Solution Brief

Zscaler + Microsoft Deliver Zero Trust Security

Integrated comprehensive security that increases productivity and delivers an exceptional user experience

Organizations around the world are working to embrace the new normal, with employees working from anywhere, on any device, along with the continued migration of on-premises applications to the cloud. While generally considered a boon for employee satisfaction and app availability, it also presents significant new challenges for organizations that seek to protect their environments with networking and security products that were never designed for remote workers or the cloud.

Securing these demanding modern work environments doesn't have to come at the expense of your employees' happiness and productivity. Hybrid employees deserve quick, painless, and reliable connections to their resources—not desk-pounding and frustration. Organizations running legacy security products that rely on VPNs and firewalls face incomplete security, inconsistent user access, an expanded attack surface, and a poor user experience.

By replacing traditional networks and inbound/outbound security gateways with direct user-to-app and app-to-app connections, Zscaler keeps your enterprise resources off the internet and invisible to threats. Zscaler's core services help Microsoft customers safely empower their workforces:

- **Zscaler Private Access (ZPA)** makes problematic 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 via a zero trust network access (ZTNA) cloud architecture.
- **Zscaler Internet Access (ZIA)** connects end users directly to the Internet and SaaS apps like Microsoft 365, reducing the cost and complexity of traditional secure web gateway products.
- **Zscaler Digital Experience (ZDX)** is a multi-tenant cloud-based monitoring platform that probes, benchmarks, and measures digital experiences for every user within an organization.

Zscaler enables organizations to provide a secure and positive digital experience by delivering fast, reliable access to all SaaS and private apps, cloud data stores, the Internet, and other enterprise assets.

> "I'm thrilled to see some of the world's largest enterprises including Sandvik, Siemens, and GE use Zscaler and Microsoft to deliver fast and direct access to Office 365, as well as applications running on Azure."
>
> **Satya Nadella,** CEO of Microsoft

Zscaler and Microsoft

Zscaler and Microsoft solutions are tightly integrated, providing our mutual customers with modern, cloud native zero trust security while increasing user productivity and accessibility. With thousands of customers benefiting from our platform solutions, it's no surprise that Zscaler has been selected as the ISV Partner Winner of important Microsoft Awards such as Zero Trust Champion of the Year and Microsoft ISV Partner of the Year, and is a founding member of the Microsoft 365 Networking Partner Program and the Microsoft Intelligent Security Association.

The Zscaler Zero Trust Exchange is the world's largest 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 distributed architecture ensures that any communication can be sent directly to the Microsoft Network efficiently and securely, bringing security closer to the user for fast access and a positive digital experience. Zscaler's modern architecture eliminates the cost, complexity and performance challenges associated with legacy VPN and firewall security products.

Recent research from industry analyst Gartner confirms this requirement, stating that Zero Trust Network Access (ZTNA) is the fastest–growing segment in network security, forecast to grow 36% in 2022 and 31% in 2023, driven by the increased demand for zero trust protection for remote workers and organizations' reducing dependence on VPNs for secure access[1].

Zscaler's integration with Microsoft includes Azure Active Directory (AD), Microsoft Defender for Cloud Apps, Microsoft Defender for Endpoint, Intune, Azure Sentinel, Microsoft Information Protection, and more. Additionally, Zscaler enables organizations to accelerate their migration of applications and environments to Microsoft securely. Let's take a closer look at how Zscaler's key Microsoft integrations benefit our customers.

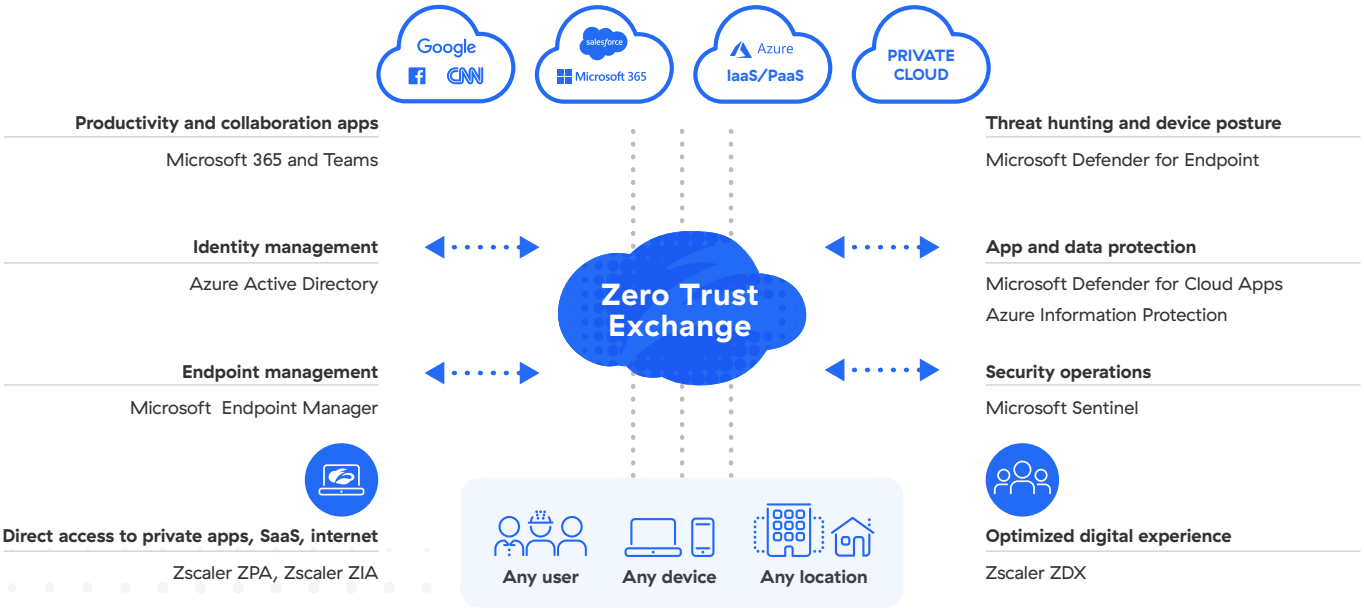

Figure 1: Zscaler and Microsoft enable the modern workforce with zero trust

[1]Gartner: Gartner Identifies Three Factors Influencing Growth in Security Spending, October 13, 2022

Protection for Resources and Endpoints

Least privileged access provides users with only the minimum level of access necessary to perform job-specific activities. It is a crucial element of information security that helps organizations protect their sensitive data by restricting unauthorized access and lateral movement to business applications and resources. The Zscaler Zero Trust Exchange takes this a step further by first establishing a user's identity and full context for the connection request, such as the user's device, their location, the application in question, and its content.

To help establish the user's identity, Zscaler integrates with Azure AD. This enables administrators to utilize Azure AD to control access to Zscaler and allows authorized users to automatically sign-in to Zscaler using single sign-on (SSO), multifactor authentication (MFA), and conditional access to applications. Working together, Zscaler and Azure AD deliver zero trust network access to internal apps including Oracle, SAP, and legacy-protocol workloads via Zscaler Private Access (ZPA). They also ensure that only authorized users have access to SaaS applications and the internet via Zscaler Internet Access (ZIA), enabling employees and partners to securely work from anywhere.

Protecting endpoints against threats, including zero day attacks is accomplished via integration of the Zscaler Cloud Sandbox with Microsoft Defender for Endpoint APIs, delivering Extended Detection and Response (XDR) visibility. Zscaler processes hundreds of billions of transactions per day, detecting, blocking, and signaling threats and zero day exploits. When the Zscaler Sandbox identifies a threat, it automatically signals Defender and requests the machine ID, file hash, and other data for the endpoints that have been exposed. Microsoft Defender for Endpoint then utilizes the new file signature to quickly detect, isolate, and remediate infected endpoints throughout the organization.

For the securing and managing of corporate and BYOD mobile devices, Zscaler integrates with Azure AD and Microsoft Intune to provide endpoint posture control enforcement. Microsoft Intune also automates the deployment and provisioning of Zscaler Client Connectors to endpoints and applies Intune posture policies. This integration also automates the assignment of mobile apps to users, app configuration, and the removal of enterprise data from mobile apps. User and group access to Zscaler resources are controlled within the Microsoft Intune console. To date, Zscaler has deployed over 36 million Client Connectors worldwide.

> "We want to get rid of VPNs. ZPA with Azure AD will make it possible for employees to access all internal apps from anywhere."
>
> **Jason Truong**
> VP, Network & Security Engineering & Operations, Humana

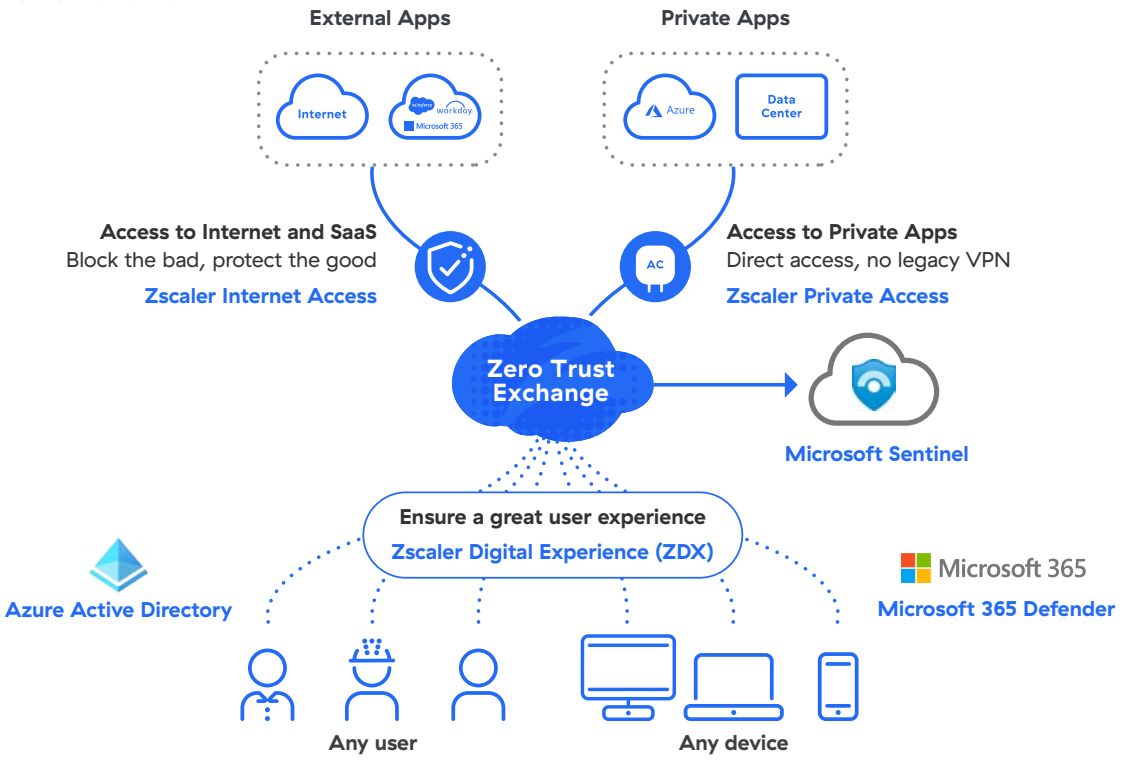

Figure 2: Zscaler and Microsoft provide zero trust security to SaaS, Internet, and private applications

Protection for Data and Apps

The Zscaler + Microsoft integration allows you to seamlessly secure data and applications in the cloud or wherever they reside. Zscaler Internet Access (ZIA) provides secure access to internet and SaaS applications, while Zscaler Private Access (ZPA) provides secure connectivity to private apps. ZIA includes Cloud Data Loss Prevention (DLP), Cloud Secure Web Gateway (SWG), Advanced Cloud Sandbox, and more. Integration with Microsoft Information Protection (MIP), which helps organizations discover, classify, label, and protect sensitive documents and emails to prevent inappropriate sharing, provides layered security that protects sensitive data.

Zscaler Cloud DLP provides inline policy enforcement based on data classification and labeling created by MIP. Zscaler's built–in file decoding capability detects AIP's labels, even for encrypted files, then takes appropriate action based on Zscaler's DLP policies to enforce data exfiltration controls and protect organizations from insider threats and compliance violations. Accordingly, if a document is classified as confidential by AIP, Zscaler can prevent it from being uploaded to unsanctioned web and SaaS applications, such as Google Drive or Dropbox.

Zscaler and Microsoft have also partnered to provide a closed-loop Cloud Access Security Broker (CASB) that discovers and controls access to cloud applications and discovers shadow IT across all users, regardless of location or connection. The integration of Microsoft Defender for Cloud Apps with ZIA provides both in-band and out-of-band CASB protection along with Zscaler Nanolog Streaming Service (NSS). Zscaler NSS streams real-time log data into Defender, which uses the logs to perform application discovery and classify them as sanctioned, permitted, or unsanctioned applications. Administrators can then define security policies in Defender, which are enforced inline through Zscaler Internet Access to block access to unsanctioned apps globally.

Protecting Infrastructure

Organizations with legacy security products face significant challenges when trying to aggregate the logs from multiple firewalls, routers, VPN concentrators, proxy servers, and other devices—often from multiple vendors with different management consoles and interfaces. Zscaler and Microsoft integrations enhance and simplify the identification, prioritization, and remediation of threats while proactively hunting them as well. For example, Azure Sentinel provides SIEM and SOAR capabilities, and integrates with Zscaler Internet Access (ZIA) and Zscaler Nanolog Streaming Service, which consolidates logs from all users into a central repository. This enables administrators to analyze transaction data by user, device, application, and location in real time.

Zscaler accelerates and streamlines this process by adding a ZIA connector to the Azure Sentinel console, which 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. This lets admins quickly view dashboards, create custom alerts, and improve investigation to protect users, data, and apps wherever they reside.

Fast, Secure Access to Azure, Microsoft 365, Teams and More

Organizations with legacy VPN and firewall solutions face challenges when remote users need to access SaaS and Internet applications. Network traffic must be backhauled to security products in the data center for user access and data inspection, resulting in network congestion, poor performance, unhappy users, and increased calls to the IT Help Desk.

The Zscaler Zero Trust Exchange is the world's largest inline security cloud with over 150 points of presence (PoPs) around the world, peering with Microsoft globally. Our platform solves the challenges associated with legacy security architectures, with Zscaler Internet Access (ZIA) enabling local breakouts for fast, direct access to Microsoft 365, eliminating reliance on VPNs and backhauling traffic to the data center.

In addition, Microsoft 365 traffic can be prioritized over other traffic (e.g. YouTube or general internet traffic) by using Zscaler Bandwidth Control. Zscaler also automatically whitelists Microsoft 365 traffic, as recommended by Microsoft. Plus, Zscaler fingerprints all Microsoft 365 applications and frequently updates them, eliminating the challenges caused by VPNs and firewalls that include tracking URL and IP address changes, which result in inconsistent access and delays in applying product updates. Zscaler is a founding member of the Microsoft 365 Networking Partner program with traffic from thousands of enterprise customers running through our Zero Trust Exchange every day.

Workforce satisfaction is critical, and Zscaler and Microsoft balance zero trust security with a positive, reliable experience for end users that also provides organizations a competitive advantage as they seek to attract and retain the next generation of employees. Zscaler ZDX, our digital experience monitoring solution, seamlessly integrates with Microsoft Teams through secure APIs to access granular user and application telemetry data within a single platform. This, in conjunction with networking, endpoint, and performance signals from other apps, allows ZDX to run powerful correlations and machine learning. The result? IT teams are able to quickly detect and resolve user connectivity issues so they can keep users happy and productive while reducing calls to the IT Help Desk.

Zero Trust Security for Cloud Workloads

Zscaler Workload Communications reimagines cloud connectivity by enabling zero trust for cloud workloads, delivering simple, secure access for workloads to the internet and private applications. Unlike legacy network solutions, Workload Communications provides a direct-to-Azure architecture using the proven Zscaler Zero Trust Exchange platform to verify trust based on identity and context, enabling secure workload-to-internet and workload-to-workload communications across multiple regions and Azure Availability Zones and workload-to-workload communications within an Azure environment.

Workload Communications eliminates the network attack surface by directly connecting workloads to the internet and to private applications using a full proxy architecture. This dramatically simplifies connectivity by eliminating routing, VPNs, transit gateways, transit hubs, and firewalls, while allowing for flexible forwarding and easy policy management by using the proven ZIA and ZPA policy framework.

> “We rolled out ZIA to our entire environment – over 200,000 devices. Using it with Microsoft 365 gives our users a better experience...”
>
> **Jason Truong,** VP, Network & Security Engineering & Operations, Humana

Our unique approach provides three key benefits to Azure users:

- Zero attack surface and data loss prevention: Take traffic off the corporate network by using a direct-to-cloud architecture and make applications in Azure environments invisible to cyberthreats, reducing the risk of data loss.
- Simplified cloud connectivity: Our zero trust architecture helps you avoid performance bottlenecks by connecting workloads to other applications directly, eliminating IP overlap issues and the need for route distributions.
- Superior application performance at scale: Zscaler is built on a truly distributed architecture where every communication that reaches our service edge is instantly processed for identity and context. Our peering relationship with the Microsoft Network ensures the shortest path between applications no matter where they are hosted, reducing latency and improving application performance.

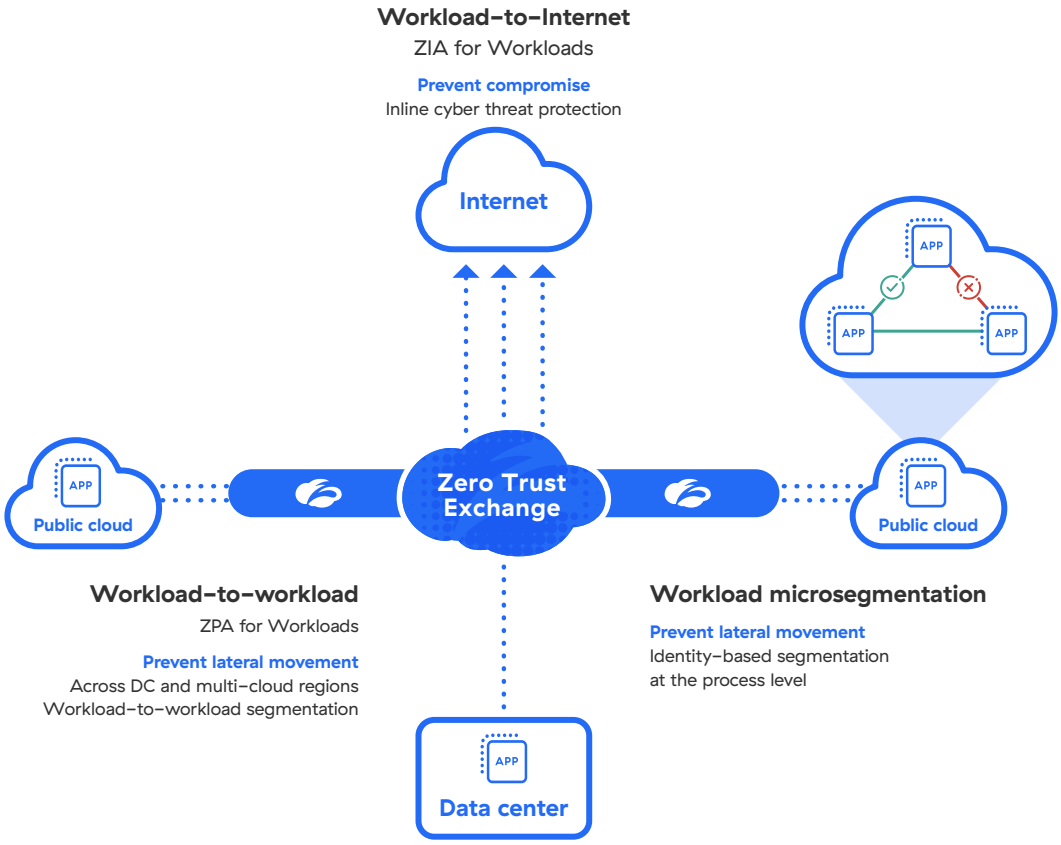

Figure 3: Zscaler provides zero trust security for Azure Workloads

Zscaler and Microsoft Power the Modern Workforce

Zscaler and Microsoft integrations enable organizations to seamlessly secure their work from anywhere environments, protecting enterprise assets while powering an optimized, reliable digital experience for all users. The Zscaler Zero Trust platform enables fast, secure access to business applications, private applications, internet, and SaaS, protecting business assets and data without compromising speed or reliability. Our joint customers also benefit from:

- The Zscaler Zero Trust Exchange is the world's largest inline security cloud with over 150 points of presence (PoPs) around the world, peering with Microsoft globally for fast performance
- Fast, direct connectivity between remote users and their SaaS and private applications, which eliminates the cost and complexity of legacy VPNs and firewalls, minimizes the attack surface, and prevents threats from moving laterally across the network
- A direct-to-Azure architecture that secures workload communications, simplifies connectivity, and improves performance
- Consistent zero trust security and efficient routing, which reduces latency and accelerates workload migration to Azure
- Optimized access to Microsoft 365 and Azure workloads keeps users happy and productive, while helping organizations attract and retain the next generation of employees
- Increased business agility for a competitive edge

Learn more about Zscaler zero trust security solutions and visit us at the Azure Marketplace today.

About Microsoft

Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

Microsoft

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange 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 SASE-based Zero Trust Exchange is the world's largest inline 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