IGEL for U.S. Federal Government

The Secure Endpoint OS Platform for the Mission-Critical Edge

Deploy your Zero Trust IT strategy with confidence, delivering desktops that are secure by design, operationally efficient, and cost-effective at scale.

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 secure endpoint OS platform** that simplifies management, eliminates threat vectors by design, and dramatically reduces endpoint total cost of ownership (TCO).
- At its core, IGEL delivers a hardened, stateless OS environment—one that eliminates entire categories of endpoint risk by design and enables mission access regardless of network conditions or device ownership.

Reduce endpoint TCO by up to 75%

Move to Windows 11 in the cloud with existing hardware.

Reduce endpoint attack surface by up to 95%

Endpoint recovery in minutes with IGEL Business Continuity

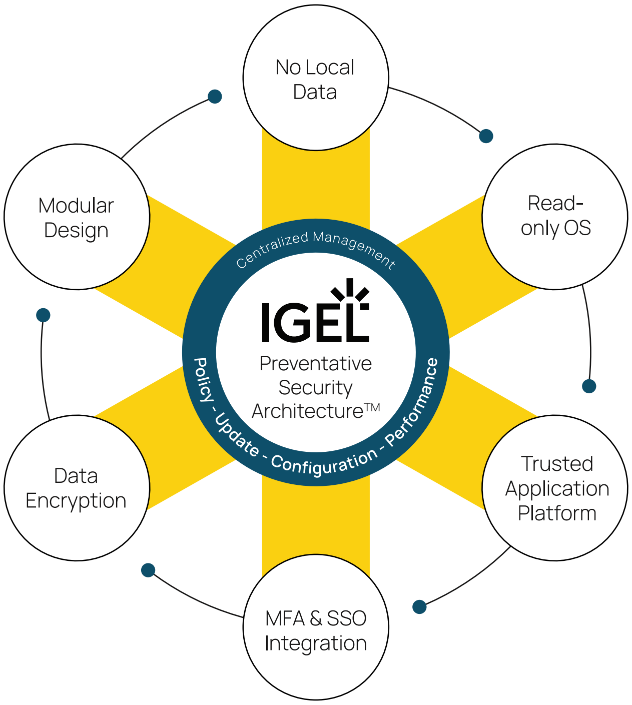
NCAGE Code: 8B8G0
Entity ID: 079742696

igel.com

Why IGEL?

- Secure by design
- Replaces monitor/detect/remediate
- Removes the endpoint vulnerabilities targeted by hackers
- Minimizes the attack surface - only what the user needs
- Removes the need for a complex security stack

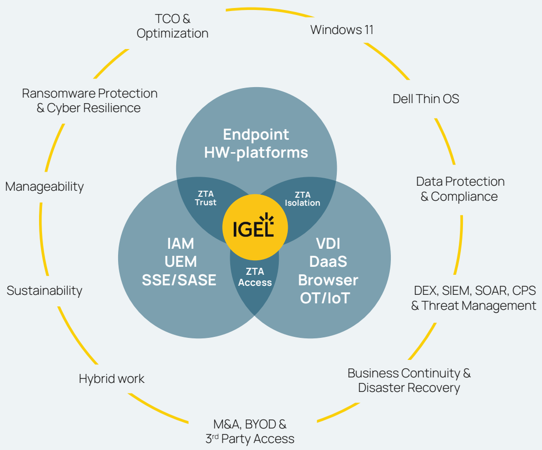
Preventative Security Architecture™


No Local Data
Read-only OS
Trusted Application Platform
MFA & SSO Integration
Data Encryption
Modular Design
Centralized Management
IGEL
Preventative Security Architecture™
Policy - Update - Configuration - Performance

Learn about the IGEL Preventative Security Model™

IGEL Preventative Security Model™

Prevent ransomware and other cyberattacks. Curate an adaptive secure desktop with integrated partners, orchestrated by the IGEL OS platform at the core of the model. Reduce the attack surface and a bulky security stack.


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

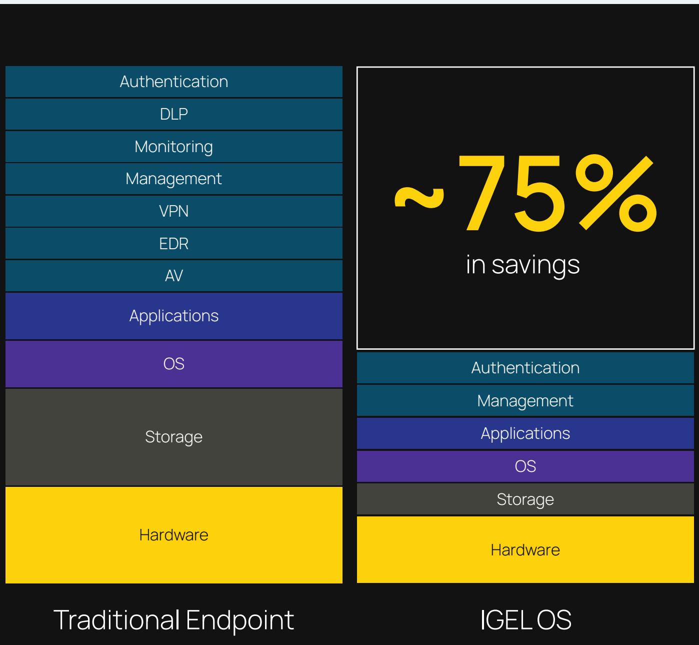
IGEL is a registered trademark of IGEL Technology GmbH. All hardware and software names are registered trademarks of the respective manufacturers. Errors and omissions excepted. Subject to change without notice. © 07/2025

IGEL Ready

Partner Ecosystem
igel.com/ready

LG · hp · 90Meter Smartcard Software · Cisco · omnissa
nerdio · Nutanix · Microsoft · Ping
Microsoft Intune · liquidware · Microsoft Entra ID · Island
Trellix · okta · paloalto networks · citrix
zscaler · Jabra GN · SentryBay · aws
appgate · netskope · poly · zoom

and many more....



Reduce Total Cost of Ownership

Achieve up to 75% savings in your endpoint budget by implementing the Preventative Security Model™.

- Reduce the costs of testing, patching, and managing a large software stack
- Increase endpoint efficiency 22%+
- Extend the lifecycle of hardware from 3-5 years to 6-8 years and more.

Calculate potential savings now at **igel.com/tco-calculator**

Key Differentiators

Device Pillar Compliance by Design:

- IGEL OS verifies cryptographic boot integrity, blocks unauthorized software, and supports CAC/PIV and FIDO2 MFA. Its centralized UMS platform provides full visibility, posture tracking, and device inventory, satisfying core Device Pillar objectives.

Preventative Security Model™:

- IGEL enforces security before detection is needed. No writable OS, no local data, no attack surface to persist threats—enabling compliance without traditional AV/EDR stacks.

Tamper-Resistant, Low-Footprint Architecture:

- IGEL OS is under 2GB, immutable, and requires no persistent storage. Devices can run from USB (UD Pocket), disk, or virtual instance, ideal for disconnected, contested, or tactical use cases.

No Hardware Refresh Needed:

- IGEL enables Zero Trust enforcement on existing x86 hardware, reducing capital costs and accelerating modernization goals like Windows 11 migration, CDM posture improvement, and ZTMM maturity.