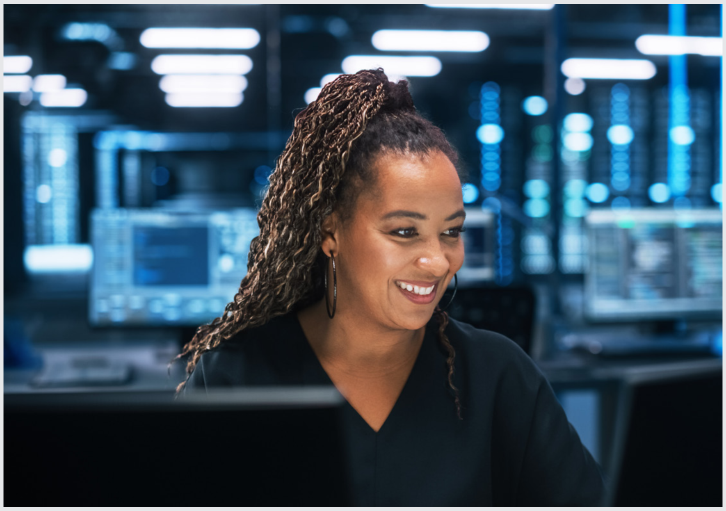
sonet.io

White Paper

From Risk to Resilience: Rethinking How You Access Legacy Software

Modernizing app delivery with zero trust security without rewriting code, deploying infrastructure, or compromising compliance.

Legacy software is still mission-critical for many enterprises—but how it's accessed has become a major liability. VPNs expose internal networks, data on endpoints is vulnerable, and tools like RDP and VDI add complexity and operational overhead. These models make it nearly impossible to enforce zero trust principles or ensure full visibility.



This paper explores how IT teams can shift from reactive security workarounds to a resilient, identity-based approach to legacy app delivery. By delivering applications through the browser with built-in zero trust controls, organizations can secure legacy systems, meet modern compliance requirements, and eliminate the infrastructure and configuration burdens that weigh down traditional solutions.

No code rewrites. No device installs. No compromise.

The Problem: Legacy App Access Is a Security Blind Spot

Despite investments in cloud and zero trust frameworks, many enterprises still rely on outdated methods to deliver legacy applications. VPNs provide broad network access, creating unnecessary exposure. RDP and VDI depend on trusted endpoints and add significant complexity and cost. Even with defined access policies, enforcement is inconsistent and visibility is limited leaving IT teams with blind spots they can't afford.

Legacy apps, often deployed in data centers or on-prem servers, remain tightly coupled to device-specific access, making it hard to control risk, onboard external users, or meet audit requirements. As security expectations rise, these delivery methods become liabilities.

Many IT teams recognize the paradox. They've kept legacy systems running with tools like Citrix or VPN, but those tools now create security and operational debt. One IT director shared:

> *"Yes, we had to load a Citrix client on every laptop. That's how we access AX 2012. Citrix is literally only used today for AX 2012. Everything else runs locally."*

While minimal in scope, this kind of isolated use case still brings full infrastructure requirements, endpoint configuration, and security gaps that IT teams must absorb.

Why Traditional Tools Break Zero Trust Principles

Zero trust isn't just a policy, it's an architectural mindset. But most traditional app delivery solutions violate its core assumptions:

Legacy Tool	Zero Trust Breakdown
VPNs	Provide broad network access violating least privilege
RDP Clients	Require full trust in the endpoint and network
Citrix / VDI	Add operational complexity but rely on layered point solutions
Endpoint Installs	Expand the attack surface and lack centralized visibility

Even when VPN or Citrix is used for just one app, they expose broad access by default. As one director pointed out, "There's some role-based restriction, but broadly speaking, yeah, users can download data to Excel, work on it, and reupload."

This lack of fine-grain control or monitoring makes audit readiness and compliance difficult especially when data movement happens on unmanaged devices.

In short, legacy tools assume trust at the wrong layers. They rely on perimeter defense, not identity- or context-driven access. And they make session monitoring or data protection difficult, especially in hybrid or BYOD environments.

Why Now? Rethinking What 'Works'

Legacy application delivery methods like Citrix, VPNs, and RDP often continue not because they're ideal, but because they're familiar. As one IT director put it:

> *"Just because it's working and not causing massive pain doesn't mean it's the best solution," said an IT director at a national equipment services firm.*

This mindset is shifting. Forward-thinking IT leaders are no longer satisfied with "working," they're evaluating what's optimal. And with security, compliance, and operational efficiency under pressure, outdated delivery models are falling short.

The numbers back it up. According to Enterprise Strategy Group, 97% of enterprises still rely on at least one Windows app, and 44% run 50 or more. Yet 32% of respondents say they'll replace all their Windows apps in the next three years, an aggressive goal that would require rewriting more than one app per month. As Gabe Knuth, Analyst at

Enterprise Strategy Group, noted during the EUC World Independence Keynote (2024):

> *"If we could have migrated these apps, we would have by now."*

Rather than wait for ideal conditions or stretch limited teams thin, many organizations are modernizing the way these apps are delivered by applying zero trust security, removing infrastructure burdens, and enabling access via browser without touching the apps themselves.

Rethinking Access: Secure Delivery Without Infrastructure

Despite the rise of SaaS and browser-delivered tools, legacy Windows applications still dominate enterprise environments. Even organizations investing heavily in modern platforms report running 100+ Windows apps in parallel. These aren't going away anytime soon and most can't be easily rewritten or replaced.

The problem isn't the apps. It's the outdated, insecure, and infrastructure-heavy ways they're delivered.

Sonet.io enables secure, identity-driven delivery of Windows, terminal, and thick-client applications via browser. It separates access from endpoint trust, eliminates the need for VDI or VPN, and enforces zero trust policies at the delivery layer with no code changes required.

How Sonet.io Enables Zero Trust for Legacy Apps

The leading driver for virtual desktop and application delivery today isn't performance, it's security.

As Analyst Gabe Knuth observed:

> *"Security is always the number one reason organizations make any decision about desktop virtualization."*

That's why Sonet.io delivers not just application delivery but built-in zero trust enforcement, session control, and full visibility for every legacy session.

Traditional tools secure the network perimeter. Sonet.io secures the application delivery model applying policy and control where user activity actually happens.

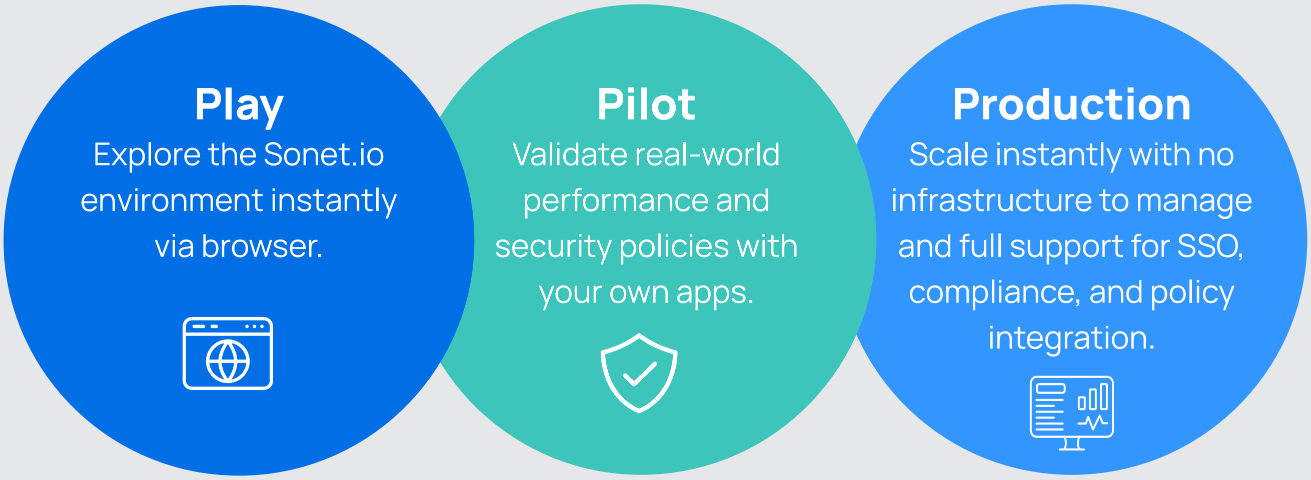
Key Capabilities:

- **Zero Infrastructure Exposure** – Apps stay where they are; Sonet.io handles delivery in the cloud.
- **Granular Access Controls** – Set policies by user, role, or group using existing SSO.
- **Integrated DLP & Session Controls** – Watermarking, clipboard restrictions, and full session recording are built in.
- **No Endpoint Risk** – No client installs or agent management. Users access apps via secure browser sessions. One IT lead noted, "Sonet opens up some freedom to access things from anywhere, regardless of device." That flexibility is critical but must be paired with strong controls on data movement, session behavior, and user roles.
- **Audit-Ready Visibility** – Real-time activity logs, alerts, and downloadable session records for compliance.

This model allows IT to apply consistent security to every app session, regardless of where the app lives or what device the user is on.

Getting Started: A Simple, Fast Path to Secure App Delivery

With Sonet.io, implementation is measured in hours, not weeks. The delivery model follows a proven path:



Play
Explore the Sonet.io environment instantly via browser.

Pilot
Validate real-world performance and security policies with your own apps.

Production
Scale instantly with no infrastructure to manage and full support for SSO, compliance, and policy integration.

There's no endpoint install, no rack and stack, and no lengthy provisioning process. Most teams are delivering apps within a day.

Conclusion: Secure the Past, Prepare for the Future

Legacy software isn't going away but the way it's delivered must evolve. With Sonet.io, IT teams can protect critical applications, meet modern security standards, and simplify operations without rewriting code or trusting endpoints.

It's not just faster or cheaper. It's fundamentally more secure.

Ready to See It?

Schedule a demo

Contact Sales
sales@sonet.io

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