

Secure, Resilient Retail Endpoints for a High-Risk, Always-On Sector

Executive Summary

Retailers are increasingly in the crosshairs of cybercriminals, with endpoints serving as frequent entry points in attacks that disrupt operations and compromise customer data. IGEL offers a secure-by-design endpoint platform that hardens every device, reduces attack surfaces, and supports rapid recovery—all while significantly lowering endpoint TCO.

Whether powering in-store POS systems, digital signage, or back-office devices, IGEL protects retailers from escalating threats while enabling agility, sustainability, and operational uptime.

Like a storefront with bulletproof glass and locked-down cash drawers, IGEL ensures everything critical is protected—inside and out.

Secure by Design: Preventative Security Model™

IGEL OS applies a proactive Preventative Security Model, eliminating the vulnerabilities that plague traditional retail endpoints. Combined with an extensive partner ecosystem, IGEL delivers an end-to-end Zero Trust solution that:

- Uses a read-only OS to block ransomware and malware installation
- Stores no local data, reducing the risk of breaches and theft
- Verifies endpoint integrity via a Trusted Application Platform
- Provides a modular footprint, minimizing exposed components

Integrates with leading identity, MFA, and SASE providers

Why IGEL for Retail?

- Hardened endpoints reduce ransomware and breach risk
- Fast recovery keeps stores running and revenue flowing
- Modernize without expensive hardware refreshes
- Deploy digital signage and POS from the same platform
- Slash costs, boost agility

Massive Cost Optimization

- Extend hardware life—run IGEL OS on existing devices
- Replace costly endpoint software stacks
- Reduce support and IT overhead
- Retailers typically see up to **75% TCO savings** across endpoint estate.

Compliance and Support

- PCI DSS-aligned endpoint protection
- Built-in encryption and read-only architecture
- 24/7 enterprise-grade support

Enabling Zero Trust for Modern Retail

IGEL supports Zero Trust frameworks tailored for retail environments—working as the endpoint enforcement layer in a broader partner-integrated ecosystem. From access control and identity verification to secure network connectivity, IGEL simplifies Zero Trust implementation without requiring retailers to rip and replace existing systems.

Deep integrations with industry-leading providers such as Microsoft Entra ID, Okta, Ping Identity, Zscaler, Palo Alto Networks, and Netskope allow IGEL-powered endpoints to participate natively in authentication, policy enforcement, and continuous compliance monitoring.

IGEL supports Zero Trust principles across retail:

- **User:** SSO and contextual access with Entra ID, Okta, Ping
- **Device:** Secure boot, encryption, tamper-proof configuration
- **Applications:** Admin-controlled execution, locked-down browser sessions
- **Data:** No sensitive info stored locally; secure in transit
- **Network:** Tight integrations with Zscaler, Netskope, Palo Alto

IGEL Adaptive Secure Desktop

IGEL Adaptive Secure Desktop is a curated workspace delivery framework that delivers exactly what each retail role requires—no excess, no risk. It enables store associates, warehouse teams, contact center agents, and corporate staff to access their environments with the right apps and security controls tailored to their job function.

This approach replaces one-size-fits-all images and over-permissioned endpoints with a flexible model based on context, role, and delivery method. Built on IGEL OS and orchestrated through IGEL UMS, it supports:

- Local Linux apps for fast in-store workflows
- Progressive web apps for task-based tools
- Hardened enterprise browser sessions for SaaS
- Full virtual desktops for finance or operations roles
- IGEL Managed Hypervisor for legacy POS or kiosk compatibility

The Adaptive Secure Desktop framework enables retailers to:

- Deliver fit-for-purpose desktops per role
- Reduce endpoint complexity, improving security and manageability
- Accelerate onboarding and support retail expansion
- Provide consistent experiences across locations and form factors
- Just-in-time delivery of apps and tools
- Role-based access with minimal endpoint exposure
- Flexible delivery: VDI, SaaS, secure browser, local apps
- Unified endpoint control from HQ via IGEL UMS

Retailers can reduce complexity, strengthen security, and accelerate deployment across stores, warehouses, and contact centers.

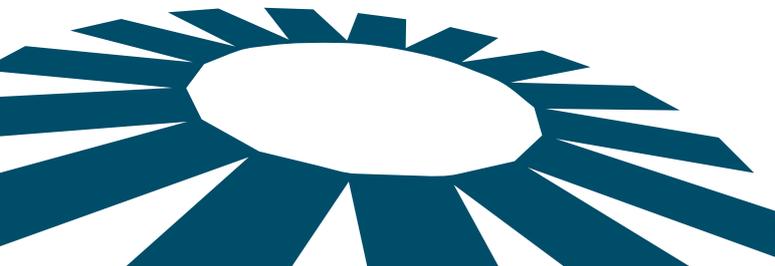
Built-In Business Continuity

Retail operations can't afford downtime—yet POS terminals, signage, and customer service stations often rely on fragile, outdated devices. When attacks or failures occur, reimaging or hardware replacement is slow and costly.

IGEL turns any compatible device into a secure fallback option. With no reliance on local disks or heavy infrastructure, IGEL restores retail operations in minutes:

- USB Boot: Immediate failover with IGEL UD Pocket
- Dual Boot: Fall back to IGEL OS from failed Windows image
- Managed Hypervisor: Securely run legacy retail apps or OSes

Contact us for a demo on www.igel.com/get-started/try-for-free.



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. © 05/2025



Visit us at www.igel.com