



How Enterprises Cut Endpoint IT Costs by 62%

AN ROI STUDY



[READ THE REPORT →](#)

Table of Contents

- Executive Summary 3
- ROI Study Methodology & Approach 4
- Industry Spotlights: ROI Across Sectors 6
 - Industry Spotlight: Healthcare 7
 - Industry Spotlight: Financial Services 9
 - Industry Spotlight: Government..... 11
 - Industry Spotlight: Manufacturing 13
 - Industry Spotlight: Retail 16
- Exploring Savings Categories 18
 - Hardware Savings: Extending the Life of Endpoints 18
 - IT Department Labor Savings: Simplifying Endpoint Management 20
 - Software Savings: Eliminating Redundant Endpoint Costs 22
- Conclusion: Unlocking Endpoint ROI and Building the Future 24

Executive Summary

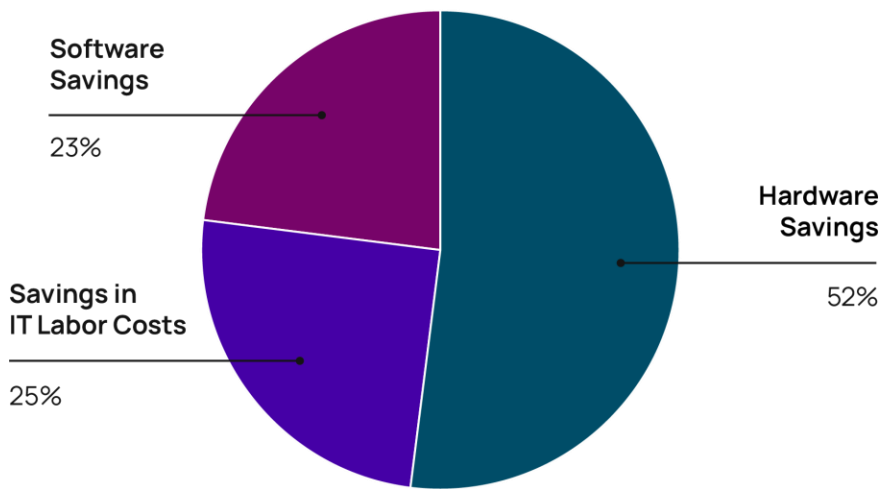
CIOs and CISOs are constantly being asked to do more with less. Budgets are tight, yet the demands on IT continue to grow – deliver stronger security, enable flexible work models, and provide a seamless, high value user and customer experience.

Traditional endpoint strategies make that balance harder to achieve. Frequent hardware refresh cycles, stacked endpoint software agents, and heavy IT labor overheads consume scarce resources without delivering proportional strategic value.

IGEL offers a fundamentally different approach. By transforming the enterprise endpoint to be secure by design, deliver just what the user needs and become the access device for the next generation of Zero Trust hybrid and cloud-delivered applications, IGEL helps organizations cut costs in three tangible, measurable areas:

- **Hardware:** Extending device lifecycles and avoiding premature refreshes.
- **IT labor:** Reducing administrative overhead and support burden.
- **Software:** Eliminating redundant endpoint security and management tools.

The results are clear. Across more than 150 customer TCO analyses in healthcare, financial services, government, manufacturing, and retail, organizations working with IGEL calculated on average:



62%

reduction in endpoint IT expenditure

\$900,000+

in annual savings per organization

These savings arrive at a critical moment. Tens of millions of devices did not make the Windows 11 migration, forcing organizations to either pay for costly extended support or replace hardware that still works.

At the same time, enterprises are shifting rapidly to cloud-first models, moving workloads to SaaS, VDI, and DaaS and implementing Enterprise Browsers, SASE and ZTNA for Zero Trust.

In this environment, IGEL provides a smarter way forward: preserve existing hardware, simplify operations, and unlock budget for the security and innovation initiatives that matter most.

IGEL is not just another endpoint technology. It is a proven platform for unlocking endpoint ROI – helping organizations deliver more security and better experiences with fewer resources.



For too long, the economics of the endpoint have been ignored. Organizations have accepted spiraling costs and complexity as the price of doing business – as if there were no alternative. IGEL proves there is.

We help enterprises dramatically reduce costs while creating a more secure and sustainable endpoint strategy. But the real opportunity goes beyond savings. IGEL is changing the endpoint conversation, turning it into the foundation for the next generation of computing – built on Zero Trust, SASE, and cloud-first architectures. That's the future our customers are investing in."

– Klaus Oestermann, CEO, IGEL

ROI Study Methodology & Approach

The report is based on the ROI analysis produced by a 3rd party tool from Ecosystems.io, an independent Customer Value Management solution that has been tailored for IGEL. This report is built on insights from more than 150 Total Cost of Ownership (TCO) analyses conducted with enterprise organizations across a range of industries including healthcare, financial services, government, manufacturing, and retail. Each analysis drew on real customer environments including existing endpoint estates, IT budgets, refresh cycles, licensing commitments, and support structures.

By aggregating these studies, we provide a comprehensive and credible view of the savings that may be achieved with IGEL across diverse industries and organizational sizes.

The IGEL ROI model is designed to capture both tangible cost reductions and broader business value. It evaluates three primary categories of potential hard cost savings as well as additional categories of soft cost savings. The hard cost savings are:

1. **Hardware Savings:** Avoiding refresh costs and reducing new device spend.
2. **IT Department Labor Savings:** Lowering administrative overhead for deployment, management, and support.
3. **Software Savings:** Eliminating redundant endpoint agents, security tools, and management licenses.

These pillars form the core of the ROI case for CIOs and CISOs, providing the most direct, measurable, and universally applicable financial benefits.

While not featured in this paper, IGEL's TCO tools also provide detailed models for employee productivity, risk mitigation, and sustainability. These categories are often essential for building a complete business case, particularly for organizations with security-first mandates, ESG targets, or hybrid work priorities.

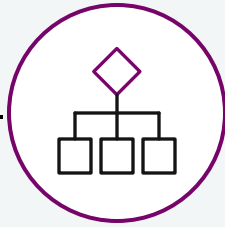
Each TCO analysis followed a structured approach:

- **Baseline Definition:** Existing endpoint costs, including device lifecycle management, licensing fees, IT labor, and software/security overhead.
- **IGEL Model Application:** Projected costs under an IGEL deployment, including extended device lifespan, simplified IT operations, and reduced software stack.
- **Comparative Analysis:** Direct comparison of baseline vs. IGEL model, with savings quantified in dollar terms and percentage reductions.
- **Validation:** Each analysis reviewed with customer stakeholders to confirm assumptions and accuracy.

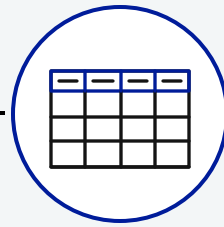
The result is a robust, industry-validated ROI framework that CIOs and CISOs can rely on for budgeting, strategy, and executive decision-making.



Step 1:
Collect Baseline
Data



Step 2:
Apply IGEL
ROI Model



Step 3:
Quantify Savings
by Category



Step 4:
Validate and
Present ROI Findings

Industry Spotlights: ROI Across Sectors

Each industry faces unique challenges in endpoint IT – from compliance and security to scalability and cost pressure. Across every sector analyzed, IGEL consistently delivered substantial and measurable ROI.

Industry	Avg. Annual Savings	Avg. Reduction in Endpoint IT Spend	Hardware Savings	IT Labor Savings	Software Savings
Healthcare	\$800,000	62%	48%	27%	25%
Financial Services	\$3,500,000	62%	70%	13%	16%
Government	\$350,000	63%	48%	12%	40%
Manufacturing	\$1,300,000	65%	66%	19%	15%
Retail	\$500,000	55%	41%	36%	23%
All Industries (Avg.)	\$900,000	62%	52%	25%	23%

Industry Spotlight: Healthcare

Reducing Costs While Driving Improved Outcomes

Healthcare organizations operate arguably the most mission critical IT environments. Virtual desktops have long been utilized due to the benefits of 'follow-me' desktops coupled with badge tap authentication enabling clinicians to focus more time on patient care and less time on the technology. Healthcare has long been a focus for IGEL ensuring no patient information is stored at the endpoint, the broad set of peripherals can be seamlessly utilized and complex workflows are supported.

By the Numbers

From an analysis of more than 50 healthcare organizations:

\$800,000+

Average annual savings per organization

62%

Average reduction in endpoint IT expenditure

Avg. Savings
Distribution:

48%

Hardware savings

27%

IT Labor savings

25%

Software savings

These savings directly translate into more capital available for frontline care investments, cybersecurity initiatives, and digital transformation projects.

Example Use Cases

Shared Clinical Workstations for EMR / EPR Access

IGEL OS BENEFITS:

- **Fast EHR / EPR Access:** Badge access tap on, tap off and tap over – reduces chances of charting under the wrong ID and lost notes should the physician be interrupted during documenting a patient.
- **Speech Mic Support:** Support for leading speech mics and dictation software.
- **Support Multi-Factor E-Prescribing Workflows:** Support for fingerprint and smart card authentication peripherals for positive identification during e-prescribing.

Patient Registration Kiosks

IGEL OS BENEFITS:

Kiosk Mode Support: The endpoint device is locked into an application to ensure patients cannot accidentally disable the endpoint from its required task.

- **Broad Form Factor Support:** IGEL supports a broad range of devices from HP, Lenovo, LG and Dell including laptop and tablet form factors supporting choice in the kiosk form factor.
- **Broad Peripheral Support:** Support for cameras, scanners and signature pads.

Digital Signage

IGEL OS BENEFITS:

Enhanced Security: Strengthen digital signage with the IGEL Preventative Security Model™ to eliminate these devices as a potential ransomware attack vector.

- **Repurpose Devices:** Repurpose Windows devices that cannot move to Windows 11 to reduce TCO and e-waste.
- **Centralized Management:** Manage digital signage devices in the same way as other IGEL OS devices including session shadowing for potential troubleshooting.

Industry Spotlight: Financial Services

Security and Scale at Lower Cost

Financial institutions operate with strict security requirements, complex compliance mandates, and hundreds of thousands of endpoints supporting employees across global offices. Traditional endpoint management and security approaches often lead to excessive costs with financial services demonstrating the highest average hardware savings vs other industries.

IGEL enables financial services organizations to reduce these costs dramatically while strengthening their overall security posture. By extending hardware lifecycles, centralizing management, and minimizing reliance on third-party endpoint agents, IGEL delivers a secure, cloud-ready platform at significantly lower cost.

By the Numbers

From an analysis of 11 financial services organizations:

\$3.5million+

Average annual savings per organization

62%

Average reduction in endpoint IT expenditure

Avg. Savings
Distribution:

70%

Hardware savings

13%

IT Labor savings

16%

Software savings

These savings free up substantial capital that can be redirected into priority initiatives such as Zero Trust security, SASE adoption, and regulatory compliance programs.

Example Use Cases

Trading Floors

IGEL OS BENEFITS:

High-performance Graphics: Supports streamlined interaction with data-intensive applications, GPU enabled virtual and physical workstations.

- **Enhanced Security:** The read-only operating system, secure boot, encryption protocols, IGEL Preventative Security Model™ minimizes vulnerabilities and prevents trading data downloads from unauthorized access or tampering.
- **Seamless Integration with VDI/DaaS/SaaS/Remote Workstations/Secure Browser:** IGEL OS enables secure access to financial tools hosted on virtual desktop infrastructures (VDI) or desktop-as-a-service (DaaS) platforms, such as Microsoft Azure Virtual Desktop, Windows 365 Cloud PC, Omnissa, Citrix, and Island Enterprise Browser.

Call Centers

IGEL OS BENEFITS:

Locked-Down Environment: Prevents call center agents from downloading or extracting sensitive customer information.

- **Centralized Security Management:** Ensures compliance with regulatory standards such as PCI DSS for secure transactions.
- **Secure Remote Access for Work-from-Home Agents:** Allows flexible work models while supporting strict security policies.
- **Peripheral Compatibility:** Supports high-quality webcams, microphones, and headsets for virtual consultations. Also, scanners, signature pads, receipt printers, and check readers for seamless transaction processing.
- **Telephony:** Integration with softphones or virtual phones e.g. Genesys Cloud.

Branch Banking

IGEL OS BENEFITS:

Kiosk Mode for Self-Service Terminals: Restricts endpoints to specific financial applications, reducing security risks and making access secure for staff and clients.

- **Peripheral Compatibility:** Supports scanners, signature pads, receipt printers, and check readers for seamless transaction processing.
- **No Local Data Storage:** Ensures no sensitive customer data is stored locally, protects personal and financial information from breach if devices are stolen or compromised.
- **Secure Virtual Desktop Access:** Advisors can access secure cloud-hosted applications while ensuring compliance with PCI DSS and GDPR.
- **Centralized Management:** Simplify endpoint configuration, updates, and policy enforcement with IGEL UMS to distributed branch offices.
- **Significant Savings:** Repurpose existing hardware, reduce energy consumption, and secure shared workspaces to lower total cost of ownership.

Industry Spotlight: Government

Doing More with Constrained Budgets

Government agencies face unique challenges in endpoint IT. Strict regulatory requirements, heightened security demands, endpoint devices placed on restricted networks and deployed into hostile territory and the need to serve citizens efficiently, all compete for limited IT budgets. As Zero Trust requirements become mandatory, traditional endpoint strategies are unsustainable.

IGEL helps government organizations by complying with Zero Trust requirements, delivering the highest levels of security and driving the highest levels of ROI by extending the life of their devices, streamlining IT operations and eliminating redundant software costs. By providing a secure, optimized endpoint OS designed for highly secure environments, IGEL enables agencies to modernize endpoints without large-scale capital investments.

By the Numbers

An analysis of 11 Government organizations found:

\$350,000+

Average annual savings per organization

63%

Average reduction in endpoint IT expenditure

Avg. Savings

Distribution:

48%

Hardware savings

12%

IT Labor savings

40%

Software savings

These savings free up substantial capital that can be redirected into priority initiatives such as Zero Trust security, SASE adoption, and regulatory compliance programs.

Example Use Cases

Field Offices and Agencies

IGEL OS BENEFITS:

Provides secure, policy-controlled access to applications via VDI/DaaS solutions like Azure Virtual Desktop, Citrix or Omnisia.

- **Reduces the attack surface in distributed environments** through Zero Trust capabilities through the IGEL Preventative Security Model.
- **No information is stored on the endpoint device** ensuring there is no data breach in the event of loss or theft.
- **Supports a wide range of peripheral devices** such as printers, scanners, signature pads and cameras that may be utilized for delivering public services.

Classified and Secure Facilities (DoD, Intelligence, and Cybersecurity Centers)

IGEL OS BENEFITS:

The IGEL Preventative Security Model significantly improves endpoint security by eliminating the attack vectors targeted by bad actors.

- **Supports NIST CSF** and other cybersecurity frameworks.
- **Simplifies endpoint provisioning** in secure networks with remote management.
- **Provides a trusted endpoint** for secure VDI/DaaS solutions adhering to federal standards.

Endpoint Business Continuity

IGEL OS BENEFITS:

Quickly Reconnect Workers: Clean boot compromised Windows devices to IGEL OS enabling employees to access collaboration resources and public services to be re-instated.

- **Enable BYOD or remote work:** Secure BYOD access from remote workers or contractors.
- **Prevention is Better Than Cure:** Avoid endpoint ransomware through the IGEL Preventative Security Model.

Industry Spotlight: Manufacturing

Extending Asset Lifecycles at the Edge

Manufacturers operate large numbers of distributed endpoints across plants, warehouses, and offices. These devices are critical for production monitoring, logistics, and workforce support, but frequent refresh cycles and complex management demands make them costly to maintain.

In recent years, the convergence of IT and OT networks has shone a spotlight on cyber-security exposing systems that were not designed for frequent security updates, remote management or cyber-resilience. Shop-floor environments in particular are capital intensive, and refreshing thousands of devices requires interruptions to manufacturing and places a heavy burden on IT budgets.

IGEL enables manufacturers to extend the life of existing endpoints while delivering a modern cyber-security to the edge. By decoupling workloads from the device and delivering them through 11VDI, DaaS, or through virtualized Windows endpoints with IGEL Managed Hypervisor, IGEL ensures that even older devices remain secure and productive. This approach aligns with manufacturers' focus on cost efficiency, reliability, and operational resilience.

By the Numbers

From an analysis of 11 manufacturing organizations:

\$1.3million+

Average annual savings per organization

65%

Average reduction in endpoint IT expenditure

Avg. Savings
Distribution:

66%

Hardware savings

19%

IT Labor savings

15%

Software savings

These savings allow manufacturers to redirect funds toward automation, supply chain digitization, and Industry 4.0 initiatives.

Example Use Cases

Logistics Centers and Warehousing

IGEL OS BENEFITS:

Peripheral Support: Integrates with scanners, printers, and RFID reader tracking devices for seamless logistics operations.

- **Secure Operations:** Protects sensitive shipment data and ensures secure communication with carriers.
- **Centralized Control:** Enables IT admin to manage endpoint devices across various locations and secure access to critical applications from one IGEL UMS console.

Digital Signage

IGEL OS BENEFITS:

Enhanced Security: Strengthen digital signage with the Preventative Security Model™ to eliminate these devices as a potential ransomware attack vector.

- **Repurpose Devices:** Repurpose Windows devices that cannot move to Windows 11 to reduce TCO and e-waste.
- **Centralized Management:** Manage digital signage devices in the same way as other IGEL OS devices including session shadowing for troubleshooting.

Production Line Terminals

IGEL OS BENEFITS:

Security: IGEL's Preventative Security Model delivers endpoint security protecting critical manufacturing systems as IT and OT networks converge. IGEL OS is read-only, stores no data on the endpoint, and is encrypted.

- **Fast Secure Access:** Single sign-on (SSO) ensures only authorized personnel can access sensitive production data from any device. Badge tap access enables production line employees and shift workers to quickly move between workstations to access targets, instructions, safety, metrics, and more according to user profiles.
- **Virtualized Legacy Windows Workloads:** IGEL Managed Hypervisor virtualizes legacy workloads to enable execution on new hardware without replacing production systems.

- **Centralized Control:** Enables supervisors to securely manage dispersed endpoint devices to access enterprise applications from one management console.
- **Peripheral Compatibility:** Support for scanners, RFID readers, and labelling devices.
- **Reliable Uptime:** Lightweight IGEL OS ensures minimal disruption during operations with a small footprint. IT admins can assign apps to user profiles and enable streamlined updates.

Industry Spotlight: Retail

Retail organizations manage highly distributed IT estates, often with thousands of endpoints spread across diverse sites including stores, warehouses, front of house and back-offices. Supporting these environments traditionally requires frequent hardware refreshes, significant IT labor, and costly endpoint software – expenses that directly impact already thin margins.

IGEL helps retailers simplify endpoint management, reduce refresh frequency, and eliminate redundant software costs. With IGEL, endpoints act as secure access points for SaaS, VDI, and DaaS workloads, ensuring a consistent user experience across hundreds or thousands of locations without the burden of heavy device requirements.

By the Numbers

From an analysis of 16 retail organizations:

Nearly \$500k

Average annual savings per organization

55%

Average reduction in endpoint IT expenditure

Avg. Savings
Distribution:

41%

Hardware savings

36%

IT Labor savings

23%

Software savings

These savings allow retailers to reinvest in digital transformation projects such as omnichannel platforms, supply chain optimization, and enhanced in-store customer experiences.

Example Use Cases

Digital Signage and In-Store Displays

IGEL OS BENEFITS:

Secure Kiosk Mode: Locks signage and interactive displays into specific applications, preventing unauthorized access or tampering.

- **Centralized Management:** Enables IT to centrally update, troubleshoot and manage thousands of digital display screens and centrally monitor devices via IGEL UMS.
- **Optimized Performance:** Provides a lightweight OS with minimal resource requirements, ensuring smooth playback of HD video, animations, and interactive content.
- **Cost-Effective Hardware Extension:** Allows retailers to repurpose existing hardware for digital signage, reducing capital expenditure on new displays.
- **Broad Platform Support:** Ensures seamless integration with Enterprise Browsers, SaaS-based signage platforms, and cloud-hosted content management systems (CMS).

IT & Security Operations

IGEL OS BENEFITS:

Zero Trust Security Framework: The IGEL Preventative Security Model supports Zero Trust architectures integrating with leading security SASE, IAM UEM and DEX vendors. IGEL OS removes the attack vectors targeted by bad actors.

- **Conditional Access Identity and Access Management:** Integration with leading IAM vendors enables conditional access including only enabling managed endpoint devices to authenticate, helping to protect against stolen credential attacks.
- **Centralized Endpoint Management:** IT can manage all corporate and retail store endpoints remotely via IGEL UMS ensuring the latest security patches.
- **Seamless SaaS & VDI Integration:** Supports corporate access to Citrix, Omnisia, Microsoft Azure Virtual Desktop, and SaaS productivity tools.

Business Continuity in Retail

IGEL OS BENEFITS:

Rapid Endpoint Recovery: IGEL OS enables fast recovery of compromised Windows endpoints with IGEL Dual Boot and USB Boot. Endpoint devices are clean booted in seconds enabling access to critical communication applications or restored retail systems.

- **Secure, Read-Only OS:** Protects against ransomware and malware by preventing unauthorized changes or data storage on endpoints.
- **Remote Management:** Allows IT teams to quickly reconfigure and restore access to retail applications via IGEL UMS.
- **Hardware-Agnostic Flexibility:** Supports repurposing existing desktops, laptops, and thin clients to reduce downtime and hardware replacement costs.

Exploring Savings Categories

Hardware Savings: Extending the Life of Endpoints

The Challenge of Traditional Endpoints

Traditional endpoints are expensive to purchase, maintain, and refresh. Standard operating systems run hundreds of background services and processes, requiring significant CPU and memory resources. As a result of the continually increasing workload, devices quickly become obsolete, forcing organizations into costly refresh cycles every 3 to 5 years.

The Windows 11 migration compounded this problem: many existing endpoints cannot meet Windows 11 hardware requirements, pushing organizations toward premature device replacement. For CIOs and CISOs, this represents a massive capital expense.

The Industry Shift: Cloud-First, Centralized Data

Over the past decade, enterprise IT has steadily shifted toward a cloud-first or hybrid strategy. Mission-critical applications and data have been centralized, with workloads increasingly delivered through SaaS, VDI, and DaaS. This architectural change fundamentally alters the role of the endpoint. With workloads and data delivered from the cloud, the endpoint no longer needs to run a heavy, traditional operating system. In fact, doing so often increases risk, complexity, and cost.

How IGEL Unlocks Hardware ROI

The Challenge of Traditional Endpoints

IGEL changes the economics of endpoint computing by enabling organizations to deliver only what the user needs in hybrid and cloud first environments:

- **Optimized OS:** IGEL's secure endpoint OS is just 1.5 GB compared to a traditional OS footprint of 64 GB. Devices remain viable longer because they only run the services required to access cloud-delivered applications.
- **Repurpose Devices:** Existing endpoints can be converted into IGEL-powered devices instead of being replaced, often doubling the lifespan of the endpoint and eliminating entire refresh cycles.
- **Buy more energy efficient, lower power devices when refresh is required:** Due to the smaller workload running at the endpoint, lower power processors (e.g. i3, i5 vs i7, i9) can deliver an exceptional user experience for most use cases.
- **Windows 11 Migration Relief:** Rather than buying new hardware, organizations can host Windows workloads in the cloud (e.g., Windows 365 or Azure Virtual Desktop) and access them securely through IGEL on existing devices.

THE RESULT:

Millions of dollars saved by avoiding or deferring endpoint purchases – while enabling a more secure, cloud-ready IT model.

By the Numbers

Across industries, From the analysis of 150+ organizations:

- **52% of savings** come from hardware cost avoidance.
- **Organizations avoided hundreds to thousands** of device purchases annually by extending lifecycles.
- **In manufacturing, 66% of total savings** came from hardware lifecycle extension.

On average, **52%** of IGEL ROI comes from hardware lifecycle extension.

IT Department Labor Savings: Simplifying Endpoint Management

The Operational Burden of Traditional Endpoints

Managing traditional endpoints is time-consuming and resource intensive. Large operating systems require multiple layers of security and management software, platform training, and retraining, frequent patching, complex configuration, and support from multiple security and management agents. IT departments often dedicate significant staff time to:

- Imaging and configuring new devices
- Patching and updating large OS environments
- Responding to frequent end-user support tickets
- Attending training or taking certifications for multiple products
- Recovering systems compromised by ransomware or malware

This overhead translates directly into higher costs. In many organizations, the effective support ratio is just one IT administrator per 5,000 endpoints – a model that strains resources and increases risk as environments scale.

The IGEL Advantage in IT Operations

IGEL dramatically reduces the operational burden by simplifying endpoint management. Its small, modular OS footprint, combined with centralized administration tools, allows IT teams to do more with fewer resources.

Key differentiators include:

- **Faster Deployment and Configuration:** IGEL installs in minutes versus hours for traditional endpoints. Imaging and provisioning are streamlined with minimal dependencies.
- **Reduced Patch Management:** With a smaller, modular OS, patching cycles are less frequent and less complex.
- **Lower Support Volumes:** IGEL OS's reduced complexity reduces helpdesk tickets and simplifies troubleshooting.
- **Remote Support Built-In:** IT teams can resolve issues faster with integrated remote assistance tools.
- **Secure by Design:** By reducing the attack surface, IGEL minimizes the likelihood of ransomware or malware recovery efforts.

THE RESULT:

IGEL customers often achieve IT admin-to-user ratios as high as 1:20,000, compared to 1:5,000 with traditional endpoints.

By the Numbers

From the aggregated analysis of 150+ organizations:

- Customers report up to 4× improvement in IT admin-to-user ratios.
- Helpdesk call volumes are significantly reduced, cutting both cost and response times.

25% of all savings with IGEL come from IT labor efficiency.

Software Savings: Eliminating Redundant Endpoint Costs

The Hidden Cost of Endpoint Software

Traditional endpoints require a complex software stack to secure, manage, and support the device.

Typical additions include:

- Antivirus and Endpoint Detection & Response (EDR/XDR) tools
- Data Loss Prevention (DLP) software
- Backup and recovery agents
- VPN clients
- Endpoint management and monitoring tools

Individually, each license adds incremental cost. Collectively, they create an expensive ecosystem that drives up per-device spending and increases operational complexity.

The IGEL Advantage in Software Efficiency

IGEL reduces or eliminates the need for this heavy software layer. Its secure-by-design OS minimizes the endpoint attack surface and provides the core security and management capabilities enterprises require without layering multiple agents. While leading security platform agents are supported IGEL OS, they are generally added for compliance reasons or telemetry reasons rather than as a necessity as with traditional endpoints.

With IGEL, organizations can:

- Eliminate costly endpoint security tools such as antivirus, EDR, or VPN clients.
- Reduce backup and recovery requirements, since no critical data is stored on the endpoint.
- Simplify compliance with built-in security and centralized management.
- Lower licensing and support overhead, replacing a stack of endpoint agents with a single modular OS.

This streamlined approach not only reduces costs but also improves security by reducing dependencies and points of failure.

By the Numbers

From the aggregated analysis of 150+ organizations:

- **Customers eliminate multiple endpoint agent licenses**, with annual savings ranging from hundreds of thousands to several million dollars depending on scale.
- In healthcare, for example, **25% of overall savings came from software stack reduction**.

23% of all IGEL ROI comes from software savings.



Conclusion: Unlocking Endpoint ROI and Building the Future

The evidence is clear. Across industries, organizations that adopt IGEL can achieve substantial, measurable ROI. From these analyses, organizations projected on average a 62 percent reduction in endpoint IT expenditure, equating to nearly one million dollars in annual savings per organization. These savings are validated consistently, whether in healthcare, financial services, government, manufacturing, or retail.

But the IGEL story is not only about reducing costs. By extending device lifecycles, simplifying IT operations, and eliminating redundant software stacks, IGEL frees up scarce resources to be reinvested where they matter most: strengthening security, enabling hybrid and cloud-first strategies, and delivering better experiences for employees and customers alike.

Endpoints have long been treated as a sunk cost – a necessary burden that consumes budget year after year. IGEL challenges that assumption. With IGEL, the endpoint becomes a source of ROI and the foundation for the next generation of secure, agile, and sustainable computing.

For CIOs and CISOs, the choice is simple: continue to accept the high costs and inefficiencies of traditional endpoint strategies, or unlock a new model where security, efficiency, and value go hand in hand.

IGEL delivers the proven ROI today, and the strategic foundation for tomorrow.

Let's talk ROI – **contact IGEL** for an analysis today.