Return-to-Office Blueprint: Modernizing the Workplace with Zero Trust

WHITEPAPER

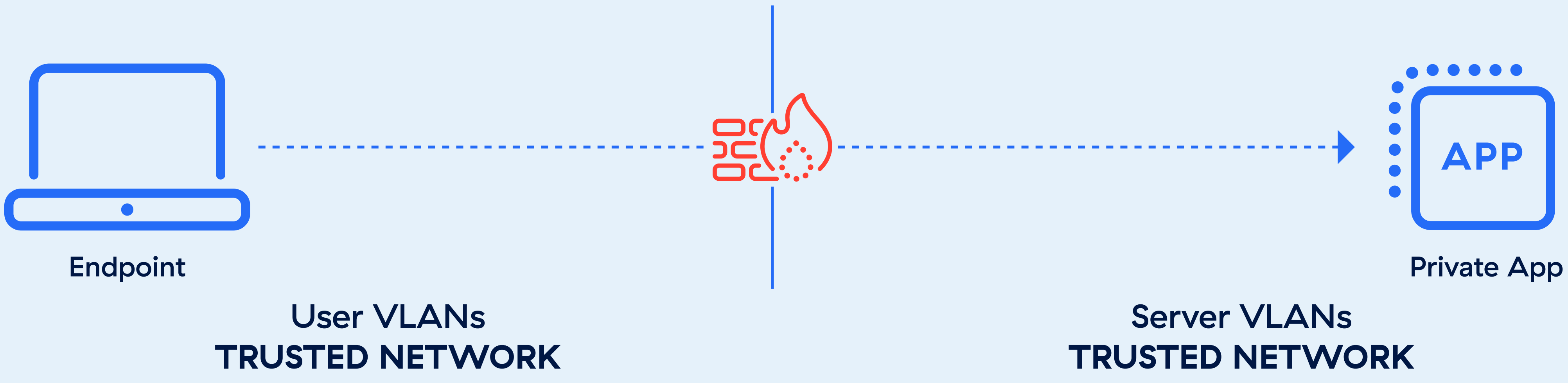
Returning to the office is not a return to the past. Employees may be returning to offices, but applications and data are not. Years of remote and hybrid work have fostered employees' reliance on and familiarity with cloud-based applications. Employees returning to the office expect the same—if not greater— IT reliability and responsiveness. Returning to "the way we've always done it" will not deliver on that expectation.

The migration of applications and data to the cloud requires a new look at how to deliver on premise security without impacting productivity. Zero trust, initially embraced to enable secure remote work, holds the same benefits for on-premises staff and should be viewed as a key enabler of the modern workplace.

Traditional Office Security: Trust in the Walls

Corporate networks were historically designed like fortresses, where trust was assumed for any user or device operating within the physical office walls—–inside the security "perimeter." This model worked when office systems were static, and everyone plugged into the same infrastructure.

In the traditional perimeter-based network security model, connecting to the agency office put the workstation device on the trusted network:



In the traditional model, connecting to the network implied access to all applications, resources, and data available on that network. To help mitigate the concerns of an unauthorized user or device connecting to the trusted network, you might implement a tool like Network Access Control (NAC) to control admission to the network – for example, don't let an untrusted device connect unless it has a certificate issued by the agency PKI.

This is a good step, but it leaves a lot to be desired from a segmentation and least privilege access security model, as the Trusted Network approach provides:

- Broad, Unrestricted Access
- Limited, Granular Controls
- Internal Network Vulnerabilities

These attributes of a trusted network approach—the assumption of broad access privileges, limited segmentation, and the inherent discoverability of internal networks—no longer align with the realities of today's advanced threat landscape. In a world of increasingly sophisticated cyberattacks, insider threats, and the proliferation of remote access tools, perimeter-based security models fail to address modern vulnerabilities. Attackers exploit the inadequacies of legacy architectures by bypassing weak segmentation controls and gaining lateral movement once inside the network, often using legitimate credentials to avoid detection. This reality necessitates a paradigm shift in how organizations approach security, transitioning from a 'trust by default' network to one that operates on zero trust principles: verifying and validating every access attempt dynamically, across all users, devices, and applications.

Instead, organizations need an approach that:

- Narrows access scope with granular app specific connections
- Introduces dynamic policy enforcement based on identity and device posture
- Enables ongoing assessment with continuous, per-access evaluation

This is not a future-looking architecture. It is available now with the zero trust network architecture (ZTNA) that was built to support remote work.

Zero Trust Enabled Workplace

As employees began working from everywhere, applications shifted to the cloud, and traditional assumptions about trust fell apart. The approach of zero trust that replaces "assume trust" with "always verify" became the most effective option to provide users the access they needed.

In the context of returning to the office, zero trust takes on new urgency. In recent years, the majority of applications and IT services have moved to the cloud, driving productivity gains and operational efficiencies. Reverting to outdated, pre-cloud, perimeter-based practices is counterproductive and incompatible with the modern workplace.

Zero trust is more than a security enhancement—it's a strategic opportunity to reimagine and future-proof the modern office. A zero trust approach unlocks agility, scalability, and cost savings for organizations. Whether setting up a new branch, building temporary collaboration hubs, or managing hybrid teams, zero trust eliminates the need for expensive network installations like MPLS or telco-managed solutions. It also reduces unnecessary dependence on intricate on-premises security infrastructure.

Most importantly, zero trust ensures relevance. As tools and workflows continue to evolve, organizations with a zero trust foundation can seamlessly integrate new technologies without being held back by outdated network configurations. They can free themselves from firewalls and other legacy appliances forever and future-proof their security strategy.

Users are back in office but your apps are not

Today, most work happens via cloud-based applications, even for employees sitting in a company's headquarters. The office is no longer the hub for all things IT. In truth, modern office workers are no different from remote employees in how they access resources.

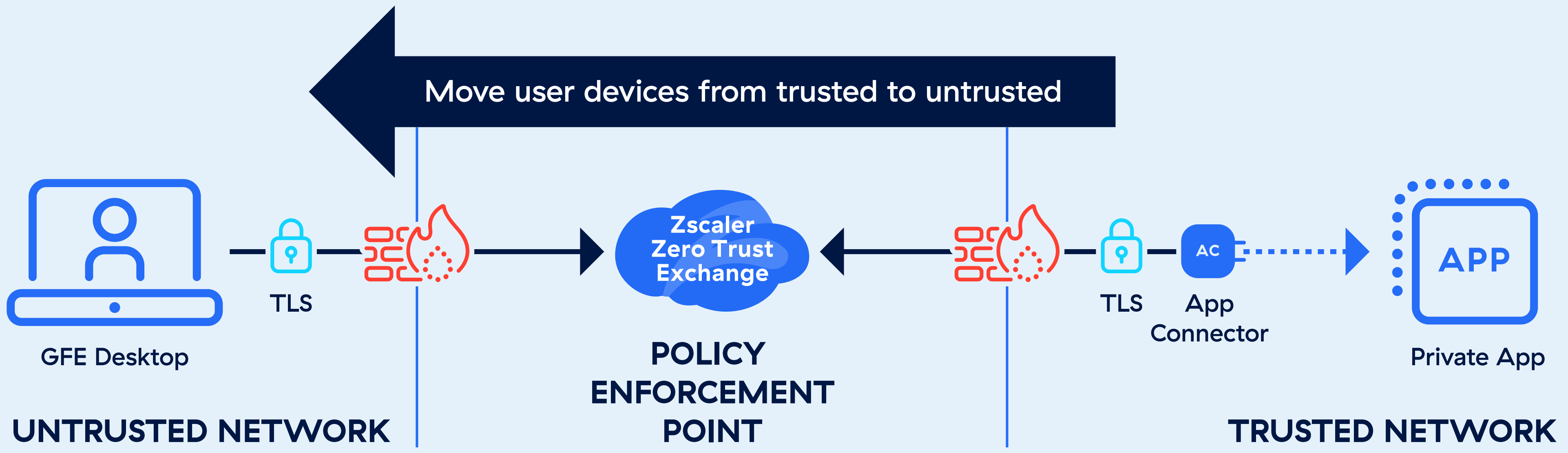
This fundamental shift has introduced several challenges:

- **Offices as Connectivity Bottlenecks:** Users returning to the office often backhaul cloud-bound traffic through the corporate network, creating unnecessary latency and incidents.
- **Diminished User Experience:** Employees may notice degraded application performance when working from the office compared to their remote setups. The issue isn't always the network—it could be anything from slow DNS resolution to poorly optimized Wi-Fi. But without visibility, pinpointing the root cause is a guessing game for IT.
- **Disjointed Monitoring Tools:** Legacy monitoring systems often focus on network availability instead of actual user experience metrics like application performance, latency, or endpoint health.

Rethinking Office Networks

Imagine a "café-style" internet model, where employees connect to the internet just as they would from home. While this outlook may be a radical shift, the logistics to make it happen are already available with zero trust network architecture.

In this scenario, there is no presumption of trust by connecting to the network. As a result, the user workstations are no longer considered trusted but now are protected the exact same way as a user working from home, using the same access policies.



Ultimately, coming into an agency office and connecting to the network shouldn't provide users with any more application or resource access than they would have when working over their home ISP. The network should be transport-only without any presumptive privilege.

Access and authorization is based on identity, device, and the application (not IP address) being accessed. A policy enforcement point, not network firewall ACLs, arbitrates every access decision and makes a need-to-know access decision based on access policies on which applications which users should access, from what devices.

This shift in architecture requires a shift in thinking.

1. **Extend Access Policies to On-Prem Users:** Access policy follows the user, not the network they are connected to.

2. **Move from Network Access to Resource Access:** With zero trust, users jump straight to applications through policy-based, identity-driven connections. This eliminates the need to grant broad access to the network itself.

3. **Treat the Office Network Like the Internet:** Your office Wi-Fi becomes “cafe-style internet” that simply connects users to the Zero Trust Exchange, where security policies take over. No inbound traffic. No implicit trust.

4. **Continuous Trust Validation:** Zero trust evaluates each access request dynamically, monitoring device posture, context, and risk signals.

The beauty of zero trust is its ability to deliver consistency. Employees don’t need to worry about whether they’re “on-prem” or “remote.” They are accessing applications the same way no matter where they are working. This unified experience not only ensures users remain productive it also simplifies IT administration.

Improved Visibility

A robust zero trust framework ensures seamless productivity while removing the risks posed by implicit trust and outdated infrastructure. Visibility emerges as a critical capability—on par with identity, device posture, and application control—to optimize performance and resolve issues swiftly. Visibility enables IT teams to optimize application delivery directly to users as well as reduce downtime and troubleshoot faster by narrowing root causes. Visibility from the endpoint all the way to the destination provides quick resolutions as admins can see if the problem is local to the user, the transport, or the cloud destination itself.

Consider these scenarios when returning to shared offices:

- **The Office Wi-Fi Dilemma:** An employee returning to the office connects their laptop to the corporate Wi-Fi. Suddenly, they experience high latency while using Microsoft Teams, an application that worked perfectly fine at home over a simple broadband connection. Is it a Wi-Fi coverage issue? A DNS delay? A problem with the Teams server itself?

- **SaaS Latency Over Corporate Backhaul:** A user tries to access a SaaS-based CRM like Salesforce from their desk. Cloud traffic is forced through the corporate network, introducing latency due to the backhaul path.

- **Visibility Gaps for Hybrid Workforces:** A global organization grapples with consistent visibility into device health as well as SaaS and ISP performance for both remote and on-premises employees, leading to frequent trouble tickets that consume valuable IT cycles.

A key piece of achieving the Zero Trust Office is ensuring digital experience monitoring as part of the overall zero trust architecture.

Why Zscaler for the Zero Trust Office?

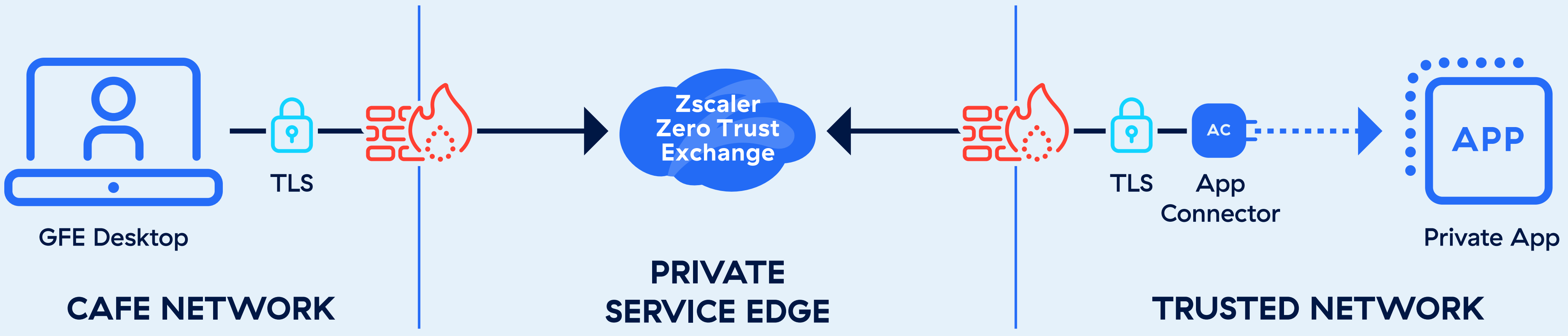
Zscaler is already a proven partner for government organizations navigating modernization efforts. As the industry's leading Cloud Security Service Provider, Zscaler is trusted by 14 of 15 cabinet-level agencies including DHS, DOJ, and GSA, to secure networks, simplify operations, and deliver cost savings. We are securing millions of users across hundreds of institutions at all levels of government.

Zscaler for Users comprises three areas of functionality to reduce risk, improve productivity, and lower cost and complexity.

- **Secure Internet and SaaS access (ZIA)** — Your users' access point to the internet and all applications, protecting against advanced threats and data loss

- **Secure Private App access (ZPA)** — Ensures users are connected via the local Private Service Edge, brokering the data connection to a private application through the agency network without going out to the Internet and back.

- **Digital User Experience (ZDX)** — Provides critical visibility into users' digital experiences — providing metrics from the end point all the way to the SaaS application — ensuring operational excellence in and out of the office.



Workplace Modernization Enabled by Zero Trust

As the workplace evolves, the definition of “office” becomes increasingly irrelevant. Whether users work from traditional office spaces, homes, or on the move, their experience must remain seamless and secure.

As employees return to the office, organizations have a unique opportunity to modernize their workplace infrastructure. Building on a zero trust foundation, ensures not only enhanced security but also scalability, agility, and long-term resilience. This is the vision of the fully realized Zero Trust Office——one where productivity thrives.

The Zero Trust Office is readily achievable today. By applying the same principles used for telework to in-office operations, organizations can significantly reduce risk, improve user experience, and create a future-ready security architecture.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**