IGEL for U.S. Federal Government

Modern Endpoint Security for the Mission-Critical Edge

Executive Summary

Federal agencies face rising mandates to modernize IT infrastructure while slashing budgets and securing against intensifying cyber threats. IGEL delivers a Zero Trust-ready endpoint platform that simplifies management, eliminates threat vectors by design, and dramatically reduces endpoint total cost of ownership (TCO).

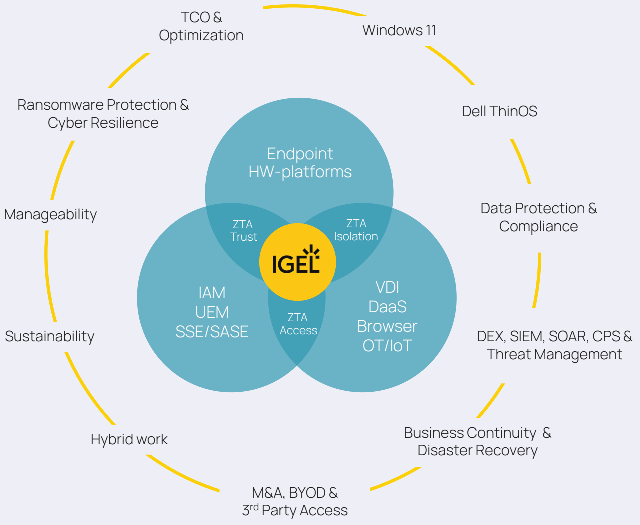
With available Identity and Credential Access Management (ICAM) integrations and an architecture aligned with NIST 800-207, IGEL enables agencies to modernize without compromise—eliminating local attack surfaces while supporting operational continuity, remote access, and resilience.

Like a classified facility with no public entrance, IGEL is secure by design—built from the ground up to keep threats out, data in, and dependable mission execution.

Security by Design: Preventative Security Model

IGEL OS enforces a Preventative Security Model that proactively eliminates the need for reactive endpoint protection layers, and works in concert with an extensive partner ecosystem to deliver an end-to-end Zero Trust solution:

- **Read-Only Operating System:** Cannot be modified by end-users, blocking malware and nation-state attacks.
- **No Local Data Storage:** No breach risk from stolen or lost devices.
- **Trusted Application Platform:** Cryptographically verifies integrity at boot and update.
- **Modular Architecture:** Minimizes attack surface—only required features are deployed.
- **Smartcard + MFA Support:** Full CAC/PIV smartcard authentication with 90Meter middleware.


TCO & Optimization
Windows 11
Dell ThinOS
Data Protection & Compliance
DEX, SIEM, SOAR, CPS & Threat Management
Business Continuity & Disaster Recovery
M&A, BYOD & 3rd Party Access
Hybrid work
Sustainability
Manageability
Ransomware Protection & Cyber Resilience
Endpoint HW-platforms
ZTA Trust
ZTA Isolation
IGEL
IAM UEM SSE/SASE
ZTA Access
VDI DaaS Browser OT/IoT

Enabling Zero Trust

IGEL aligns with Executive Order 14028 and CISA Zero Trust Maturity Models by supporting policy-based access control across key pillars:

- **User:** Native integration with CAC/PIV, Okta, Ping, 90Meterand other ICAM capabilities.
- **Device:** Secure boot, no writable file system, and remote validation.
- **Workloads:** Endpoint cannot install rogue applications—fully admin-controlled.
- **Data:** No user data or credentials reside on device.
- **Network:** IGEL integrates with SASE/SSE solutions (Zscaler, Appgate, Netskope).

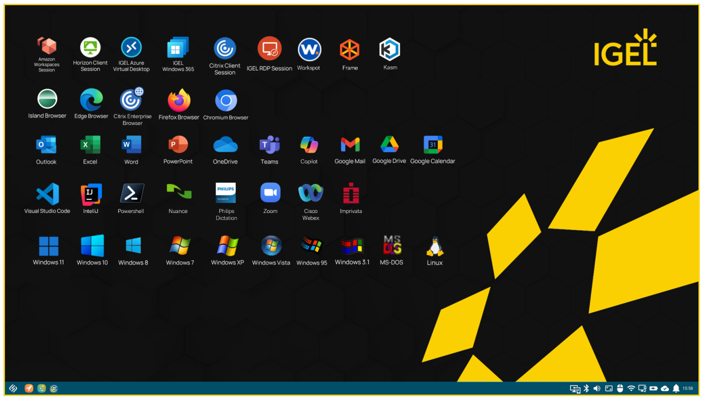
IGEL Adaptive Secure Desktop

IGEL Adaptive Secure Desktop is a curated workspace delivery framework that provides users with only the applications, tools, and access they need—nothing more, nothing exposed. It combines centralized management with context-aware delivery methods to simplify endpoint deployment and enforce Zero Trust policies at scale.

Built on IGEL OS and managed via IGEL UMS, the Adaptive Secure Desktop supports multiple delivery methods including local apps, secure browsers, SaaS, DaaS, and IGEL's Managed Hypervisor. It also can support virtual desktops. This flexibility allows agencies to tailor secure environments to specific user roles, minimizing the attack surface while ensuring high performance.

The Adaptive Secure Desktop model allows agencies to:

- Deliver fit-for-purpose desktops per user role
- Reduce endpoint complexity and permissions
- Support remote work and classified workflows securely
- Curate SaaS, DaaS, local apps, browser experiences and VDI from one console



Built-In Business Continuity

Traditional endpoints—such as Windows-based thick client laptops or desktops—remain vulnerable during cyberattacks, system failures, or software incompatibility events. Once compromised, these devices often require manual reimaging, hardware replacement, or extended downtime—creating unacceptable risk and disruption in federal operations.

IGEL addresses this challenge by embedding continuity directly into the endpoint OS. For scenarios where traditional endpoints must still be used, IGEL can act as a secure rescue layer—instantly restoring access to mission-critical systems without reliance on external infrastructure.

IGEL builds resilience into the OS itself:

- **USB Boot:** Secure boot from IGEL UD Pocket
- **Dual Boot Mode:** Fall back instantly from Windows if compromised
- **Managed Hypervisor:** Run legacy or secure Windows workloads in isolation

Massive Cost Optimization

IGEL reduces endpoint TCO by up to 75%:

- Eliminates Windows thick clients or VDI, and other endpoint security including AV, EDR, DLP agents—removes tooling cost and overhead
- Streamline operations with IGEL UMS central management
- Extend lifespan of existing hardware—supporting older x86 devices

Compliance and Support

- Support for NIST 800-207 and EO 14028
- Priority Plus Support Tier: 24/7 response SLA
- Multi-language Support: U.S. Federal deployment readiness

Why IGEL for Federal Agencies?

- Secure by Design, satisfies Zero Trust activities
- No Local Attack Surface
- Supports ICAM capabilites (Smartcard (CAC/PIV))
- Operational Resilience Embedded in the OS
- Instant Modernization with Existing Hardware
- Significant cost savings

The Secure Endpoint OS Platform for Federal Now & Next.

Contact our experts to explore how IGEL modernizes your endpoint security.