sonet.io

White Paper

Beyond the Sticker Price: A 36-Month TCO Analysis of Business Laptops and What It Means for IT Strategy

For decades, IT leaders have built device strategies around a single number: the sticker price of a laptop. But in today's distributed, dynamic, and security-focused environment, that number is increasingly misleading.

This white paper presents the findings of a 2025 total cost of ownership (TCO) analysis across three common classes of business laptops, mid-range, high-end, and GPU-enabled, over a 36-month lifecycle. The results are clear: the real cost of a business laptop is often 2–3 times higher than the purchase price once you factor in software, security, support, logistics, and lifecycle maintenance.

With mid-range laptops costing nearly $3,400 over three years and GPU-enabled systems surpassing $8,000, the economic case for rethinking endpoint strategies is growing stronger.

This paper helps IT and finance leaders understand:

- Where traditional device TCO costs are hiding
- What's driving cost growth in today's hybrid work environment
- How to evaluate modern, browser-based alternatives that eliminate device overhead entirely

If your team is managing hundreds, or even thousands, of corporate devices, this research provides the hard numbers to fuel a smarter conversation about cost, agility, and security.

Methodology

This TCO analysis models the full 36-month lifecycle cost of corporate laptops across three representative categories:

Device Categories:

- **Mid-Range Business Laptop:** ~$1,150 (typical price range $800–$1,500)
- **High-End Business Laptop:** ~$2,000 (typical price range $1,501–$2,500)
- **GPU-Enabled Laptop:** ~$3,000+ (typical price range $2,501+)

Timeframe:

- 36 months per device, aligned with common refresh cycles

Included Cost Categories:

- Hardware purchase price
- Initial setup and configuration
- International shipping and logistics
- Support and help desk services
- Software licensing: OS, productivity suites, endpoint protection, remote management, Endpoint Detection and Response (EDR), encryption, URL filtering, VPN clients, and enterprise browsers
- Security stack: Antivirus, Data Loss Protection (DLP), Multi-factor Authentication (MFA), Cloud Access Security Broker (CASB)
- Endpoint management platforms (e.g., Intune, JAMF, Workspace ONE)
- Hardware repairs and accidental damage
- Power and environmental overhead
- End-of-life decommissioning and device recovery

Data Sources:

- 2025 market benchmarks for software licensing and IT services
- Enterprise deployment data and user interviews
- Internal cost modeling from global mid-market and enterprise deployments

The result is a realistic, fully loaded view of device costs, not just at acquisition but through the entire lifecycle of deployment, use, support, and retirement.

TCO Findings: Cost Breakdown by Device Type

The 36-month total cost of ownership (TCO) analysis reveals a striking pattern: the initial purchase price accounts for a small portion of the total financial commitment. In some cases, it's less than a third of the real cost.

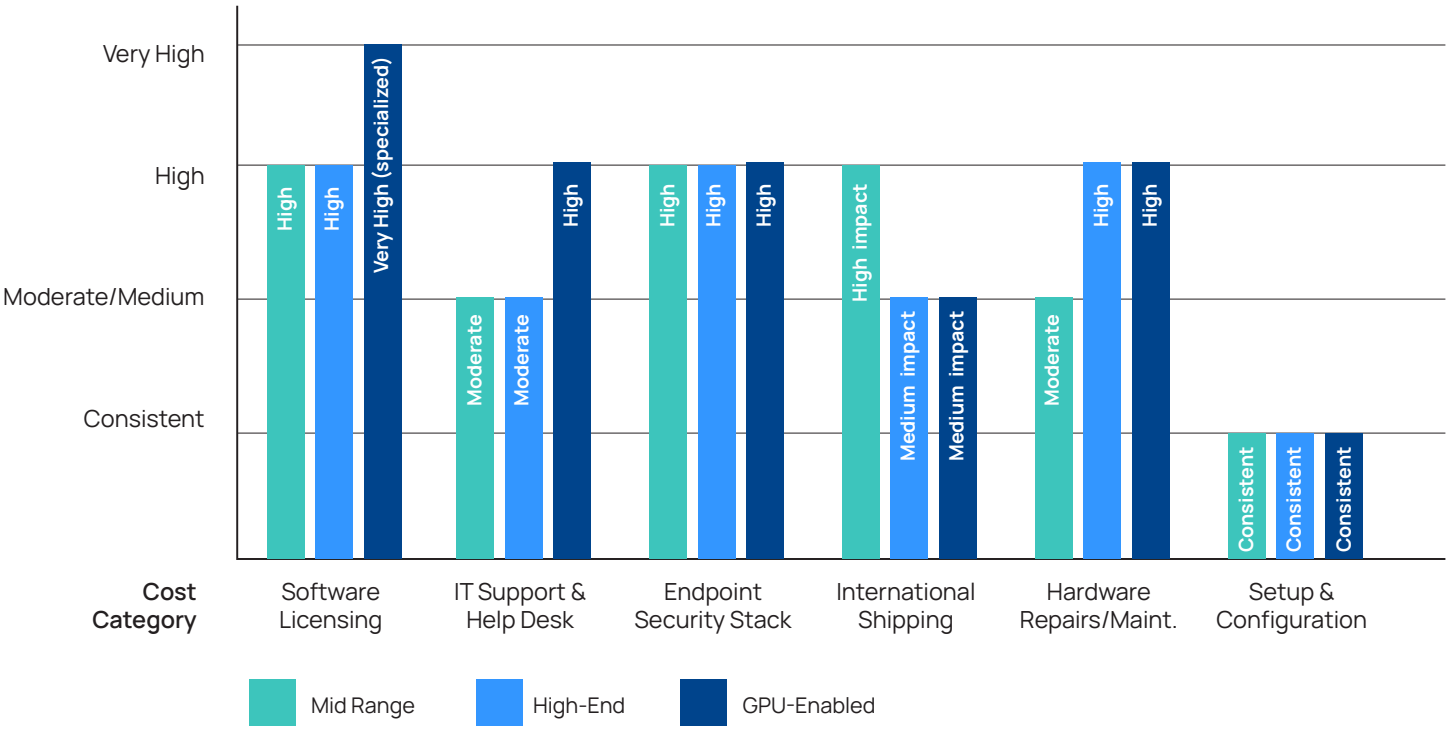
Side-by-Side Breakdown

Laptop Type	Purchase Price	Non-Purchase Costs	Total 3-Year TCO	% Over Purchase Price
Mid-Range Laptop	$1,150	$2,248	$3,398	195.5%
High-End Laptop	$2,000	$2,350.25	$4,350.25	117.5%
GPU-Enabled Laptop	$3,000	$5,364.13	$8,364.13	178.8%

Key Insight:

As device sophistication increases, so does the absolute cost of ownership. But mid-range devices exhibit the highest relative cost inflation, primarily because fixed per-device costs like security software and international shipping make up a larger percentage of their lower purchase price.

Key Cost Drivers by Category



Why It Adds Up So Fast

Every device adds not just a hardware line item, but a cascade of recurring costs:

- Licensing is annual.
- Help desk is ongoing.
- Security requires constant updates.
- Logistics are unpredictable, especially across borders.
- End-of-life returns often fail, leaving assets lost or unsecured.

Most of these costs go underreported, are spread across departments, buried in IT services budgets, or assumed as baseline.

What's Driving These Costs Higher in 2025 and Beyond

The total cost of business laptops isn't just high, it's growing. As IT teams scale support for global, hybrid, and temporary workers, the operational demands around each device have multiplied. And beyond the obvious cost centers, there are hidden line items, like peripherals, that further inflate the total cost of ownership.

Remote and Global Workforces

Supporting a distributed workforce means more than just getting laptops into the hands of users. It means shipping, tracking, and supporting a complete workstation—often across borders and time zones.

Every new hire or contractor may require:

- A laptop, pre-imaged and configured
- Compatible power adapters, docking stations, or video cables
- Peripheral accessories like scanners, webcams, headsets, or printers
- Pre-approved devices for compliance or compatibility reasons

Shipping these kits globally creates cost, risk, and administrative overhead. Customs delays, asset loss, and failed Return Merchandise Authorization (RMA) returns are common. Once deployed, these assets also increase the IT support burden, especially when something breaks or fails to connect.

With Sonet.io, users can access everything they need from any device they already own, and use their existing peripherals without compatibility concerns. There's no need to source or ship accessories. Users can plug in what they have and get to work, securely, through the browser.

Software and Security Stack Expansion

Most corporate laptops require:

- OS and office productivity suites
- Endpoint protection and EDR
- VPN clients, Remote monitoring and management (RMM) tools
- MFA, encryption, DLP, CASB
- Specialty tools (especially for GPU-enabled workstations)

Most of these are licensed per device, with recurring costs and setup complexity that scale linearly as headcount grows.

Peripheral Provisioning

Device provisioning isn't just about laptops. For many users, especially remote workers, IT must also supply:

- Docking stations, webcams, headsets, and specialty adapters
- Printers and scanners for field teams, customer-facing roles, or compliance workflows
- Known-compatible peripherals to avoid support tickets and configuration issues

Each additional item increases cost and complexity, especially when shipped globally. Support teams are left managing not just devices, but a growing array of accessories that vary by user, region, and task.

But the impact goes beyond logistics and support. Every endpoint, and every peripheral connected to it, expands your attack surface.

Modern attackers increasingly exploit user devices to gain entry. Once compromised, those devices can become launch points for deeper intrusion.

- 70% of data breaches begin on endpoint devices, often triggered by phishing or malware (Verizon Business 2023 Mobile Security Index)
- 80–90% of ransomware attacks start on unmanaged or poorly secured machines (Microsoft Digital Defense Report 2023)
- Common attack paths include outdated software, unpatched vulnerabilities, and user-installed apps

These risks aren't theoretical, they're central to why securing every endpoint has become so resource-intensive. With browser-based delivery, applications and data never touch the local device. Users work securely with their own peripherals, from any machine, without increasing IT risk or complexity.

Rising Support Burden

Supporting end users with corporate devices doesn't end at setup. It's a continuous drain on IT time and resources. Over a three-year lifecycle, each device is a potential support magnet.

Common issues include:

- **Broken hardware** – cracked screens, failed hard drives, damaged ports, spilled coffee
- **Performance complaints** – devices running slow due to bloatware, malware, or user-installed software
- **Agent or VPN conflicts** – VPNs that fail to connect, endpoint agents that interfere with normal workflows
- **Peripheral setup** – compatibility issues with webcams, printers, and other accessories
- **Security remediation** – chasing down misconfigured or non-compliant machines

Each incident pulls IT into reactive mode, slows down users, and increases operational overhead. The more devices in play, the higher the total volume of these disruptions.

With Sonet.io, users access apps securely through a browser—no agents, no installs, no local performance issues. Devices are abstracted away from the work itself, which means no break/fix cycle, no rebuilds, and no lost days to "my laptop is acting weird" tickets.

Environmental and Power Costs

While modest on a per-device basis, power, cooling, and disposal costs add up, especially when multiplied across thousands of machines. And with sustainability becoming a board-level concern, the long-term impact of device-heavy operations is under new scrutiny.

Bottom Line

The combination of global logistics, recurring software licensing, support workload, and security stack complexity makes device-centric IT delivery more expensive and less sustainable each year.

In a 2025 context where agility, security, and cost-efficiency matter more than ever, the legacy model is showing its age.

Strategic Implications: Why Device-Centric IT Models Are Breaking Down

The traditional model of issuing corporate laptops for every user made sense when teams were centralized, networks were closed, and IT could control every endpoint. But in 2025, that model is cracking under pressure.

Lagging Onboarding = Lost Productivity

Every week a new user waits for a shipped laptop is a week of lost output. For contractors and offshore teams, the delay can stretch into weeks while the clock ticks on project timelines, billable hours, and security risk.

Device Management Doesn't Scale

Managing devices at scale means managing:

- Software licensing and renewals
- Endpoint patching and compliance
- Support requests and break/fix logistics
- RMA returns and asset tracking

As the business grows, the overhead grows faster. Instead of accelerating business outcomes, IT gets bogged down in device support.

Device-Based Security Creates Risk and Downtime

Most enterprises rely on a layered stack of endpoint security tools: EDR, VPN clients, DLP agents, CASB plugins, patching software, and browser hardening extensions. Each one adds complexity and potential failure points.

- Endpoint software can conflict with apps, reduce performance, or even break the device
- VPN issues are a top cause of support tickets, especially for global users
- EDR agents require regular patching and version control; mistakes can be catastrophic
- CrowdStrike's 2024 update error crashed over 8.5 million Windows machines worldwide, costing billions in lost revenue and support costs

These risks are unique to the device-centric model. When apps and data live on the endpoint, any failure becomes business-critical.

Budget Predictability Suffers

Device-related costs are distributed across multiple budget lines: hardware, software, shipping, support, security. This fragmentation hides the true cost and makes forecasting difficult. CFOs and procurement teams face unpredictable spikes in spend, especially when device refresh cycles hit.

Hybrid and BYOD Use Cases Are Hard to Support

Business needs have evolved. IT now supports:

- Contractors needing access for 30 days
- Employees switching to personal devices
- Offshore teams with unknown hardware environments

With a device-centric model, each new scenario requires workarounds, manual approvals, and security exceptions.

The Strategic Choice

IT leaders now face a clear decision:

1. **Double down on device-centric models** and accept the rising costs, complexity, and constraints…
2. **Or shift to a more agile, browser-based delivery model** that eliminates device dependencies entirely.

The rest of this paper explores what that shift looks like and what it makes possible.

A New Model: Browser-Based App Delivery

In contrast to the traditional device-centric approach, browser-based application delivery allows organizations to provide secure access to enterprise applications without provisioning hardware, installing software, or managing endpoints.

This model eliminates the device as a dependency. Instead, work is delivered directly through the browser, layered with fine-grained security, visibility, and access control.

How It Works

In a browser-based model, applications are no longer installed or executed on the user's local device. Instead, they run in the cloud and are rendered securely in the browser. This means apps and data never reside on the endpoint removing

the need for local installs, persistent storage, or intensive endpoint security stacks.

Users authenticate via single sign-on (SSO) and access their full workspace, including web apps, desktop apps, and even legacy systems, through a secure browser portal. IT controls access via policies, records session activity, and enforces security measures centrally.

What It Eliminates:

- Device procurement, shipping, and RMA logistics
- Endpoint agent installation and versioning (e.g., Intune, RMM tools)
- Endpoint security stack and firewall exceptions (e.g., VPN clients, antivirus, DLP agents)
- Per-device software licensing
- Delays in onboarding and offboarding
- Risk from data residing on user endpoints

Key Benefits of Browser-Based Delivery

Benefit	Impact
Fast Onboarding	New users can be provisioned in minutes, from any device
Zero Device Overhead	No hardware shipping, no agents, no refresh cycles
Built-in Zero Trust	Granular access policies, session monitoring, DLP all managed centrally
Lower TCO	Per-user pricing removes hidden costs and simplifies budgeting
Global Access	Users can securely work from any location or device—corporate or BYOD
Reduced IT Load	Admins spend less time troubleshooting, configuring, and supporting devices

Who It's For

This model is especially powerful for:

- Organizations with large contractor or offshore teams
- Enterprises undergoing digital transformation
- Companies retiring legacy VDI or VPN systems
- IT leaders aiming to consolidate security and simplify delivery

By decoupling application access from device ownership, IT regains control, improves security, and accelerates responsiveness to business needs.

Next, we'll compare the economic impact of the two models, traditional vs. modern, with side-by-side TCO modeling.

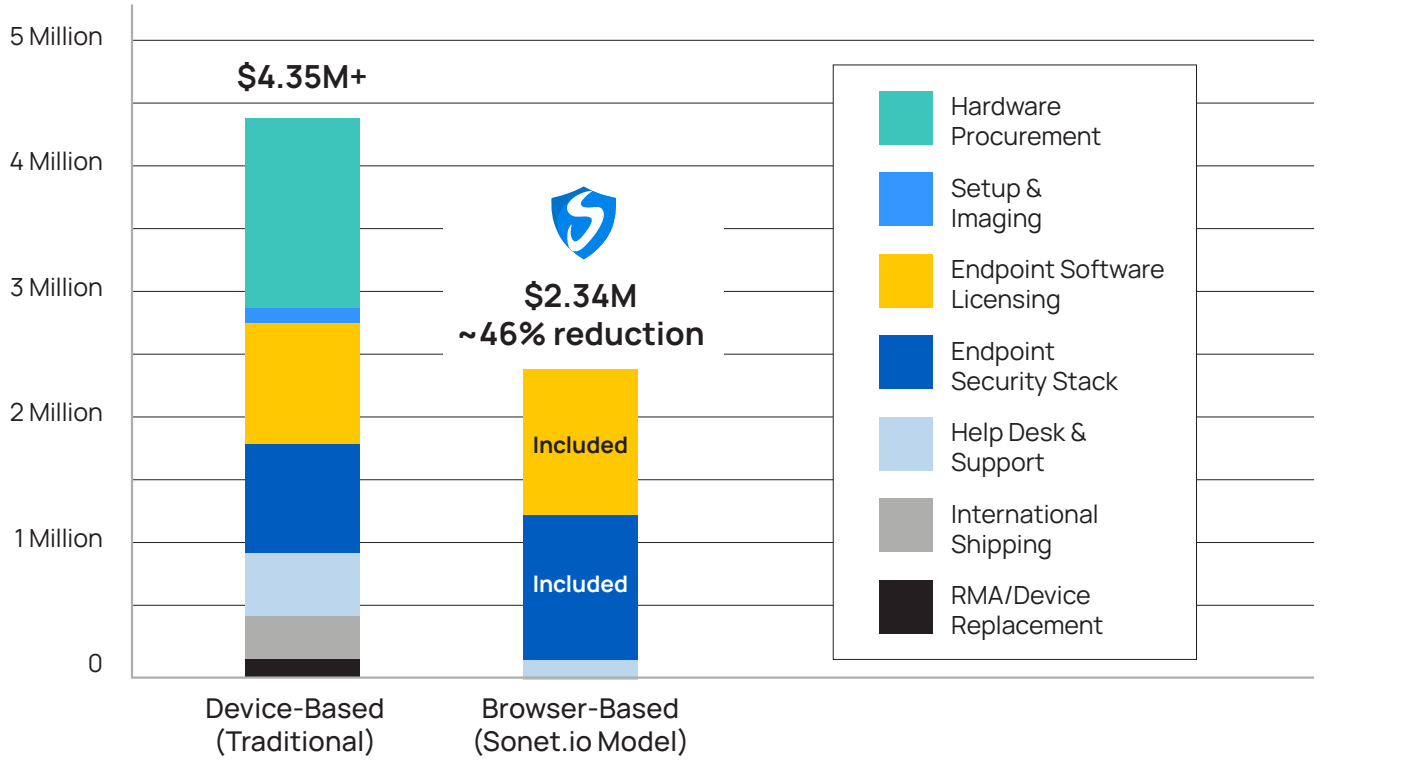
Scenario Modeling: Traditional Devices vs. Browser-Based Delivery

To quantify the financial impact of moving away from device-centric IT, we modeled a scenario comparing the 36-month cost of managing 1,000 users using traditional laptops versus a browser-based delivery model.

Scenario Assumptions

- 1,000 users over 3 years
- Mix of mid-range and high-end laptops
- Global workforce (30% international)
- Traditional model includes shipping, software, security, and support
- Modern model uses a flat per-user subscription with no device or shipping costs

Total Cost Over 3 Years (1,000 Users)



*Note: Application licensing (e.g., Microsoft 365, SaaS subscriptions) is not included in this model. These costs are assumed to be equivalent across both approaches.

Unmodeled, But Critical: Security Risk Reduction

While this model captures hard costs, it does not include potential losses tied to security breaches or compromised endpoints, which are rising in frequency and severity.

Traditional endpoints increase exposure by:

- Storing local credentials and cached data
- Running unmanaged or out-of-date agents
- Requiring VPNs and open firewall ports
- Being lost, stolen, or tampered with in uncontrolled environments

Browser-based delivery changes this. With Sonet.io:

- Apps and data never touch the endpoint
- Zero trust policies control access by identity and posture
- Session activity is recorded and monitored centrally

This architectural shift drastically reduces your attack surface mitigating risks that could otherwise cost millions in breach response, fines, and lost productivity.

Key Takeaways:

- Traditional device delivery costs nearly double a browser-based model.
- Even without factoring in user downtime, onboarding delays, or risk exposure, the cost delta exceeds $2 million over 3 years for 1,000 users.
- With browser-based delivery, costs scale predictably and securely with no infrastructure required.

Strategic Takeaways for IT, Security, and Finance Leaders

The traditional device delivery model isn't just expensive—it's operationally siloed. IT owns onboarding and provisioning. Security owns endpoint protection, VPN policy, and data loss prevention. And Finance tries to track it all.

With browser-based delivery, these boundaries begin to dissolve.

If you're a CIO or VP of IT, ask:

- How much time is my team spending on provisioning, troubleshooting, and hardware logistics?
- How fast can we onboard (and offboard) a user securely—anywhere in the world?
- What's the true ROI of our endpoint investment?

If you're a CISO or Security Leader, ask:

- How much of our security effort is dedicated to securing the endpoint itself?
- Could we reduce our threat surface by shifting the execution layer off the device entirely?
- Are we overcomplicating compliance? If access is centralized and activity is logged, can we simplify audits and prove control without agent sprawl?

With Sonet.io, security and IT no longer need to build parallel workflows. Policies are enforced centrally. Sessions are monitored in real-time. No data lives on the endpoint. Security is embedded in the delivery model, not bolted on.

If you're in Finance or Procurement, ask:

- Are we accounting for the full TCO of each device?
- How predictable is our IT budget year over year?
- Could we reallocate endpoint costs toward higher-impact initiatives?

Conclusion: Time to Rethink Device-Centric Delivery

Forward-looking organizations are reducing complexity, not adding to it. They're shifting away from managing machines and focusing on delivering secure access to work, wherever it needs to happen.

Browser-based app delivery enables that shift.

It simplifies access. Slashes cost. And strengthens security by design.

Laptops aren't going away, but your reliance on them doesn't have to define your strategy.

This white paper lays bare the cost of doing things the old way. The future of IT is lighter, faster, and built for secure scale. It's time to stop managing hardware and start delivering work.

Appendix: Cost Inputs and Assumptions

Device Purchase Prices

- Mid-range: $1,150
- High-end: $2,000
- GPU-enabled: $3,000

Recurring Costs

- Software Licensing: $20–$40/month average per device
- Endpoint Security Stack (AV, DLP, MFA, CASB): $10–$20/month average per device
- Endpoint Management Platforms (e.g., Intune, JAMF): $8–$12/month average per device
- EDR (Endpoint Detection & Response): $5–$10/month average per device
- VPN Clients & Infrastructure: $3–$8/month average per device
- URL Filtering, Encryption, Enterprise Browsers: $5–$10/month average per device
- Help Desk & Support: $15/month average per device
- International Shipping (One-Time): $150–$300 per device
- Setup & Imaging (One-Time): $50–$150 per device

Modern Model Pricing

- Sonet.io: comprehensive Application Delivery Platform - $75 per concurrent user per month, including control plan, compute, security (zero trust, DLP, geo-fencing), and observability (logging, alerts, session recording).
- Assumes no physical infrastructure, no shipping, and centralized admin

sonet.io

Work Securely From Any Device

sales@sonet.io

Find us online at **sonet.io**

3031 Tisch Way, 110 Plaza West
San Jose, CA 95128