citrix

The last mile of zero trust: securing the browser

Executive summary

Zero Trust has reshaped how enterprises grant access to applications and data. Identity is verified, devices are assessed, and traffic is inspected.

For organizations pursuing a secure access strategy, delivering any app, to any user, on any device, this foundation is critical.

But in most environments, enforcement still stops short of where work actually happens: the browser.

Today's enterprise risk does not come from unauthorized access alone. It comes from what authorized users can do inside SaaS applications, such as copying data, downloading files, interacting with GenAI tools, and working from unmanaged devices. Those actions occur inside the browser session, often beyond the reach of traditional access controls.

This is the last mile of Zero Trust, and for many enterprises, it remains unsecured.

Securing the work means extending Zero Trust enforcement beyond login and into the live browser session itself.

A reality check for modern secure access environments

Across enterprise environments, a few patterns show up consistently:

- SaaS access is protected, but in-session actions are not.
- VDI is used to “contain” SaaS risk, even when isolation is the only control.
- Endpoint agents don’t extend to contractors, partners, or BYOD users.
- Security teams rely on access controls to address problems that arise after login.

These are not architectural failures. They are the natural result of Zero Trust strategies that evolved around network and identity controls, while enterprise work shifted into the browser.

To truly secure the work, enforcement must move closer to user interaction.

Why the browser is the final enforcement point

The browser has become the default workspace for enterprise applications. CRM, collaboration, finance, HR, development tools, and GenAI services are all delivered through it.

Yet most security controls focus on network paths, authentication events, and managed endpoints. They do not consistently enforce policy at the moment of interaction, when data is viewed, copied, shared, or exfiltrated.

As a result:

- Sensitive actions go ungoverned once access is granted.
- Unmanaged devices create blind spots.
- Security teams compensate with heavier tools and exception workflows.

Zero Trust answers who can access an app. Secure access must also determine what happens next. The browser is now the enforcement point that completes the model.

The pressure on security leaders

Security leaders are accountable for protecting data across:

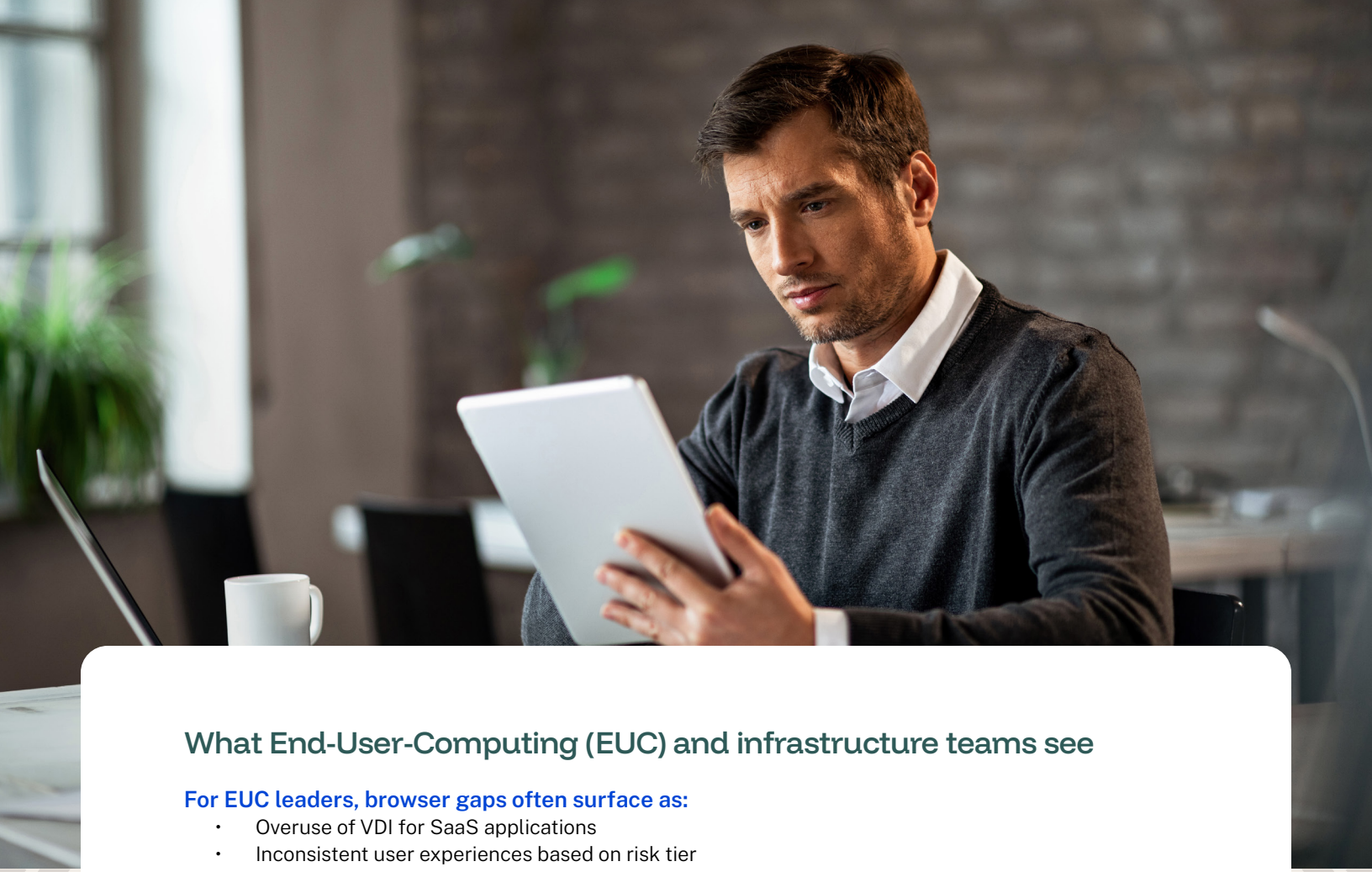
- Managed and unmanaged devices
- Employees, contractors, and third parties
- SaaS, internal apps, and emerging AI services

Existing approaches force tradeoffs:

- SSE and CASB platforms enforce access and traffic inspection, but often stop short of in-browser actions.
- Endpoint agents provide deep control, but don’t scale to unmanaged users.
- VDI isolates risk, but may add cost, friction, and infrastructure dependency when used broadly for SaaS.

The result is layered complexity without consistent enforcement. You end up with more tools, more exceptions, and more operational drag.

What’s missing isn’t another layer. It’s enforcement inside the workspace where work actually happens.



What End-User-Computing (EUC) and infrastructure teams see

For EUC leaders, browser gaps often surface as:

- Overuse of VDI for SaaS applications
- Inconsistent user experiences based on risk tier
- Growing tension between usability and security requirements

For infrastructure teams, the impact shows up as:

- Resource-intensive virtual desktop environments supporting simple web access
- Costs that don't align with SaaS-first work
- Security requirements driving architectural sprawl

These are symptoms of the same issue: secure access controls that live outside the browser instead of within it.

What changes, and what doesn't

Closing the last mile of Zero Trust does not require replacing existing investments. It's about enforcing policy where work actually happens.

What doesn't change

- Identity, SSE, and access platforms remain foundational.
- Users continue to work in the browsers they already trust.
- No new endpoint agent is required.
- VDI remains available for use cases that truly require isolation and non-browser-based apps.

What changes

- Policy enforcement extends into the live browser session.
- Controls apply to actions, not just access.
- Security posture follows identity and context, even on unmanaged devices.
- Risk is reduced without forcing users into alternate environments.

Why browser-native security now has enterprise backing

Browser-level enforcement is no longer theoretical. It is supported by the enterprise browser ecosystem itself.

With the continued enterprise evolution of platforms like Chrome Enterprise from Google, browser-native controls are now:

- Built on hardened enterprise browser foundations
- Integrated with identity and device posture frameworks
- Designed to support managed and unmanaged scenarios

This ecosystem backing validates the browser as an enterprise-grade enforcement layer, not a workaround or a niche tool.

For secure access strategies built around "any app, any device," the browser becomes the natural, scalable control point.

A more operational Zero Trust model

When browser-level controls extend existing secure asset investments:

- Security teams reduce reliance on VDI as a security workaround.
- EUC teams simplify delivery models without sacrificing protection.
- Infrastructure teams reserve resource-intensive environments for high-value scenarios.
- Users experience consistent security without disruption.

Most importantly, secure access becomes enforceable beyond the login screen.

Where most teams start

Organizations typically validate browser-level enforcement in one of three places:

1. **SaaS applications currently delivered via VDI**
   Reduce cost and friction while maintaining control.
2. **Contractors or BYOD users accessing sensitive systems**
   Enforce policy without requiring agents or managed devices.
3. **High-risk applications such as CRM, financial platforms, or GenAI tools**
   Control data exposure at the moment of interaction.

These use cases allow enterprises to extend secure access enforcement without changing how users work.

Closing the last mile of secure access

Zero Trust has solved access. Securing the browser makes it enforceable.

By extending policy into the browser session, organizations can reduce risk, simplify operations, align infrastructure to SaaS-first strategies, and protect modern work without forcing users into heavier tools or parallel environments.

When integrated with existing identity and SSE investments, Citrix helps enterprises close the last mile of Zero Trust by securing the browser where work actually happens. With Citrix, you can validate browser-level security with Chrome, the browser your users rely on.

Want to learn more?

- **Read the Director's Guide: Offloading web workloads from VDI.**
  Understand where browser-first access can safely replace VDI for SaaS and web use cases, reducing infrastructure cost while maintaining security.
- **Explore Citrix Secure Access with Chrome Enterprise.**
  See how Citrix extends Zero Trust directly into the browser, closing critical security gaps while seamlessly integrating with existing SSE and EUC strategies.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Headquarters
851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States