zscaler™ | Microsoft

ZSCALER + MICROSOFT:

Comprehensive Multi-Domain Security with Inline Enforcement and Unified Visibility

Organizations are rapidly adopting cloud services, SaaS applications, AI copilots, and hybrid work models but many security architectures remain fragmented across identity, endpoint security, network controls, data protection, and security operations platforms. The rapid adoption of generative AI and autonomous workflows is also increasing pressure on organizations to secure users, data, and application interactions consistently across cloud and internet environments.

Together, Zscaler and Microsoft deliver end-to-end, cross-domain security by unifying Microsoft's identity, endpoint protection, analytics, and AI-driven security operations with Zscaler's inline policy enforcement for internet, SaaS, agentic and private application traffic via the Zscaler Zero Trust Exchange.

By integrating Microsoft security and productivity platforms with the Zscaler Zero Trust Exchange, organizations can enforce adaptive, risk-aware access policies, improve SOC visibility and threat investigations, protect sensitive data across SaaS and AI applications, simplify endpoint onboarding and compliance, improve digital experience for hybrid users, and extend Microsoft security investments with inline Zero Trust enforcement.

Customer Challenges

Modern enterprises face several security and operational challenges as environments become more distributed and the application ecosystem expands:

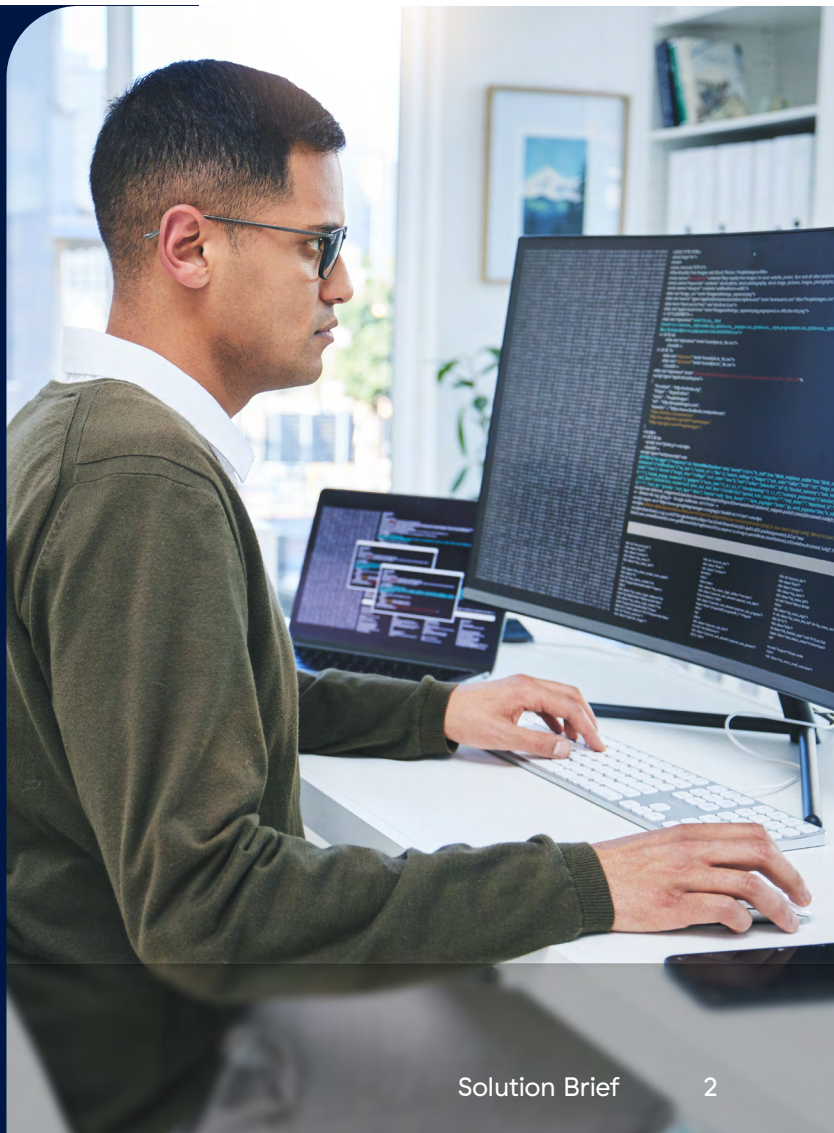
- **Access Without Continuous Enforcement:** Even with MFA and Conditional Access, risky users or compromised devices can still gain access if policy enforcement is not continuously enforced inline.
- **Endpoint and User Experience Complexity:** IT teams struggle to secure and troubleshoot distributed users across unmanaged networks, remote devices, and cloud applications.
- **Shadow IT and Unsanctioned AI Usage:** Employees increasingly use unauthorized SaaS and AI applications, creating new risks for sensitive data exposure and governance gaps.
- **Inconsistent Data Protection:** Organizations need to extend Microsoft Purview classifications and DLP policies consistently across internet, SaaS, and AI traffic flows.
- **Fragmented Visibility Across Security Domains:** Security telemetry is often distributed across identity, endpoint, web, SaaS, and cloud environments, making investigations slower and operationally complex.

Figure 1. Cross-domain security integrations between Zscaler and Microsoft.

Joint Vision: Multi-Layered End-to-End Security with Inline Enforcement

Zscaler and Microsoft share a common multi-domain Zero Trust vision centered on: continuous verification, least-privileged access, identity-aware policy enforcement, device posture validation, unified security analytics, AI-driven operations, and consistent data protection. Microsoft provides identity, endpoint security, SIEM/XDR analytics, compliance, and AI-driven security operations—serving as the intelligence platform for key security signals—while Zscaler serves as the intelligent, context-aware, inline Zero Trust enforcement layer, applying adaptive access controls across the internet, SaaS, and private applications in real time to govern user, application, and data interactions.

Together, both platforms create a layered end-to-end approach to multi-domain security to maximize security outcomes for join customers.



Zscaler & Microsoft Joint Integration Areas

Identity-Based Conditional User Access with Entra ID:

Zscaler integrates with Microsoft Entra ID for SAML-based Single Sign-on (SSO), MFA enforcement, conditional access, and SCIM provisioning. Entra ID authenticates users and evaluates access conditions while Zscaler applies inline enforcement across internet and private application traffic. Together, the solutions enable identity-aware application access, adaptive policies that change based on user and device risk, and automated user provisioning and deprovisioning.

Joint Value: Seamless, secure access built on identity, device posture, and continuous verification.

Secure Endpoint Deployment with Intune:

Microsoft Intune automatically deploys and configures the Zscaler Client Connector (ZCC) across managed devices. With Windows Autopilot, ZCC is deployed during device provisioning. ZPA also establishes a device-based (machine) tunnel as soon as the Windows device boots and has network connectivity—before any user signs in. The tunnel gives the device secure, Zero Trust access to required private resources enabling the device to complete pre-login tasks before a user logs in. Additionally, the Zscaler platform also consumes device compliance status from Entra ID and Intune to enforce posture-based access policies.

Joint Value: Simplified endpoint onboarding, stronger compliance enforcement, and operational efficiency.

Conditional Device Access with Microsoft Defender for Endpoint:

The Zscaler Adaptive Access Engine (AAE) integrates with Microsoft Defender for Endpoint (MDE) to ingest device risk scores, exposure levels, endpoint telemetry, and machine tags. These signals directly influence inline access decisions within ZIA and ZPA enabling organizations to block risky devices from sensitive apps, restrict internet access dynamically, reduce lateral movement risk, and trigger remediation workflows.

Joint Value: Real-time, risk-aware Zero Trust enforcement based on Microsoft endpoint intelligence.

End-to-End Digital Experience Monitoring with ZDX:

Zscaler Digital Experience (ZDX) collects performance signals from multiple places: the user's device (endpoint), the local network/Wi-Fi, the ISP path, and the application/service itself, and then uses Azure Data Explorer (ADX) as the backend analytics engine to store, analyze, and correlate all that telemetry at scale. ZDX also integrates with Microsoft Endpoint Analytics to ingest CPU utilization, memory performance, battery health, startup metrics giving IT teams a unified view of user experience across device, network, and application layers.

Joint Value: Faster root cause analysis and improved digital experience for hybrid users.

SaaS Governance and AI-Era Data Protection:

ZIA streams SaaS usage logs to Microsoft Defender for Cloud Apps (MDCA), which identifies Shadow IT, unsanctioned SaaS apps, and risky AI applications. MDCA risk decisions are then shared back to Zscaler for inline enforcement. In parallel, Zscaler Inline DLP recognizes Microsoft Purview sensitivity labels and extends Microsoft data protection policies across internet and SaaS traffic. This helps organizations block risky SaaS and AI apps and prevent sensitive data loss and protect Microsoft 365 data from AI-related leakage risks.

Joint Value: Consistent SaaS governance and data protection across modern AI-driven environments.

Unified SOC Operations with Microsoft Sentinel:

Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) stream DNS, URL, firewall, threat, and private application logs into Microsoft Sentinel using the Nanolog Streaming Service (NSS). Security teams can correlate Zscaler telemetry with identity, endpoint, email, and cloud signals to improve threat hunting, incident investigation, automated playbooks, and SOC visibility. The new Microsoft Sentinel Codeless Connector Framework further simplifies deployment through one-click onboarding from the Sentinel Content Hub.

Joint Value: Faster investigations, centralized visibility, and simplified SIEM operations.

Microsoft 365 Optimization & Protection with ZDX and Tenant Restrictions:

Zscaler integrates with Microsoft 365 to deliver end-to-end visibility, performance optimization, and data protection. ZDX monitors the full digital experience from the user's device to the Microsoft 365 app, surfacing insights and enabling one-click support ticket creation directly within Teams. Simultaneously, Zscaler's tenant restrictions prevent unauthorized access to external Microsoft tenants, blocking shadow IT and data leakage at the source.

Joint Value: Fast, secure, and compliant Microsoft 365 experiences.

Secure Azure Workloads with Zscaler Zero Trust Exchange:

Zscaler integrates with Microsoft Azure to extend Zero Trust across VMs, containers, and applications securing east-west and north-south traffic via Cloud Connectors, while App Connectors enable identity-based private access without inbound ports or VPN complexity. Azure Virtual WAN integration simplifies routing and centralizes policy enforcement.

Joint Value: Zero Trust security for every Azure workload, without the complexity of traditional networking.

Strategic Highlight: Advancing AI with Zero Trust

Figure 2: The Five Pillars of the Zscaler & Microsoft AI Alliance

Zscaler and Microsoft have made a deliberate, strategic commitment to ensure that AI transformation and Zero Trust security advance hand in hand as a unified vision. Through five defining milestones spanning AI agent identity, Copilot security, intelligent IT operations, and closed-loop threat response, Zscaler and Microsoft are turning the promise of secure AI transformation into enterprise reality.

The Five Pillars of the Zscaler & Microsoft AI Alliance:

1. **Non-Human Identity Governance:** As an early adoption partner for Microsoft's Entra Agent ID, Zscaler ensures AI agents are treated as first-class, non-human identities within the Zero Trust Exchange, bringing zero trust governance to AI agents.
2. **AI Productivity Without the Risk:** By combining inline prompt inspection with Microsoft Purview's data classification, Zscaler eliminates the risk of data leakage in Microsoft Copilot turning AI productivity into a secure experience.
3. **Gen AI-Powered IT Operations:** ZDX Copilot puts a generative AI assistant in the hands of IT teams to deliver natural language troubleshooting and real-time insights from over 500 data points across the Zscaler-Microsoft environment.
4. **Agentic Security at Scale:** Zscaler and Microsoft have deepened their Sentinel and Security Copilot integration to deliver closed-loop remediation, automatically revoking sessions and isolating threats without waiting for human intervention.
5. **The Innovation Never Stops:** Zscaler and Microsoft are continuously co-innovating across the full Microsoft Security stack and AI workload ecosystem to push the boundaries of secure AI, Zero Trust, and cloud transformation together.

With these innovation pillars, Zscaler and Microsoft are delivering on the transformative promise of an AI-first enterprise where AI governance, secure Copilot adoption, agentic security operations, and automated remediation are outcomes customers can count on today.

Conclusion

Together, Zscaler and Microsoft help enterprises move beyond implicit trust and fragmented point controls to a unified, cross-domain security strategy designed for modern users, modern applications, and modern threats in the age of AI.

By combining the strengths of both platforms, organizations can reduce cyber risk with adaptive access controls, secure SaaS and AI application usage, extend Microsoft policies inline, improve SOC visibility and efficiency, simplify IT operations and endpoint onboarding, and enhance the digital experience for distributed users.

The result is a scalable, AI-ready Zero Trust framework that securely connects users, devices, applications, and data anywhere, while strengthening security outcomes, improving operational efficiency, and delivering a better user experience.

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 160 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