sonet.io

White Paper

Breaking Free from Remote Work Challenges

How to Eliminate Shipping Delays and BYOD Risks While Empowering Global Teams

Legacy remote work methods are failing global IT teams.

Legacy methods for managing remote workforces—like shipping pre-configured devices or relying on unsecured BYOD policies—are creating significant operational challenges for IT leaders. These approaches delay onboarding, inflate costs, and leave organizations exposed to security and compliance risks.

Modern solutions, such as Sonet.io, transform remote work management with browser-delivered access, zero-trust security, and a simplified, scalable approach—without the need for specialized enterprise browsers.

In this white paper, you'll learn:

- The operational and financial impacts of legacy methods.
- Why unsecured BYOD is a growing security threat.
- How Sonet.io eliminates these challenges and delivers real-world results.

Why Device Shipping Is Holding You Back

Legacy device shipping processes are cumbersome, costly, and slow, creating bottlenecks for IT teams and global workers alike.

The Delays: Why Device Shipping and Procurement Slow You Down

Equipping global teams often involves significant delays, caused by both shipping and procurement challenges.

- **Shipping Delays:** Pre-configured devices often take weeks—or even months—to arrive. International logistics are frequently complicated by customs clearance, regional regulations, and supply chain disruptions, particularly during periods of high demand or geopolitical instability.
  - **Stat:** One IT leader shared that it took three months to procure and deliver laptops for new hires in Eastern Europe, leaving employees idle and delaying critical projects.

- **Procurement Challenges:** In some regions, sourcing enterprise-grade hardware is particularly difficult due to limited availability or supply chain bottlenecks. Companies often have to wait for local suppliers to restock or resort to importing devices, adding additional delays.
- **Impact on Business:** These issues stretch onboarding timelines, slow productivity, and force IT teams to focus on logistical challenges rather than strategic priorities.

The Costs: Why Legacy Processes Drain Your Budget

Legacy approaches to managing remote teams come with significant hidden costs, particularly when it comes to shipping and maintaining devices across borders. When factoring in shipping, fees, and losses, the true cost of a device often far exceeds its purchase price. These inefficiencies stretch IT budgets and make it harder to scale operations globally.

- **High Shipping Costs:** Shipping a single laptop internationally can cost anywhere from $1,000 to $3,000, depending on the destination and urgency. These costs often multiply with additional expenses like insurance and specialized packaging.
- **Customs Duties and Taxes:** Many countries impose hefty import fees on electronic devices, further inflating the cost of equipping global teams.
- **Return Costs:** When employees leave, companies face additional expenses to retrieve devices:
  - **Shipping Fees:** Returning devices internationally can be just as costly as initial delivery.
  - **Legal Fees:** Some companies incur legal costs to reclaim laptops from employees who refuse to return them.
  - **Losses:** In cases where retrieval isn't feasible, businesses often have to absorb the cost of the unreturned laptop.
- **Maintenance and Upgrades:** Beyond shipping devices for repairs or upgrades, the ongoing management of distributed hardware introduces significant operational costs:
  - **Patching Operating Systems:** IT teams must regularly patch OS vulnerabilities to maintain security. Coordinating patches across time zones adds complexity.
  - **Upgrading Applications:** Application updates often require IT intervention to resolve compatibility issues or failed installs, leading to downtime.
  - **IT Support Tickets:** Distributed devices generate frequent tickets for configuration errors, failed patches, or hardware issues—each requiring IT resources to resolve.
  - **Downtime:** Employees experience interruptions during maintenance, reducing productivity.

According to SolarWinds, downtime can cost businesses significantly. For small businesses, the average cost is approximately $427 per minute, translating to over $25,000 per hour. For larger enterprises, this escalates to about $9,000 per minute, or over $540,000 per hour. These figures underscore the critical importance of minimizing downtime to protect your bottom line.

Source: SolarWinds - "Micro-Outages Uncovered: Exploring the Real Cost of Downtime"

Compliance Risks: How Legacy Methods Leave You Exposed

Shipping, maintaining, and managing devices across borders isn't just costly—it's also risky. Legacy approaches often rely on endpoint security, which creates vulnerabilities when devices are improperly patched or misconfigured.

- **Unpatched Devices and Misconfigurations:** Improperly managed devices create significant security vulnerabilities. IT teams often struggle to ensure all distributed devices receive timely updates or are configured correctly, especially in global environments. This can lead to:
  - **Compromised User Accounts:** Hackers exploit vulnerabilities to hijack credentials and gain unauthorized access.
  - **Massive Data Breaches:** Once inside, attackers can exfiltrate data or disrupt critical operations, exposing sensitive information.
  - **Stat:** According to the 2023 Verizon Data Breach Investigations Report, the exploitation of vulnerabilities accounts for 5% of breaches, underscoring the importance of timely patching and proper configuration management.
- **The Stakes:** Losing or improperly wiping a device can lead to a data breach, damaging the trust of even the most loyal customers.
  - **Stat:** Under GDPR, organizations can face fines of up to €20M (~$20M) or 4% of global annual turnover, whichever is higher, for improper handling of sensitive data.
- **Reputational Damage:** Mishandling sensitive data doesn't just result in fines—it erodes trust and brand equity. The long-term impacts of a breach can include:
  - **Loss of Market Share:** Customers seek alternatives to protect their data.
  - **Revenue Decline:** Breaches often lead to customer churn and lost opportunities.
  - **Weakened Competitive Positioning:** It becomes harder to attract or retain clients.
- **Why These Risks Are So Common:** Legacy methods rely on managing security at the device level, which is inherently fragmented and inconsistent. The more devices and endpoints a company has, the harder it becomes to ensure proper security hygiene across the board.

> Improperly patched devices and bad configurations are among the leading causes of security breaches. With Sonet.io, you eliminate these risks by delivering secure, centralized access to apps and data—without relying on endpoint security.

The IT Strain: Why Legacy Methods Overwhelm IT Resources

Managing devices globally requires substantial IT resources. Inventory tracking, hardware maintenance, and logistics coordination consume time that could be spent on innovation or strategic initiatives.

- **Imaging and Configuration:**
  - IT teams spend hours imaging devices, installing software, and configuring settings before shipping them to employees.
  - Stat: The average time to fully configure a device is 3–4 hours per laptop, and this can increase to a full day with additional software or complex configurations.
- **Chasing Shipments:**
  - Once devices are shipped, IT teams often find themselves tracking shipments, dealing with customs issues, or coordinating with local couriers to ensure devices reach their destinations.

For many organizations, the strain of managing these tasks internally becomes too great, prompting them to outsource parts of the process to third-party providers.

- **Costs of Outsourcing:**
  - Third-party vendors charge premium fees for imaging, configuring, and shipping devices, which can add hundreds of dollars per device to the overall cost.
  - Even with outsourcing, IT teams still need to oversee vendors, manage timelines, and ensure consistency across regions.

The Impact on IT Teams:

- **Burnout and Inefficiency:** IT professionals are stretched thin, juggling device logistics with their regular responsibilities.
- **Diverted Focus:** Strategic initiatives, such as improving cybersecurity or streamlining infrastructure, take a backseat to operational tasks.

Every day a new hire waits for their hardware, hundreds of dollars in productivity are lost. A $100,000/year employee costs over $400/day—and that's before accounting for missed project deadlines or team delays. With Sonet.io, new hires can securely access their tools on day one, no hardware required.

BYOD Without Proper Security: A Ticking Time Bomb

With growing global workforces, many companies feel stuck with BYOD (Bring Your Own Device) policies to enable remote work. But without the proper security infrastructure, this approach introduces significant risks.

Lack of Protection:

Without the right security measures, accessing corporate applications and data from personal devices opens doors to cyberattacks. Legacy solutions focus on device-level security, leaving apps and sensitive information vulnerable.

Compliance Challenges:

Unsecured BYOD setups can result in inconsistent security policies, making it difficult to meet compliance standards like GDPR, HIPAA, or CCPA.

BYOD Security Done Right:

To succeed with BYOD, businesses need a secure, scalable solution that protects apps and data on every device—without sacrificing user productivity.

A Browser-Delivered Approach to Secure Remote Work

Sonet.io eliminates the inefficiencies and risks of legacy methods, empowering IT teams to scale operations securely and cost-effectively.

Speed:

Onboard global employees in minutes. Sonet.io's browser-delivered platform eliminates the need for shipping pre-configured devices or waiting for hardware setups. Workers securely access web apps, desktop apps, desktops, etc. and data on day one, using their preferred browser on any device.

Security:

Sonet.io's built-in zero-trust architecture protects the applications and data your teams rely on. Every session is secured with features like MFA, DLP, and session monitoring, ensuring corporate resources remain safe—no matter where or how they're accessed. Features include:

- **Multi-Factor Authentication (MFA):** Stops unauthorized access.
- **Data Loss Prevention (DLP):** Prevents sensitive data from being shared or downloaded inappropriately.
- **Session Monitoring:** Real-time monitoring for suspicious activity.

Simplicity:

Sonet.io's browser-delivered platform empowers IT teams to centrally manage access, enforce policies, and monitor usage—without requiring specialized enterprise browsers or additional software.

Savings:

Sonet.io reduces costs by eliminating the need for hardware shipping and retrieval, while streamlining IT management.

Category	Legacy Methods	Sonet.io
Onboarding Speed	Weeks	Minutes
Security	Inconsistent	Built-in Zero-Trust
IT Costs	High	10x Savings

How One Global Leader Transformed Their Workforce

The Problem:

A global construction leader faced delays shipping pre-configured devices to remote employees across Southeast Asia, often taking weeks. Additionally, their unsecured BYOD policy created compliance risks and frequent security breaches.

The Solution:

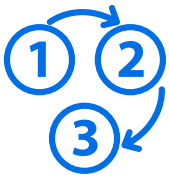
By implementing Sonet.io, the company replaced legacy methods with instant, browser-delivered access ensuring employees and contractors could connect through their preferred browsers while still being secured by zero-trust architecture—no specialized tools required.

The Results:

- 80% Faster Onboarding: Employees gained secure access to apps on day one.
- 10X Cost Savings: Eliminated hardware shipping, retrieval, and IT overhead.
- Enhanced Security: Protected sensitive data with Sonet.io's zero-trust approach.

Your Journey to Secure, Seamless Remote Work

Step 1: Assess Your Needs:



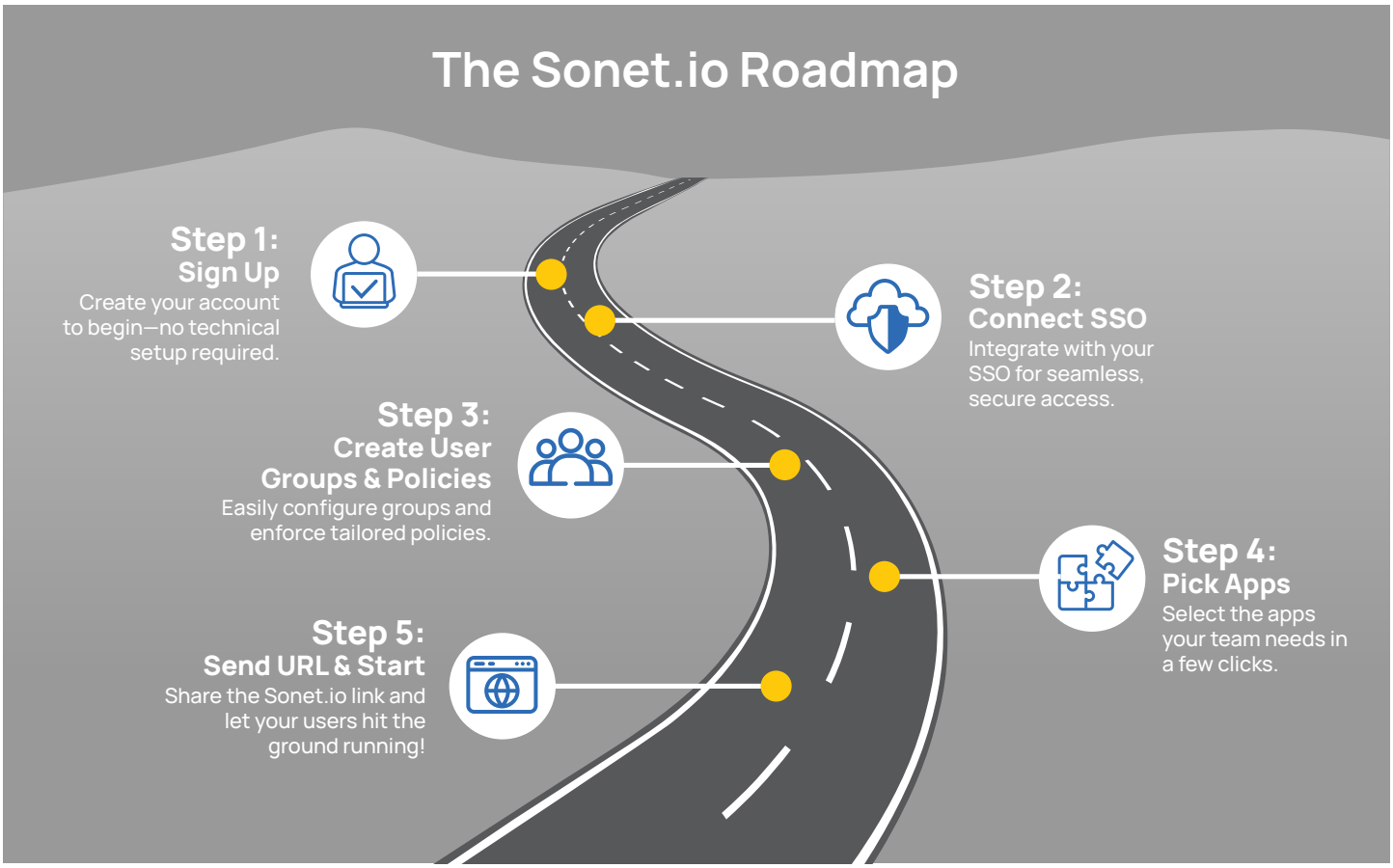
Map your current processes for onboarding, device management, and security to identify inefficiencies.

Step 2: Launch a Pilot Program:

Start with a team of remote employees to test Sonet.io's browser-delivered access and robust security features on your existing infrastructure.

Step 3: Scale with Confidence:

Roll out Sonet.io across your global workforce to reduce costs, enhance security, and improve productivity.



Legacy methods like shipping devices and relying on unsecured BYOD are no longer sufficient for managing today's global teams. Sonet.io empowers IT leaders to deliver fast, secure, and cost-effective remote access for every worker—no matter where they are.

Next Steps

Still evaluating your options? We're here to help.

Experience the Platform:
To see Sonet.io in action.

Contact Us :
Let us help you create a custom migration plan.

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