

# Microsoft and Zscaler: Better Together

Advanced Integration

## Works with MS 365

**Certified Partner**  
First Security Partner qualified under Office 365 Networking Partner Program

## Identity Management

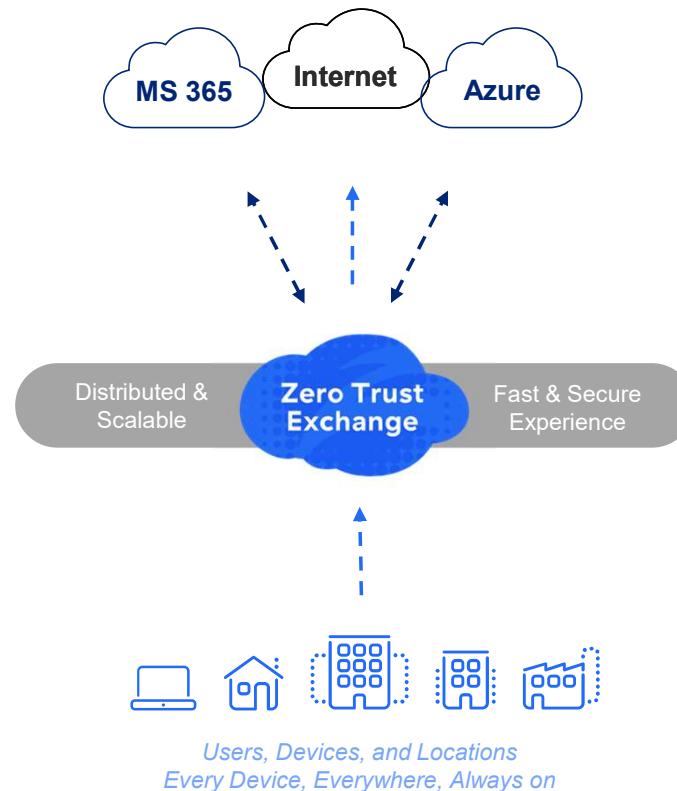
**Powerful Integrations**  
Azure Active Directory for user auth, provisioning & conditional access policies

## User Experience

**In-depth Monitoring**  
Monitor Office 365 traffic  
Monitor Microsoft Teams traffic

## Endpoint Management

**Deploy and Monitor**  
Microsoft Endpoint Manager (Intune) for easy Zscaler deployment and posture monitoring



## App & Data Protection

**Visibility, Labels & Control**  
Shadow IT control: MS Defender (Cloud Apps)  
Apply labels: MS Information Protection

## Private App Access

**Deliver Zero Trust**  
Zscaler Private Access & Microsoft Azure for Zero Trust app access

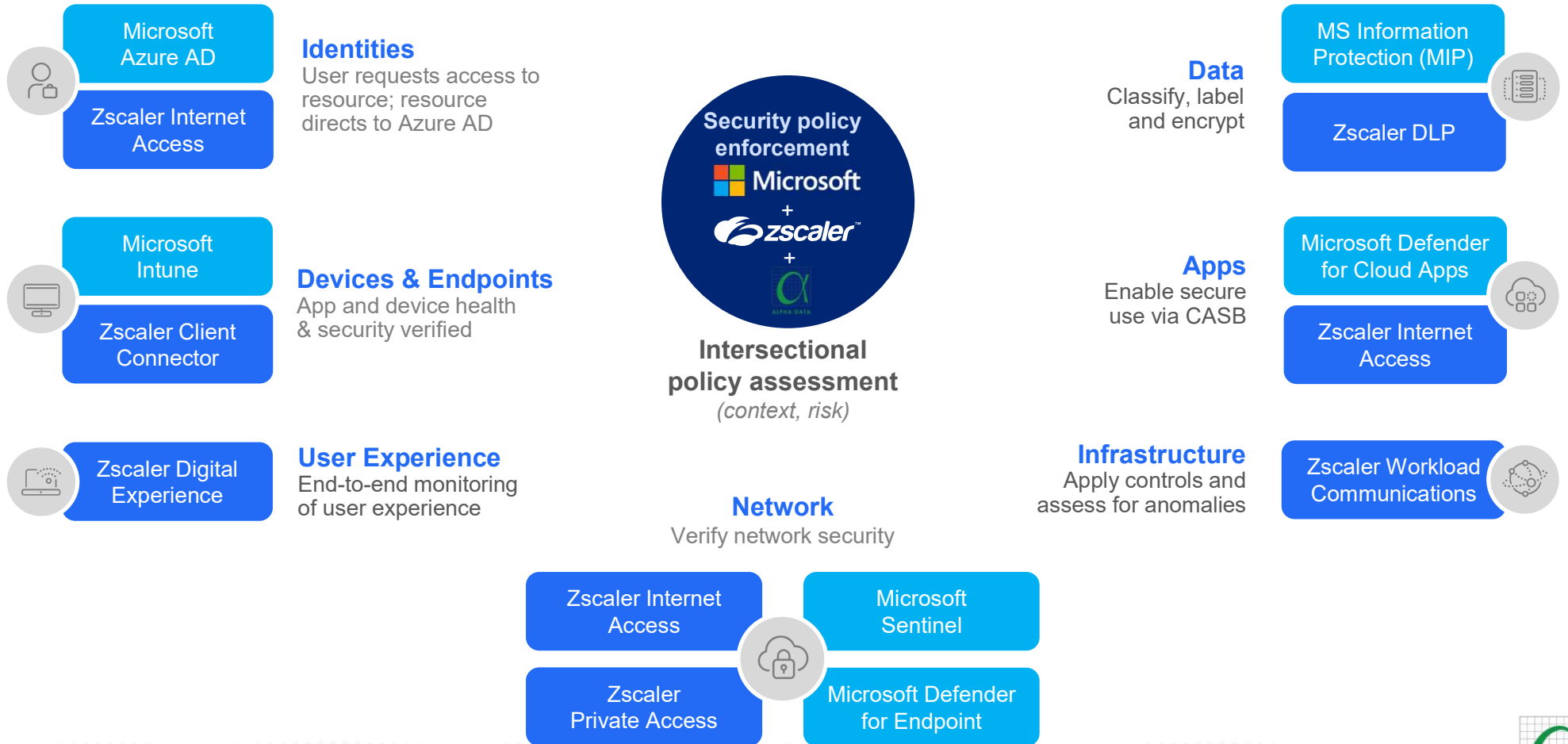
## Threat Prevention

**Protect against Advanced Threats**  
Stop unknown IOCs and enforce posture  
MS Defender (Endpoint) & ZS Adv. Sandbox

## Security Operations

**Simplify & streamline**  
Stream threat logs and leverage response playbooks with Azure Sentinel

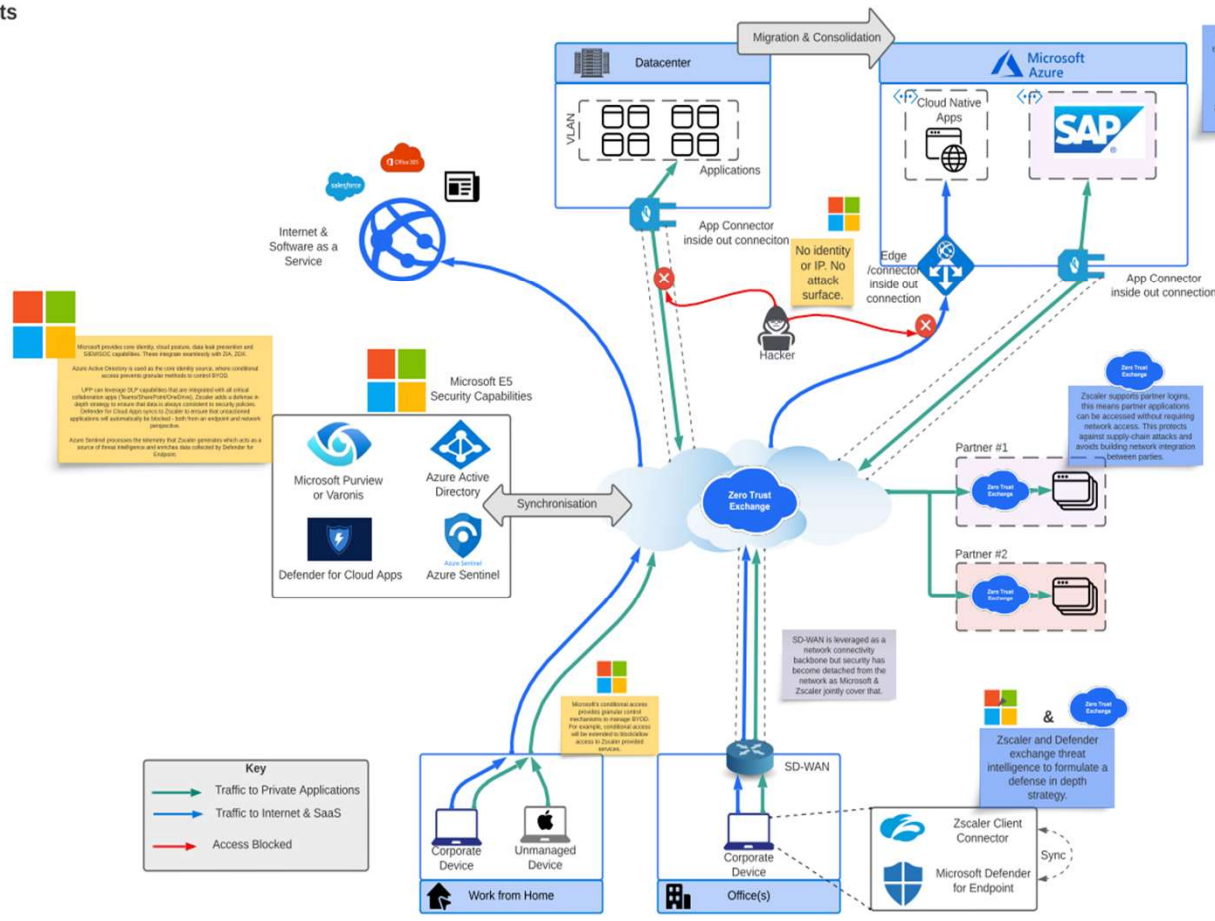
# Zscaler & Microsoft: Security Products Integrations



# Microsoft and Zscaler – Reference Architecture

## Technology Partnership Benefits

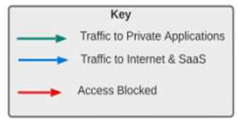
- Security Integrations**
  - Azure AD integrations for conditional access (SAML, SCIM)
  - Tenancy Restrictions for M365
  - Defender Integration for threat protection
  - Enforce DLP policies using Microsoft Information Protection labels
  - Azure Sentinel integrations, workbooks and deployment guides
  - Threat sharing for CVE Protection (MAPP)
  - Automatically block applications tagged through Defender for Cloud Apps
- App Integrations**
  - Certified Microsoft 365 networking partner, with One-click configuration (ZIA)
  - Prioritize Microsoft 365 over recreation traffic with bandwidth control (ZIA, MCAS, Cloud App Policy)
  - API integration with Teams to proactively identify user performance issues (ZDX)
  - API integrations with Microsoft 365 for posture control, threat protection, and data protection (ZIA, ZPA, MCAS)
  - Direct, Zero Trust Access to Azure Apps (Azure Virtual Wan)
- Optimized Connectivity**
  - Direct Fiber Connectivity between Microsoft & Zscaler in major cities
  - Peering with Azure and Microsoft 365 worldwide via Internet exchanges
  - Local DNS resolution to minimize latency
  - Optimized routing over Azure WAN for Microsoft 365 and Azure Apps



Services will become more cloud native over time, but this is a gradual shift. We recommend migrating cloud native applications through Microsoft App Proxy while exposing Legacy applications (e.g. SAP) through Zscaler. This creates an access fabric where both applications are accessed through the concept of identity and device trust.

Zscaler and Microsoft Teams exchange data to deliver a single pane of glass to help troubleshoot issues with Office 365.

- SaaS performance monitoring**
  - End-to-end SaaS app performance measurement
  - Granular metrics, trend analysis, and alerting
  - DNS, page fetch, availability, server response, TCP connect
- Network analytics**
  - Hop-by-hop network performance analysis
  - Latency, packet loss, hop counts
- Endpoint monitoring**
  - Unified endpoint agent
  - Device health metrics tracking
  - CPU, memory, disk, battery, WIFI



# Solution: Zero Trust Security for Workloads

Reimagine cloud connectivity with simple, secure access for Internet and private apps

## Eliminate the Attack Surface and Prevent Data Loss

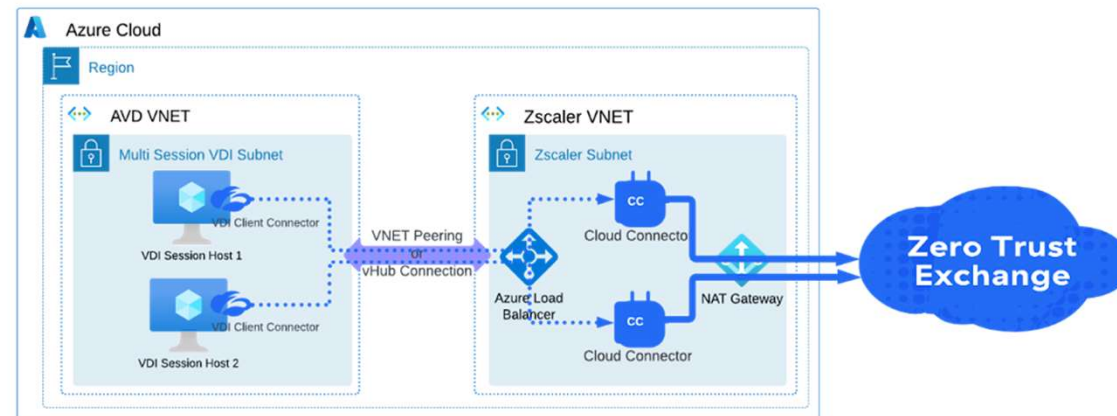
Take traffic off the corporate network by using a direct-to-cloud architecture and make applications in Azure environments invisible to cyberthreats, reducing the risk of data loss.

## Simplify Cloud Connectivity

A zero trust architecture helps avoid performance bottlenecks by connecting workloads to other applications directly, eliminating IP overlap issues and the need for complex route distributions.

## Ensure Superior Workload Performance at Scale

Every communication that reaches the Zscaler service edge is instantly processed for identity and context. Zscaler's peering relationship with the Microsoft Network ensures the shortest path between apps, no matter where they are hosted, reducing latency and improving performance.



**Customer will require Microsoft Infrastructure & Software to support up to 500 AVD Session Hosts, and a minimum of 2 Virtual Machines to host the Cloud Connector, among other Microsoft Azure components for networking and load balancing**