CONCEAL

HOW TO GUIDE

How to Transition from VPN/VDI/Proxy-Driven Access to Direct Zero Trust Access (DZTA) with Conceal

INTRODUCTION

For years, organizations have relied on VPNs, VDIs, and proxies as the standard for delivering secure remote access. These tools became the backbone of “Zero Trust” initiatives, allowing users to connect to internal resources from anywhere while enforcing authentication, authorization, and auditing.

But as workforces grew more distributed, applications moved to the cloud, and speed became a competitive necessity, this model began to show its age. What was once the de facto standard for secure access has become an obstacle.

This guide walks you through the transition from a VPN/VDI/Proxy-driven model to a Direct Zero Trust Access (DZTA) approach powered by the Conceal Browser-Native SSE Platform. It covers the evolution of the old model, the advantages of a modern approach, and a practical checklist to help your organization make the transition smoothly and confidently.

THE VPN/VDI/PROXY ERA: HOW WE GOT HERE

When the concept of Zero Trust Access (ZTA) emerged, traditional corporate networks were built around static perimeters. Employees worked in offices, and most applications ran in data centers. VPNs and VDIs were introduced to let remote users securely “tunnel” back into the corporate environment, while proxies monitored and filtered traffic to and from the internet.

Over time, this stack evolved into a typical architecture for secure access:

- VPNs created encrypted tunnels to connect remote users to private networks.
- VDIs gave users virtual desktops running in centralized environments, keeping sensitive data off personal devices.
- Proxies allowed traffic inspection, policy enforcement, and logging for compliance.

This approach offered tangible benefits:

- Tight access control through centralized policy enforcement.
- Auditability for compliance and incident response.
- Consistent user experience across regions and devices.
- Integration with enterprise authentication systems.

However, as businesses scaled and modernized, these same benefits became constraints.

Challenges with the Legacy Model

- Complex configurations require ongoing maintenance and specialized expertise.
- Latency and congestion slow down access, frustrating remote users.
- Single-threaded access points create bottlenecks and single points of failure.
- Broad network exposure grants users access to more than they need, increasing risk.
- Difficult scalability makes it cumbersome to support contractors, partners, and mobile users.
- High cost of ownership from datacenter dependencies, licenses, and support overhead.

In short, what worked well in a central-office world struggles in a distributed, cloud-first reality. Enter a better way.

THE FUTURE OF SECURE ACCESS: DIRECT ZERO TRUST ACCESS (DZTA)

The next evolution of secure connectivity is Direct Zero Trust Access (DZTA), an approach that eliminates the need for VPNs, VDIs, proxies, and backhauled traffic. Instead of routing traffic through centralized points, users connect directly to authorized applications using identity, context, and browser-based security controls.

The Conceal Approach

Conceal’s Browser-Native SSE Platform makes DZTA a reality by embedding Zero Trust principles and in-browser security directly into the browser itself. This eliminates layers of infrastructure while maintaining strong access control, visibility, and protection.

Advantages of Direct Zero Trust Access

- **No VPNs or proxies required:** Users connect directly to applications without backhauling traffic.
- **No VDI environments:** Local browsers become secure gateways without complex virtualization.
- **No traffic decryption:** Data remains private, yet secure controls still apply at the browser layer.
- **No certificate management:** Simplifies operations by removing complex PKI dependencies.
- **Simple configuration and deployment:** Users can be onboarded in minutes, not weeks.
- **Scales effortlessly:** Easily expand to contractors, partners, and global teams.
- **Stronger security posture:** Enforces granular access at the session and application level.
- **Lower cost and complexity:** Eliminates redundant infrastructure, licenses, and support costs.

THE STEP-BY-STEP TRANSITION TO DIRECT ZERO TRUST ACCESS

Transitioning to DZTA is a measured, strategic process. The goal is not to rip and replace overnight, but to methodically reduce dependency on VPNs, VDIs, and proxies while validating performance, user experience, and security outcomes at every step.

Step 1: Inventory Your Private Resources

Start by cataloging all private applications, servers, and services that currently require VPN, VDI, or proxy access. Document dependencies, usage patterns, and who needs access. This gives you a complete picture of the current environment and highlights the best candidates for your initial DZTA rollout.

Step 2: Audit Existing Zero Trust Tools

Review all tools currently providing access control and monitoring functions. This may include VPN clients, identity providers, proxies, and network access control solutions. Pay special attention to contract terms and renewal dates. Avoid committing to long-term renewals during the Conceal trial period. If needed, request 30- or 60-day extensions to maintain flexibility.

Step 3: Launch a Controlled Pilot with Conceal

Select a small, representative group of users, such as IT staff, developers, and a few trusted third-party contractors, to participate in the initial trial.

1. Enable these users within the Conceal platform.
2. Configure access to a limited number of private resources.
3. Run the pilot for approximately two weeks, closely monitoring performance, access reliability, and any support issues.
4. Gather feedback and ensure all policies are enforced as intended before expanding further.

Step 4: Expand to Additional Groups

Once the pilot proves stable, widen the rollout to include more users. Add remote workers, work-from-home employees, and international staff (if applicable). Continue to monitor metrics such as latency, access success rate, and security event logs.
At this stage, you'll start seeing firsthand how DZTA simplifies access without the delays and frustrations associated with VPN tunnels or VDI sessions.

Step 5: Begin Phased Decommissioning

After 30-60 days of successful testing, begin planning the retirement of legacy systems:

- Remove VPN agents from the endpoints of pilot users.
- Decommission unnecessary VDI resources and proxies.
- Update access policies to reflect the Conceal-managed model fully.

As legacy infrastructure is retired, operational costs drop, and your IT team gains time back to focus on higher-value initiatives.

Step 6: Reallocate Savings and Optimize

With VPN and VDI maintenance costs gone, budgets previously consumed by licenses, datacenter overhead, and helpdesk tickets can be reallocated. Many organizations reinvest these savings into new security initiatives, automation tools, or additional staff to strengthen their overall posture.

THE OUTCOME: A SIMPLER, STRONGER, SMARTER ACCESS MODEL

- Faster, more reliable application access.
- Stronger security aligned to Zero Trust principles.
- Lower operational complexity and total cost of ownership.
- Increased visibility and control across all user sessions.

With Conceal's Direct Zero Trust Access, your browser becomes your secure workspace. You can protect every user, every session, and every click without VPNs, proxies, or complicated configurations standing in the way.

CONCLUSION

The VPN/VDI/Proxy era was built for a world that no longer exists. Today's organizations need speed, scalability, and seamless security. Conceal's Browser-Native SSE Platform enables that shift by turning your browser into a secure, intelligent access layer that connects users directly to the resources they need safely, quickly, and efficiently.

Zero Trust. Line Speed. No Compromise.

That's the Conceal way to Direct Zero Trust Access.

About Conceal

Conceal delivers Direct Zero Trust Access (DZTA) through its Browser-Native SSE Platform, enabling organizations to consolidate connectivity and security into a single, unified solution. By eliminating VPNs, proxies, and complex configurations, Conceal provides real-time threat prevention, context-aware access controls, and complete visibility directly in the browser. The result is faster, simpler, and more secure access for every user, session, and click. Learn how Conceal delivers Zero Trust at line speed at www.conceal.io