industry's first SASE-native secure browser, delivering zero trust access to any user, on any device, from any location—in minutes. It extends SASE protections to the browser, securing business apps and data with leading security technologies from Palo Alto Networks. Features include advanced WildFire® malware prevention that blocks 99% of unknown threats, URL Filtering that stops 347,000 malicious URLs daily, and enterprise-grade DLP with LLM-augmented classification, over 1,000 data identifiers, and built-in compliance profiles.

Palo Alto Networks and IGEL

The integration of IGEL OS and Palo Alto Networks Prisma Access Browser allows organizations to meet the evolving security demands of a workforce increasingly reliant on the browser to perform work. Especially in industries that handle sensitive data, such as healthcare and financial institutions, it's more important than ever to safely enable work on SaaS, web, GenAI, and private applications while defending against data leakage and advanced threats.

Prisma Access Browser enables zero trust access to critical applications and data in only minutes on any endpoint that runs on IGEL OS. Protect sensitive data, gain full visibility into browsing activities, and decrease TCO by up to 79% compared to VDI—all while delivering a familiar user experience with zero learning curve.

Use Case 1: Protecting Sensitive Data in Regulated Industries

Challenge

Organizations in regulated industries (for example, healthcare and finance) must protect sensitive data and comply with strict security requirements.

Solution

With Prisma Access Browser Enterprise Data Loss Prevention, organizations gain the ability to identify and protect personally identifiable information (PII) and protected health information (PHI) with built-in compliance profiles for HIPAA, GDPR, and PCI DSS, and over 1,000 data classifiers, offering unique data protection capabilities for healthcare, finance, and other regulated industries.

Use Case 2: Secure Access for Remote and Hybrid Workforces

Challenge

Enterprises need to provide secure access to SaaS, web, GenAI, and private applications for employees working remotely or in hybrid environments.

Solution

By deploying Prisma Access Browser on IGEL OS endpoints, enterprises can secure access and protect their data in private, SaaS, web, and GenAI applications. Prisma Access Browser protects the browser-based workspace against security risks or threats that originate from the web, compromised devices, and insider risk, while IGEL OS provides a secure, managed endpoint environment.

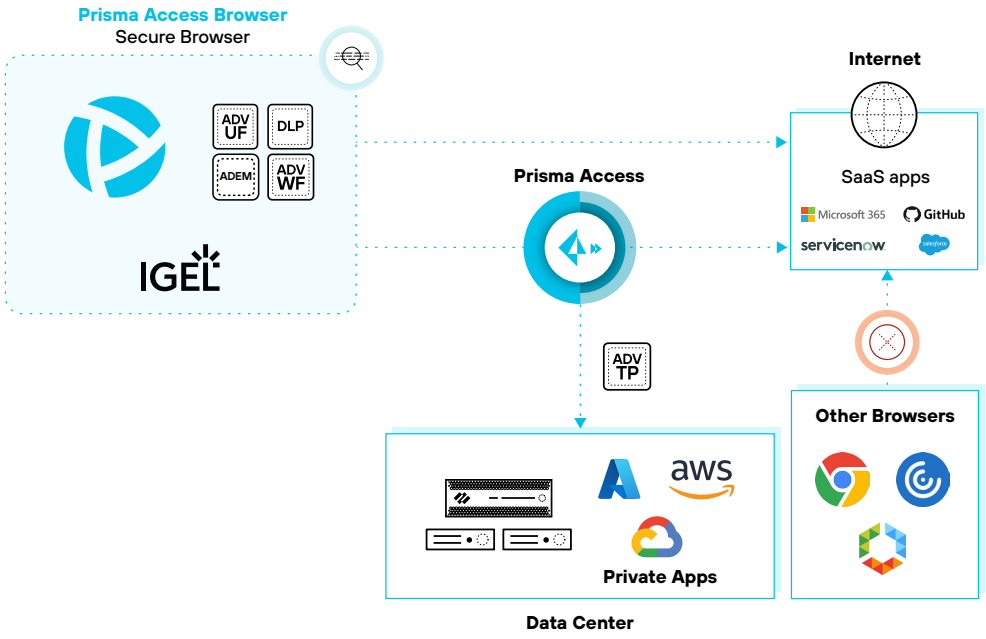

Figure 1. Secure work on IGEL devices with best-of-breed security from Palo Alto Networks

About IGEL

IGEL is a transformative OS platform for now and next. Designed for SaaS, DaaS, VDI, and secure browser environments, IGEL significantly reduces endpoint TCO and your endpoint attack surface. For more information, visit www.igel.com.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_pb_igel_051225