

# Modern contractor access checklist

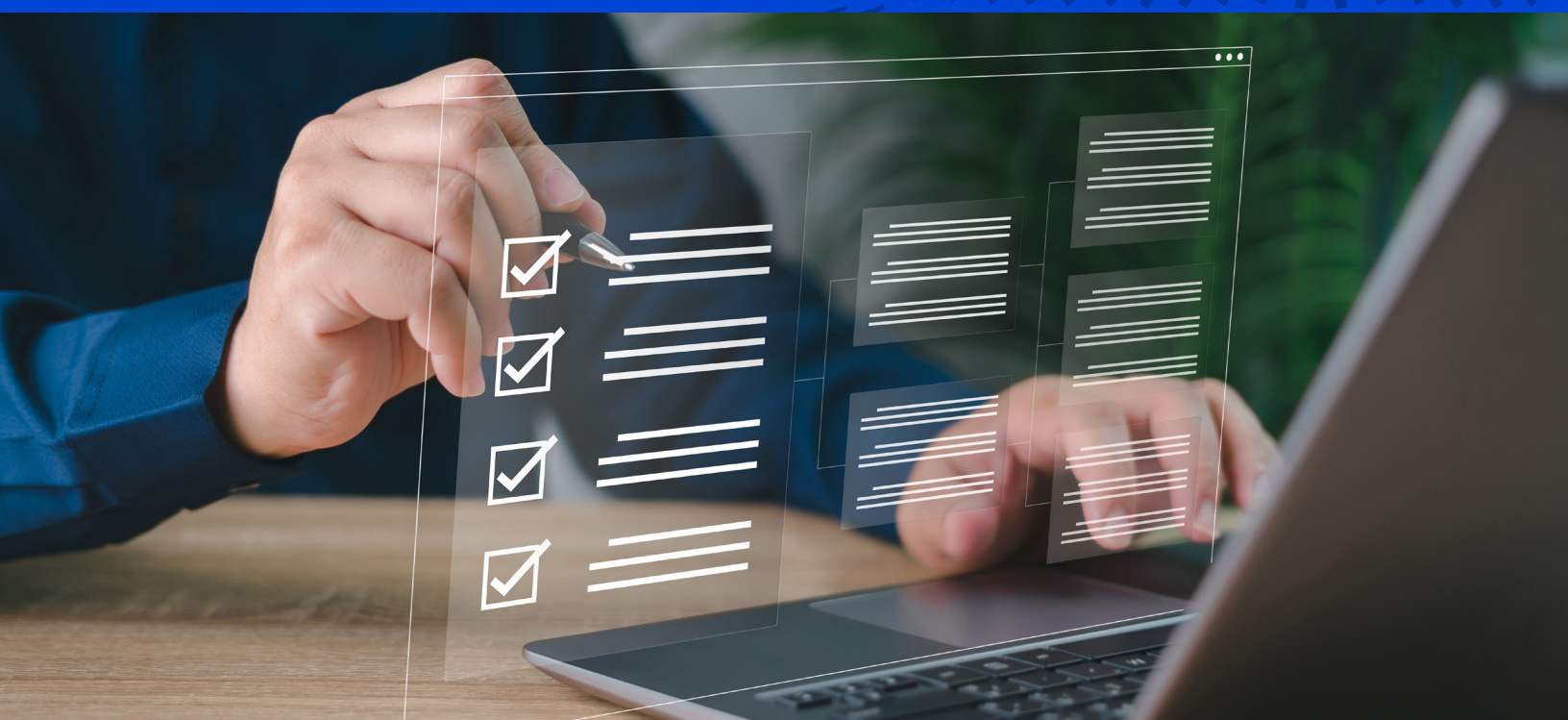
Are you over-securing,  
under-protecting, or both?

## Contractor access deserves a rethink

Contractors, partners, and third parties are essential to the operation of modern enterprises. But they are also among the highest-risk users in most environments, often working from unmanaged devices, across short engagements, and outside standard IT controls.

Many organizations still rely on VDI, VPN, or fragmented SSE tools to manage contractor access. While these approaches provide some protection, they often introduce unnecessary cost, operational friction, and security gaps, especially inside the browser, where most work now happens.

This checklist helps Security, EUC, and Infrastructure leaders quickly assess whether their current contractor access model is fit for today's browser-first, SaaS-driven work, and where browser-native Zero Trust can simplify and strengthen it.



## Self-assessment checklist

### Section 1 — Identity & access controls

- ☐ Do contractors routinely receive more access than required because granular, app-level controls are difficult to enforce?
- ☐ Do you rely on VPN access to connect contractors to internal web applications?
- ☐ Can you enforce identity-aware and context-aware policies consistently across SaaS and internal web apps?
- ☐ Can you easily segment access between contractors, partners, and employees without duplicating tooling or policies?

#### What this reveals:

VPN- and VDI-centric models often lead to over-trust and broad access, rather than least-privilege enforcement.

### Section 2 — Device trust & BYOD reality

- ☐ Can your current access model securely support unmanaged or BYOD contractor devices?
- ☐ Do contractors need to install agents or enroll devices to get access?
- ☐ Does your DLP strategy work consistently on unmanaged endpoints?
- ☐ Can you block copy/paste, screen capture, or downloads directly at the browser layer?

#### What this reveals:

Most traditional tools assume device control. Contractors rarely fit that assumption.

### Section 3 — Data loss prevention & GenAI controls

- ☐ Can you prevent contractors from pasting corporate data into GenAI tools?
- ☐ Can you stop uploads to unsanctioned SaaS applications?
- ☐ Can you restrict downloads from sensitive internal sites?
- ☐ Is screen capture controllable today for contractor workflows?

#### What this reveals:

If controls stop at the network or session level, data can still leak inside the browser.

### Section 4 — Compliance, logging & audit readiness

- ☐ Are browser activities logged clearly enough to satisfy compliance and audit teams?
- ☐ Can browser access events be exported to your SIEM?
- ☐ Do audits regularly surface gaps or manual workarounds related to contractor access?
- ☐ Do you lack visibility into what contractors actually do inside web apps?

#### What this reveals:

Limited browser visibility makes audits slower, riskier, and more manual than necessary.

### Section 5 — Cost, complexity & operations

- ☐ Do you provision VDI desktops solely for contractor isolation?
- ☐ Are you maintaining more VDI capacity than required for short-term or external users?
- ☐ Does onboarding or offboarding contractors take longer than it should?
- ☐ Are multiple teams involved in provisioning a single contractor?
- ☐ Do your SSE tools still leave gaps at the browser layer, requiring compensating controls?

#### What this reveals:

Operational overhead is often the hidden cost of legacy contractor access models.

## Interpreting your results

### Section 1 — Identity & access controls

#### 6 or more boxes checked

Your contractor access model is likely over-reliant on VDI, VPN, and manual governance. You are a strong candidate for a browser-native Zero Trust solution using Chrome Enterprise within the Citrix platform.

#### 4–6 boxes checked

You have partial coverage, but browser-layer DLP and Zero Trust controls could significantly reduce risk and operational friction.

#### 0–3 boxes checked

You have a relatively modern approach today, but browser-native controls can improve consistency, auditability, and future readiness, especially as GenAI usage grows.

## What a modern contractor access model looks like

A right-fit, browser-first contractor access model typically includes:

- Secure access from any contractor device
- No VPN and no device enrollment
- Browser-native DLP (copy/paste, upload/download, screen share)
- Consistent Zero Trust access across SaaS and internal web apps
- Exportable logs for compliance and audit
- VDI is reserved only for high-risk or regulated workflows
- Lower operational overhead for onboarding and offboarding

This approach aligns with your broader security, applying the right access method to the right workload.

## Next steps

If this checklist surfaced gaps or friction in how contractors access web and SaaS applications, the next step is to assess how browser-native Zero Trust can simplify your model without weakening security.

Start by taking the [Secure Access Readiness Check\[2.1\]](#) to quantify risk, cost, and complexity across your environment. Then learn how [Citrix Secure Access with Chrome Enterprise](#) enables secure, agentless contractor access directly inside the browser, without expanding VDI or VPN exposure.



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

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

© 2025, Cloud Software Group, Inc. All rights reserved. Citrix and the Citrix logo are trademarks or registered trademarks of Cloud Software Group, Inc. or its subsidiaries in the United States and/or other countries. All other product and company names and marks in this document are the property of their respective owners and mentioned for identification purposes only.