Implementing Zero Trust for a Modern Work Experience

with Zscaler and Microsoft

zscaler™

Created by Zscaler in collaboration with Microsoft

68% of cybersecurity professionals say their focus on remote work accelerated the priority of Zero Trust projects[1]

1. Cybersecurity Insiders, 2022 VPN Risk Report

The world has fundamentally changed in just the last few years. Today, employees and customers demand access anytime, anywhere, and from any device. Chief information officers (CIOs), chief information security officer (CISOs), and other Information Technology (IT) leaders must defend their organizations as attack surfaces expand and unknown threats proliferate while, at the same time, ensuring a user experience that is fast, reliable, and seamless.

For competitive businesses, cloud transformation provides potential for both limitless and revolutionary growth. As its multifaceted benefits come into clearer focus, enterprise companies with forward-thinking leaders are aggressively accelerating their use of more than 150 Software as a Service (SaaS) applications—like the Microsoft 365 suite—plus actively expanding private applications into the public cloud.

The rewards are truly significant. Human Resources can further recruit and retain the best talent in the industry. Operations can dramatically improve the end user experience for their employees and customers alike. As a bonus, the increased business agility provided by such a transformation allows companies to pivot more easily and remain productive even when unexpected events like national disasters or pandemics strike. But to securely and sustainably get here, the IT department must also transform their security architecture.

While the race is on to stay ahead of both hackers and competitors, IT leaders need to look backward to ensure that legacy network and security technologies as well as their associated critical business data are protected as well. A survey of cybersecurity professionals reveals that 68% say their focus on remote work accelerated the priority of Zero Trust projects. And 78% of organizations are concerned about ransomware attacks, but there remains a lack of visibility into user activity and devices.[1] With latency, limited global footprints, blind spots, and backhaul traffic, it is difficult to find and fix performance issues.

The baseline requirement for employees, partners, and customers to collaborate and thrive anytime, from anywhere, on any device—while still protecting users, business data, and applications—is Zero Trust. When natively built on top of a highly distributed, global cloud architecture, it reduces access hassles and keeps employees productive and safe. **Zscaler and Microsoft solutions are tightly integrated, providing our mutual customers with industry leading cloud-native Zero Trust security, while increasing user productivity and delivering an exceptional user experience.**

1. Cybersecurity Insiders, 2022 VPN Risk Report

zscaler™ Microsoft

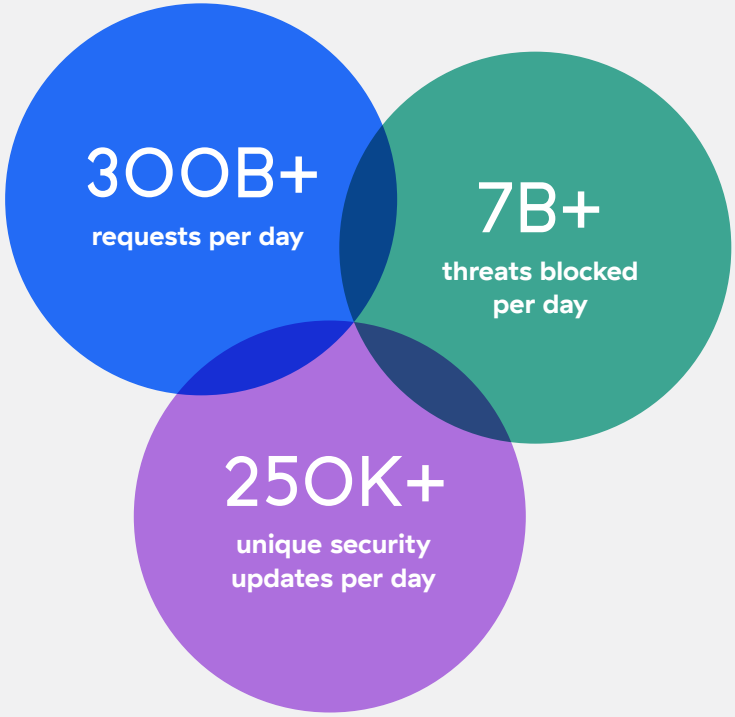
78% of organizations are concerned about ransomware attacks, but there remains a lack of visibility into user activity and devices[1]

Zscaler and Microsoft keep companies nimble, productive, and secure.

The Zscaler Zero Trust Exchange connects Microsoft customers directly to cloud resources

A Day in the Life of the Zscaler Zero Trust Exchange

Figure 1: Zscaler Zero Trust Exchange daily activity



zscaler™ Microsoft

Modern business demands an end-to-end, comprehensive security framework. The Zscaler Zero Trust Exchange is the industry leading[2] inline security cloud with over 150 points of presence (PoPs) around the world, peering with Microsoft globally. It acts as an intelligent switchboard to broker connections between users, devices, and applications wherever they reside. This brings security closer to the user for fast access and a positive digital experience without putting them on the corporate network. It reduces the security risks, cost, and complexity associated with perimeter-based security solutions that extend the network, expand the attack surface, increase the risk of lateral threat movement, and fail to prevent data loss.

The integration of these two complementary services solves both the bottom-up and top-down pressures CIOs, CISOs, and other IT professionals are feeling. Employees want to stay productive with instantaneous and seamless connections to SaaS applications like Microsoft 365, private applications, the rest of the internet, and internally managed applications. At the same time, executives and company boards are demanding the highest levels of security, a positive end user experience, and deeper insights into a borderless service and access topology.

2. Gartner: Magic Quadrant for Security Service Edge (SSE), April 10, 2023

By replacing legacy hub and spoke networks and security products (e.g. virtual private networks (VPNs) and firewalls) with direct user–to–application and application–to–application connections, Zscaler keeps Microsoft users' enterprise resources off the network and invisible to threat actors.

Three core services help Microsoft customers safely empower their workforces:

Zscaler Private Access (ZPA) makes clunky VPNs obsolete by connecting users directly to private applications, bypassing networks altogether to keep precious enterprise resources invisible to threats and minimize the attack surface.

Zscaler Internet Access (ZIA) connects end users directly to the internet and to their SaaS applications like Microsoft 365, reducing the cost and complexity of traditional network and security products.

Zscaler Digital Experience (ZDX) is a multi–tenant cloud–based monitoring platform that probes, benchmarks, and optimizes digital experiences for every user across the organization.

With this trio of offerings, Microsoft users can safely and seamlessly access the full suite of Microsoft productivity apps like Microsoft 365, along with everything else Microsoft Azure and the internet have to offer.

Microsoft and Zscaler work together to optimize user experiences, centralize enterprise visibility, and keep organizations' applications and assets safe with a Zero Trust security architecture that scales. Direct connections between your end users and their SaaS and private applications means no frustrating VPN headaches, no extended attack surface, and no opportunity for lateral threat movement.

"We want to get rid of VPNs. ZPA with Azure AD will make it possible for employees to **access all internal applications from anywhere.**"

Jason Truong
VP, Network & Security Engineering & Operations
Humana

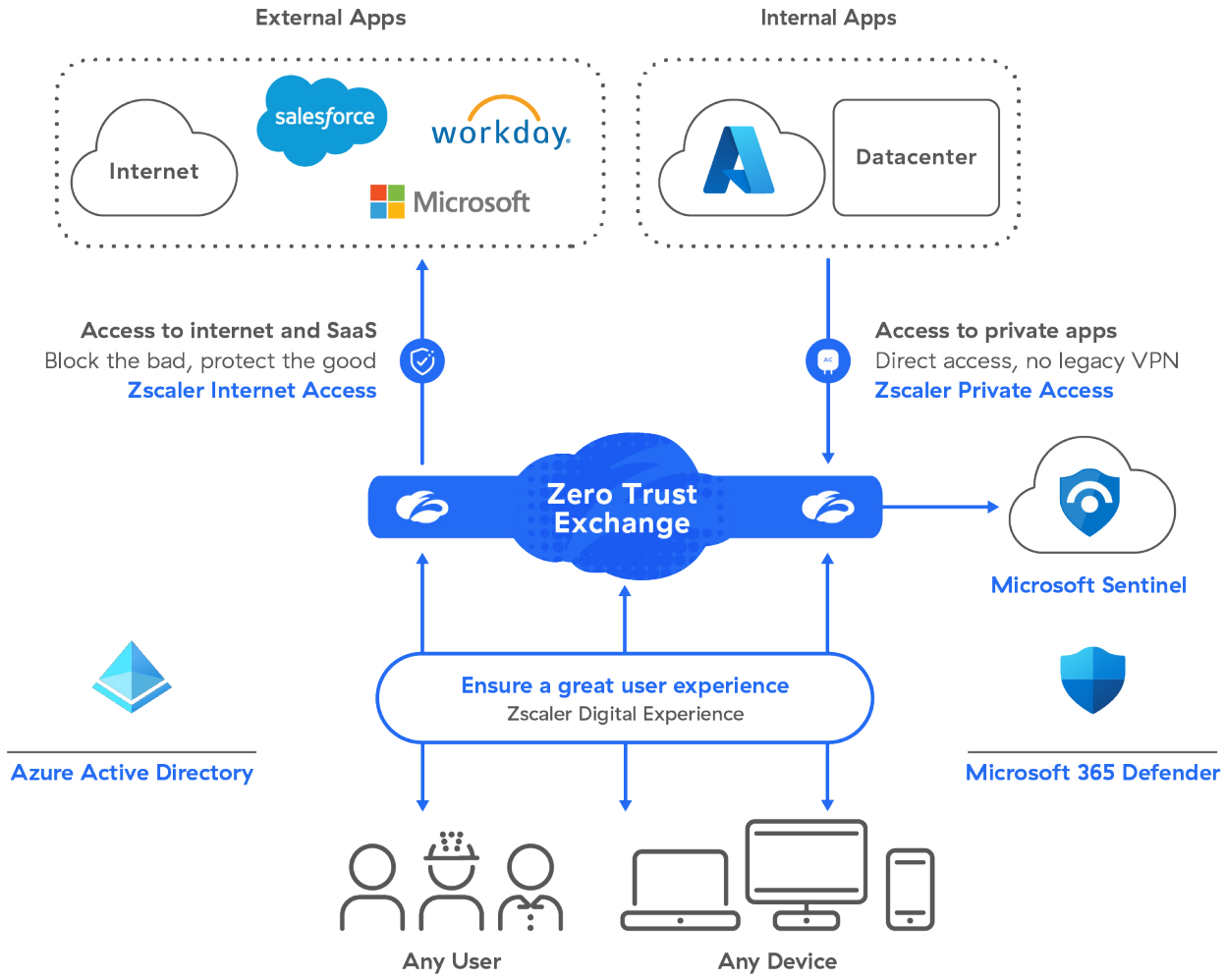


Figure 2: Zscaler and Microsoft provide Zero Trust security to SaaS, internet, and private applications.

A Zero Trust framework that seamlessly protects business data.

Secure and scale with a comprehensive, cloud-native security solution

The anytime, anywhere, any device modern workplace has been a boon for employees everywhere. With remote access, they can work from home, the office, or while on the go. For CISOs and CIOs, however, this has dramatically increased the attack surface area they must now protect from security breaches, data leaks, and lateral threat movement. Every day, new unvetted endpoints are added to networks.

A Zero Trust security posture, where each access request is evaluated, is critical. Together, Microsoft and the Zscaler Zero Trust Exchange provide secure, direct communications between your workforce and the applications and assets they need. They provide reliable protection from external threats such as phishing and ransomware, as well as more subtle internal threats like common vulnerabilities and exposures (CVEs).

When an employee attempts to sign-in to a service running on Microsoft Azure, or tries to add a file to a company folder, the Zscaler Zero Trust Exchange will first verify the user and their device. It then investigates any content, evaluates other contextual risk factors like location and behavior, determines the final destination, and then allows or denies access according to business policies. All of this is done behind the scenes, without negatively impacting the user experience.

With increased security, companies can provide additional flexibility to their employees. A Zero Trust platform, powered by industry leading solutions from Zscaler and Microsoft, results in more productive employees who can directly access any content their jobs demand, and go anywhere the internet reaches, securely.

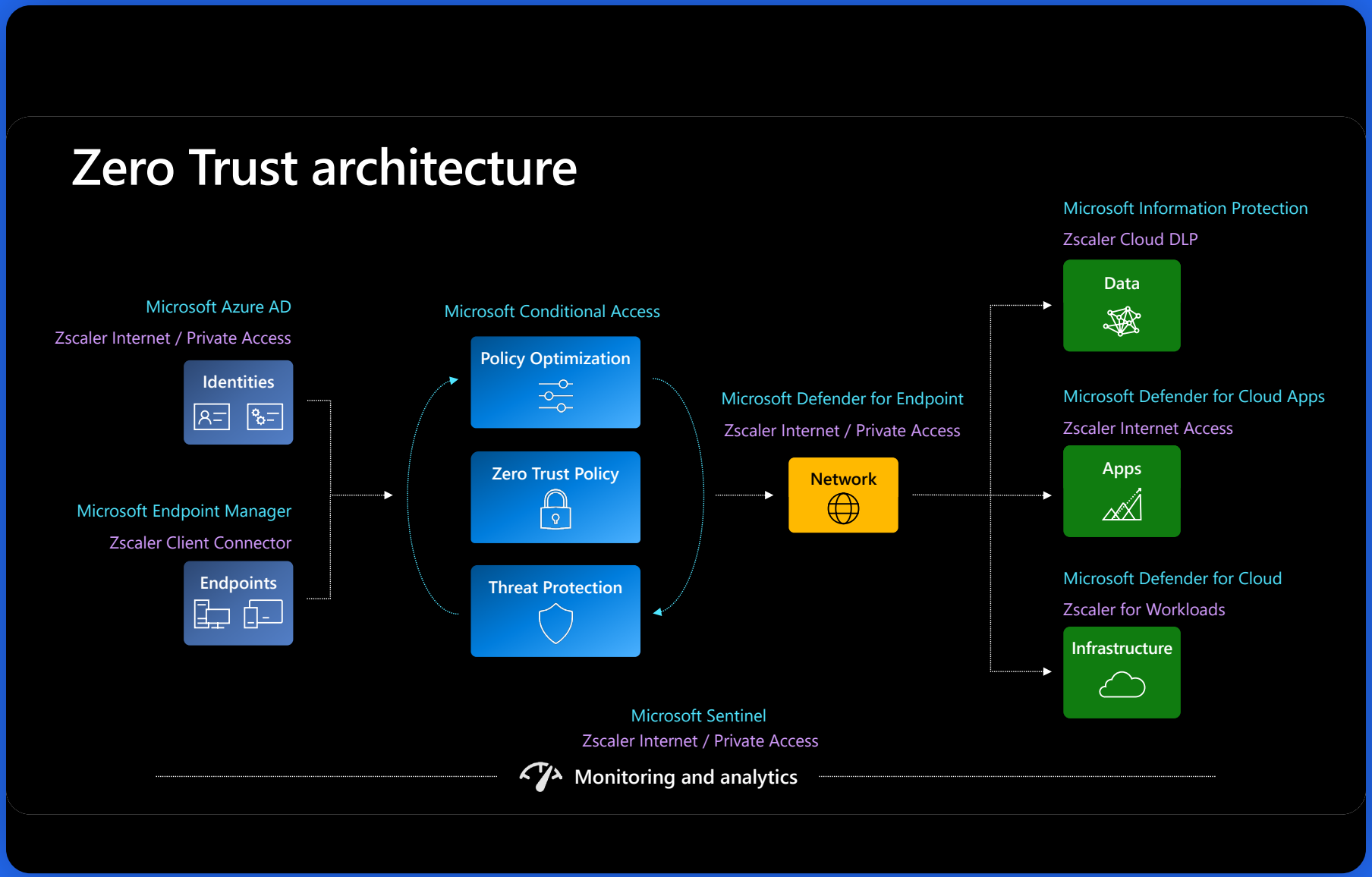


Figure 3: Zscaler and Microsoft integrations provide Zero Trust Security

Integrated solutions secure and power the modern workforce.

Your workforce needs to access resources anytime, anywhere, and from any device

The COVID-19 pandemic is now mostly in the rearview mirror, but the structural shifts it brought to the global workforce are here to stay. The work-from-home movement has accelerated the adoption of SaaS applications, and hybrid footprints of on-premises data centers and private clouds with a SaaS-like approach.

Security solutions from Zscaler and Microsoft enable our customers in their Zero Trust journey. Our integrations benefit our mutual customers with tangible security enhancements and flexibility to meet their specific business needs. These integrations reduce business risk, increase productivity, and decrease costs as organizations embark on their digital transformation.

A few key integration examples include:

01

Zscaler integration with Microsoft Azure Active Directory delivers Zero Trust network access (ZTNA) protection across any environment. It enables organizations to confidently authenticate each user before authorizing connections to specific enterprise resources across modern and classic productivity applications—using legacy protocols as needed. Seamless and fast access to applications makes your employees more productive as they work from anywhere, using any device—all while providing the Zero Trust security your organization needs.

02

Paired with the Zscaler Cloud Data Loss Protection (DLP) service, Microsoft Information Protection lets you set automated labels that can be used to block highly sensitive files. This prevents data exfiltration and ensures compliance across all your employees, independent of the device. Meanwhile, your employees can continue to share key data and stay productive while working from anywhere.

03

If a user attempts to access a suspicious file online, it is sent to the ZIA Cloud Sandbox. There, Zero-Day Threats are handled safely by detonating suspicious files. It can then communicate with solutions like Microsoft Defender for Endpoint to generate alerts, trigger an investigation, pause ongoing process execution, and/or quarantine suspicious files on any endpoint device. An Indicator of Compromise is also generated to prevent future executions.

04

The Zscaler Zero Trust Exchange, in tandem with Microsoft Defender for Cloud enables customers to securely implement hybrid and multi-cloud environments. As a result, applications and workloads can securely communicate with each other across clouds and on-premises, and with other internet services.

05

The integration of Microsoft Defender for Cloud Apps with ZIA enables real-time streaming of log data into Defender, which uses the logs to discover applications and classify them as sanctioned, permitted, or unsanctioned. Administrators can then define security policies in Defender, which are enforced by ZIA globally.

06

The integration of ZIA with Microsoft Sentinel allows billions of threat logs and transactions to be quickly ingested. As a result, Sentinel has more data points, which enables better threat intelligence, visibility, and detection globally.

07

ZPA enables organizations to migrate on-prem applications to Microsoft Azure more quickly. By providing Zero Trust security before, during, and after migration, Zscaler enables organizations to avoid the time, cost, and complexity that comes with legacy VPN and firewall security products.

08

Zscaler also works in tandem with Microsoft Intune to provision and configure Zscaler Client Connector, which can be further extended via Windows Autopilot. Device posture checks by Microsoft Intune or Defender provide security to ensure that critical applications are only accessed by authorized users.

A user experience so good it's a competitive advantage.

Security shouldn't impede the best user experience possible

Employees across the enterprise appreciate the fast, reliable access to SaaS and private applications, cloud data stores, the internet, and other enterprise assets available when Zscaler and Microsoft replace frustrating, outdated VPN and firewall connections.

For CIOs, CISOs, and their teams, ZDX is a game changer. ZDX provides end-to-end visibility and troubleshooting of end-user performance issues for any user or application, regardless of location. ZDX also provides powerful inspection and diagnostic tools to pinpoint performance issues across each application, network, or device so companies can continually improve their employees' experience.

The ZDX Score provides an aggregated user experience performance metric tracked over time at the user, application, location, department, and organizational level. It incorporates a varied set of metrics from the end user device, network path, and SaaS/cloud application. It provides insight into the current state of the end user experience to enable more informed decisions. This empowers IT administrators to proactively troubleshoot and provide remediation as needed to deliver a positive experience for users across the organization.

Zscaler is part of the Microsoft 365 Networking Partner Program, ensuring that users accessing the world's most popular productivity suite are provided with a quick, optimized access experience. This includes minimal latency and faster file throughput all while allowing you to let go of legacy hub and spoke architectures and the cost and complexity associated with VPNs, firewalls, and other point products.
The addition of bandwidth controls, Transmission Control Protocol (TCP) window shaping, and direct peering further improve performance.

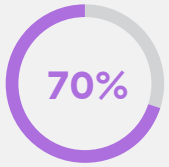
To recruit and retain the best talent in a competitive environment, companies must provide an exceptional experience for both their employees and their customers. This requires moving away from clunky legacy solutions that introduce latency and expand the attack surface. The deep integrations between Zscaler and Microsoft provide organizations with reliable, frictionless access and a competitive advantage as they seek to attract and retain the next generation of employees.

When CIOs and CISOs at the forefront are constructing an end-to-end security architecture, they appreciate the seamless integration of the Zscaler Zero Trust security platform—a leader in the Gartner Magic Quadrant for Security Service Edge (SSE)—with Microsoft's leading position in areas such as access management, analytics, security information and event management (SIEM), extended detection and response (XDR), and Endpoint Protection. Zscaler and Microsoft provide comprehensive security and a cloud-native, highly distributed architecture that keeps employees connected and nimble.

3. Gartner Identifies Three Factors Influencing Growth in Security Spending, October 13, 2022
4. Gartner: Magic Quadrant for Security Service Edge (SSE), April 10, 2023

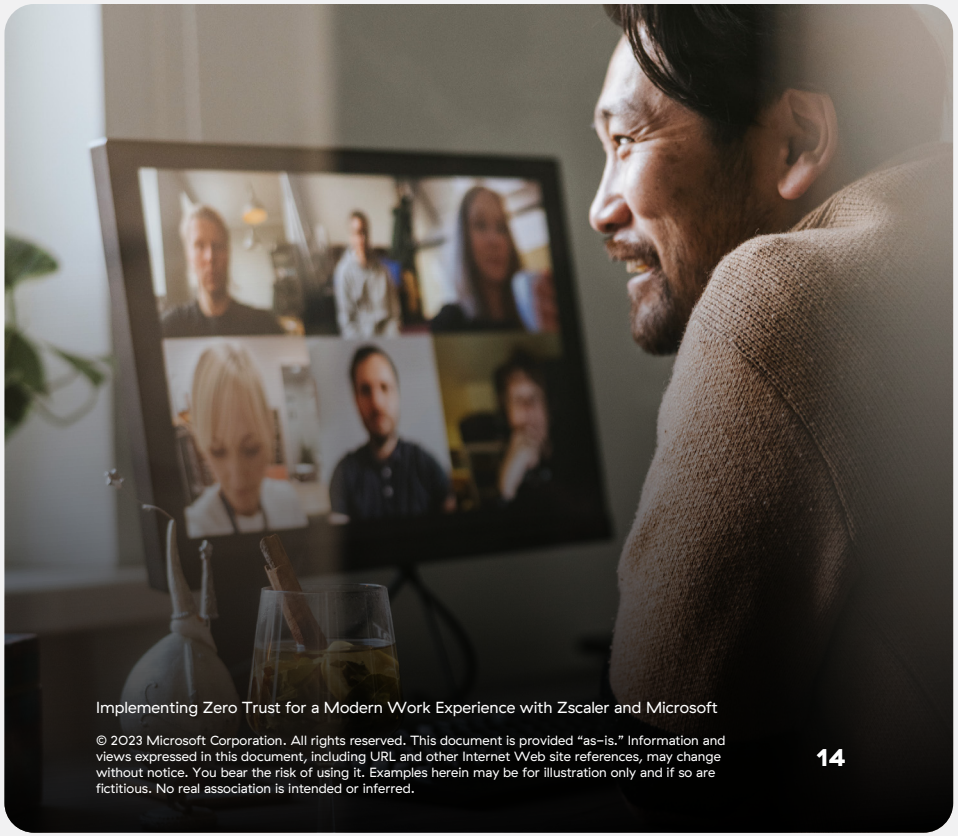
zscaler™ Microsoft

Good riddance, VPNs!



70% of **new remote access deployments will utilize ZTNA** rather than VPN services by 2025[3]

By 2025, 80% of organizations seeking to procure SSE-related security services will **purchase a consolidated SSE solution**[4]



Zscaler and Microsoft: **proven and integrated Zero Trust solutions**

As companies seek new ways to accelerate their digital transformation, enable remote bring your own device (BYOD) work, and shift company assets, infrastructure, and processes into the cloud, the need for comprehensive Zero Trust protection keeps multiplying. The prospect of trying to defend a cloud–first enterprise from external cyberattacks and internal security compromises may seem daunting.

Zscaler and Microsoft integrations can help you simplify your journey to a seamlessly secure work–from–anywhere environment, protecting enterprise assets while powering an optimized, reliable digital experience for all users. The Zscaler Zero Trust platform enables fast, direct, and secure access to public applications, private applications, the internet, and SaaS; protecting users, applications, and data without compromising speed or reliability.

With Zscaler and Microsoft technologies working in tandem, organizations can confidently embrace cloud–first services and hybrid workforces while obtaining integrated, comprehensive Zero Trust security that increases productivity and delivers an exceptional user experience.

zscaler™ Microsoft

Learn how you can accelerate your digital transformation with Zero Trust security:

Discover Zscaler Solutions →

Discover Microsoft Solutions →

Visit Zscaler at the Azure Marketplace →

Created by Zscaler in collaboration with Microsoft

Implementing Zero Trust for a Modern Work Experience with Zscaler and Microsoft