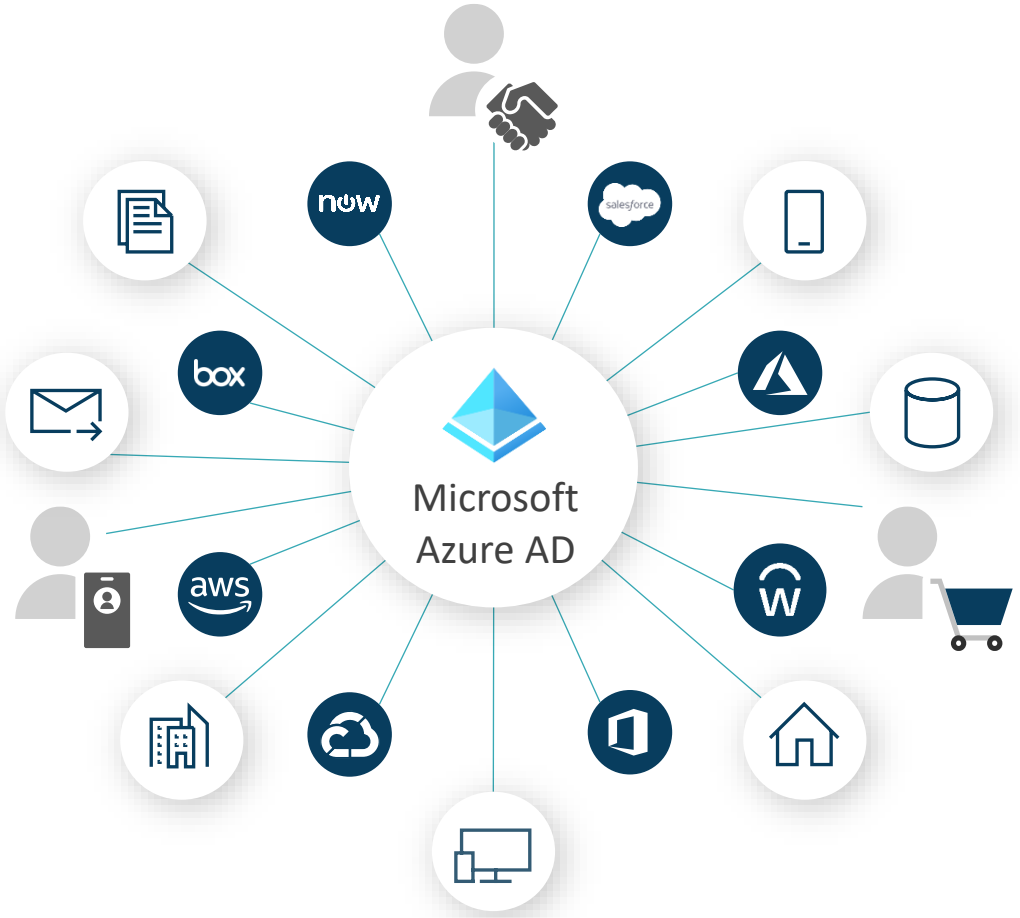
Modern Work with Microsoft 365

ANDREJ ORLOV

Sn8mann

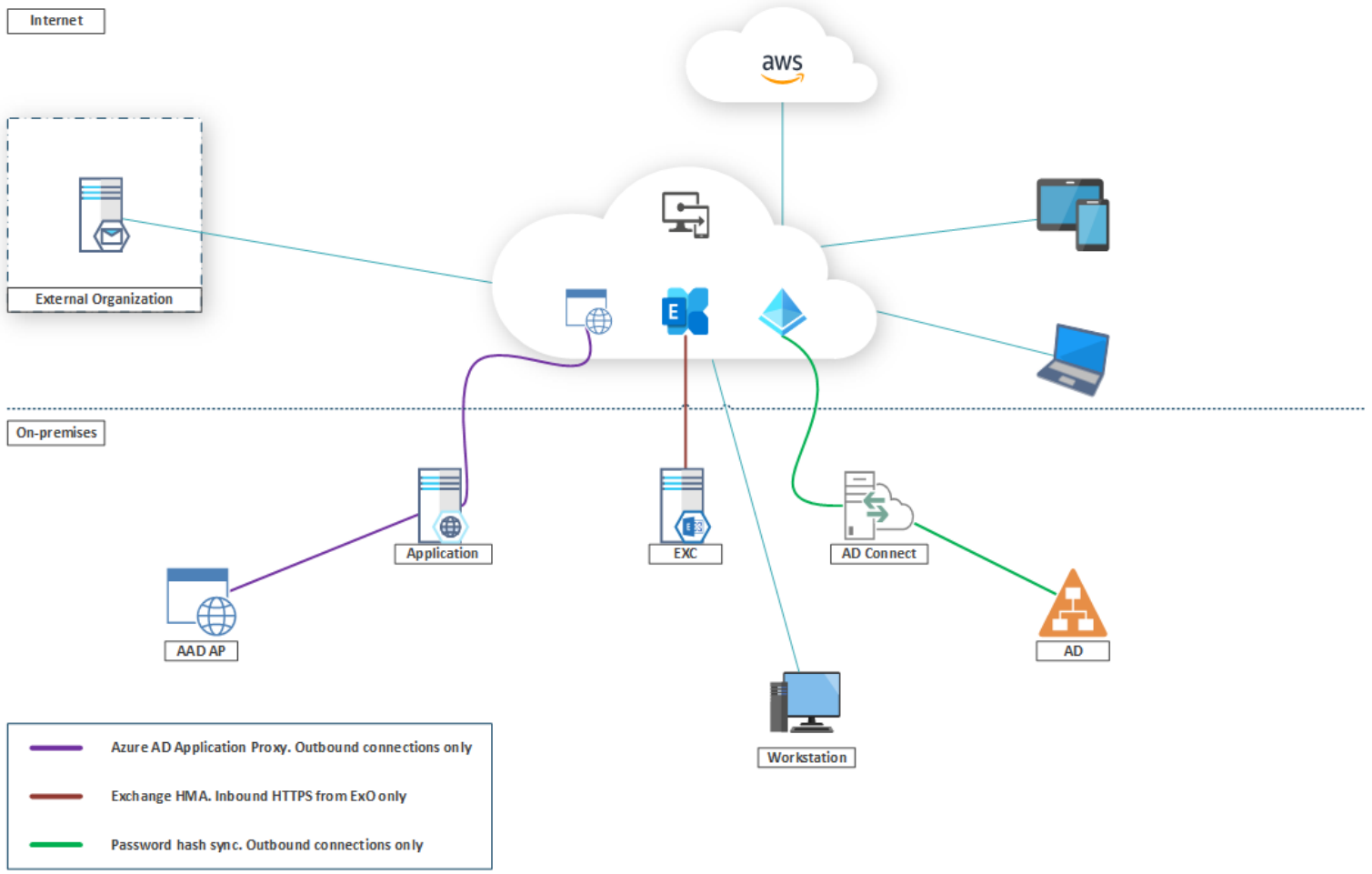
Modern Work Security design principles

- Build a Comprehensive Strategy
- Use Identity as Primary Access Control
- Assume Zero Trust
- Embrace Automation
- Design for Resilience
- Focus on Information Protection
- Drive Simplicity
- Educate and incentivize security
- Drive Continuous Improvement



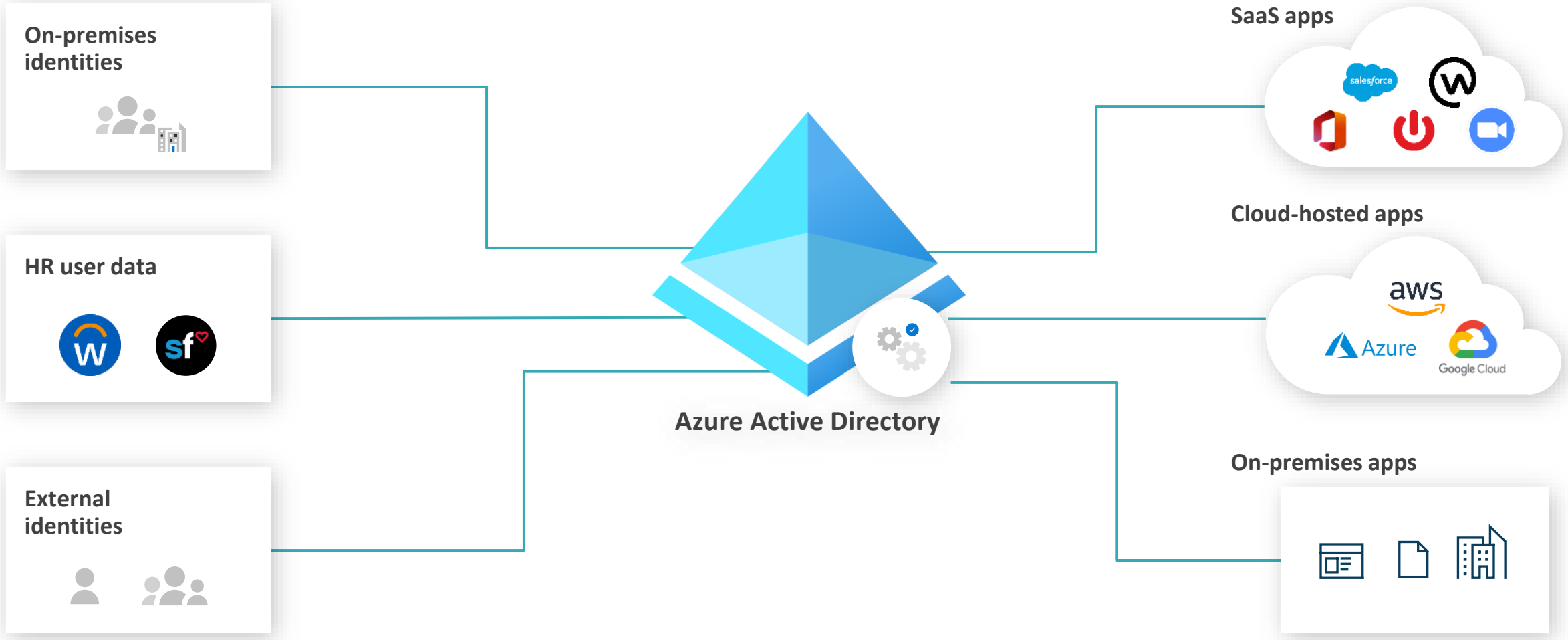
Reference architecture

Enterprise security environments are complex and include both on-premises and cloud assets



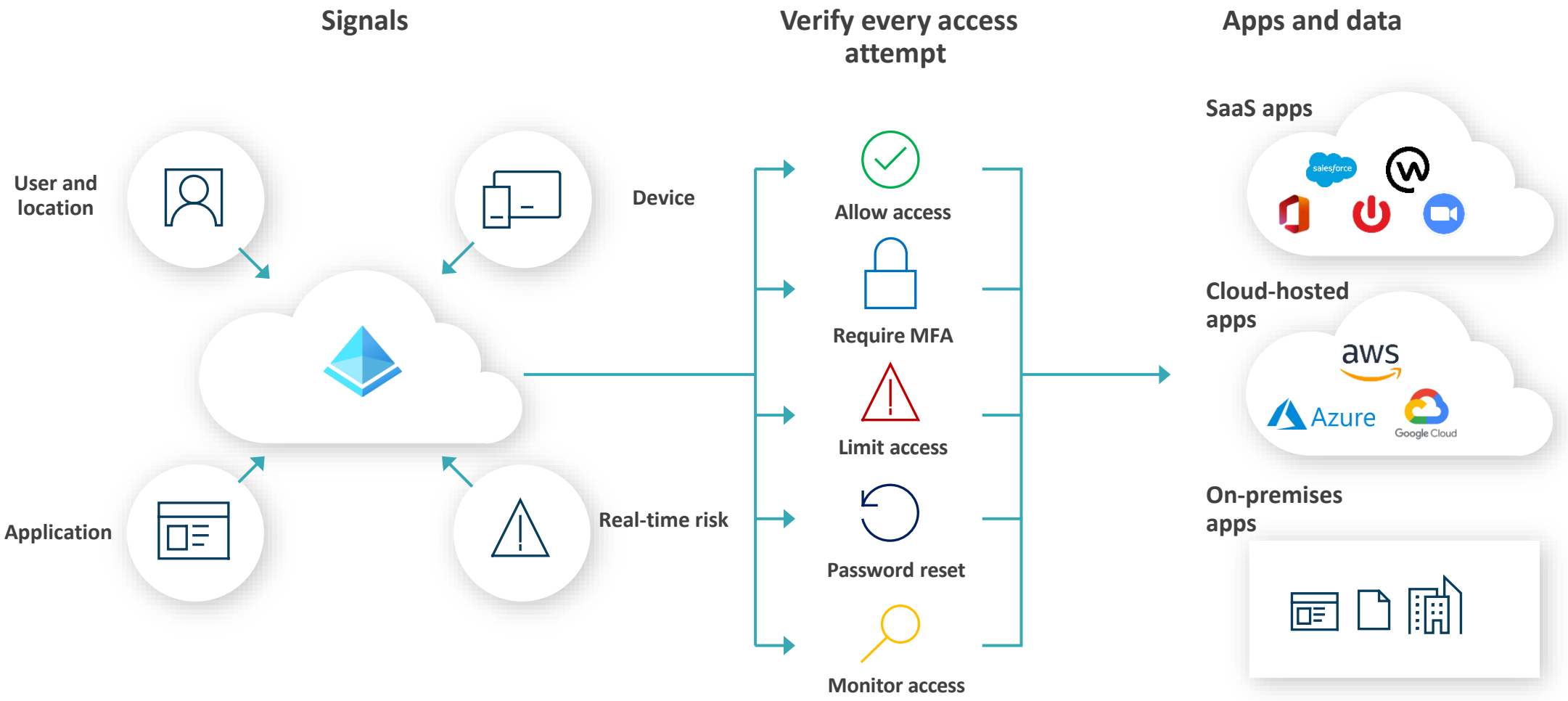
Unified identity management

Manage your users and their access



Conditional Access policies across all your apps

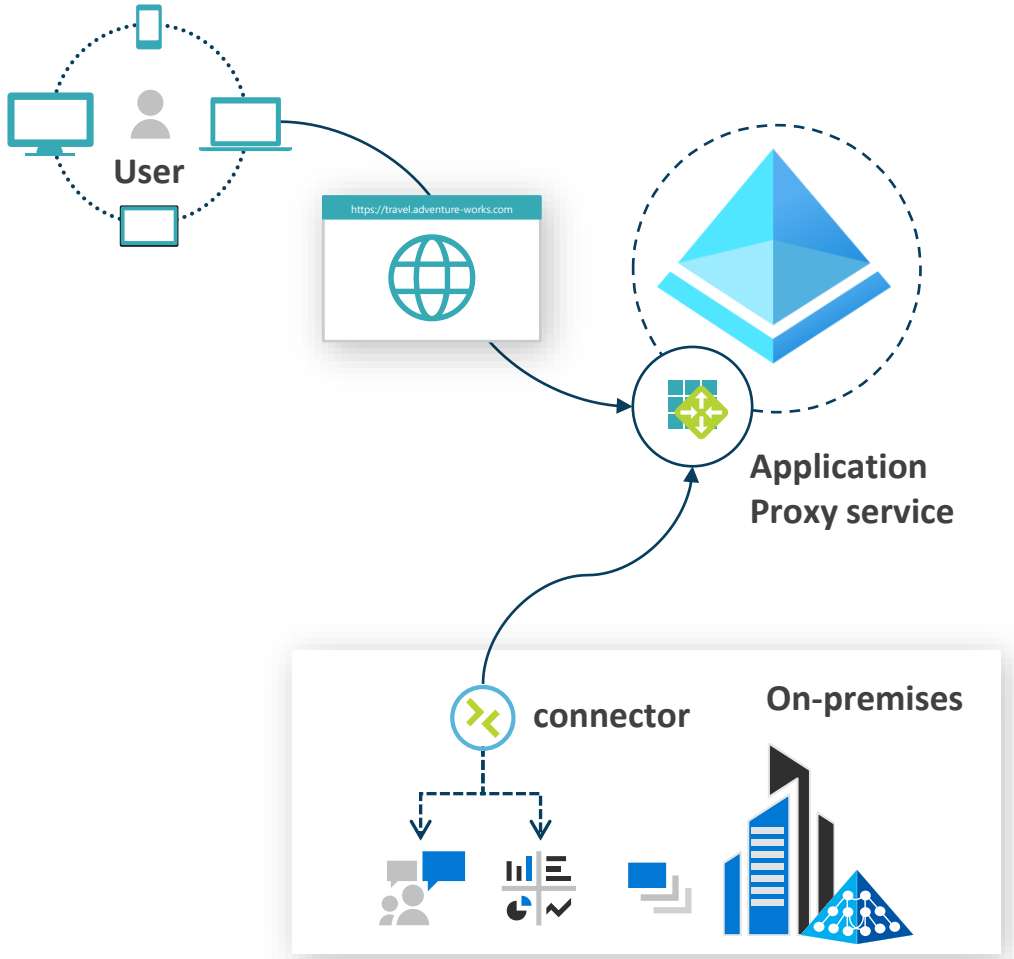
Enable Zero Trust with strong authentication and adaptive policies



Azure AD Application Proxy

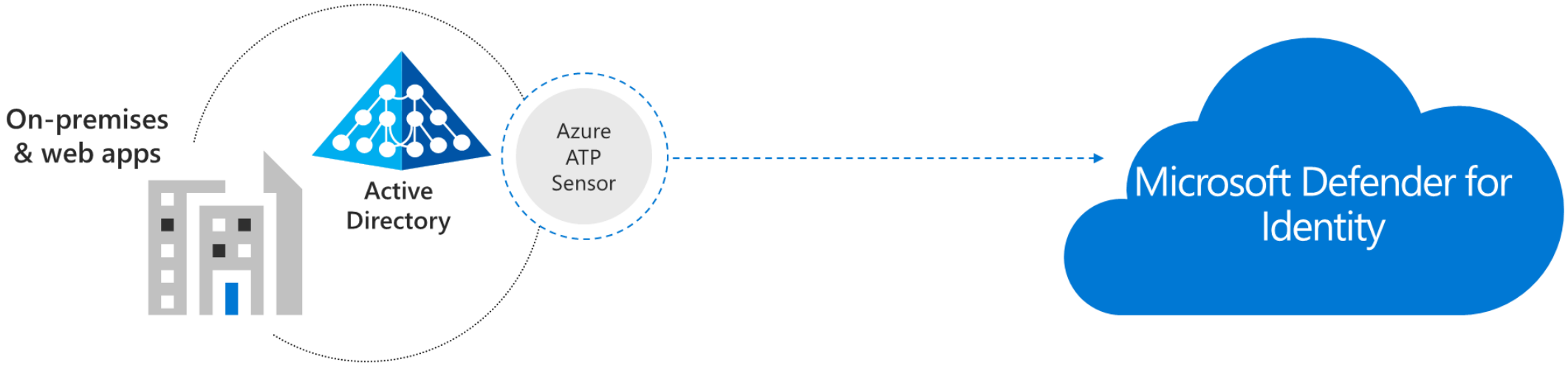
Securely connect to on-premises web apps without a VPN

- Outbound connections only
- Native support for legacy authentication protocols
  - Header-based
  - Forms- or password based
  - Integrated windows authentication
  - SAML
  - Remote desktop gateway



Microsoft Defender for Identity

Detection of On-premises Identity Attacks



Network traffic analytics

Inspect network traffic: NTLM, Kerberos, LDAP, RPC, DNS, SMB

Security events and Active Directory data

Inspect events, event tracing and profile active directory entities

User behavior analytics

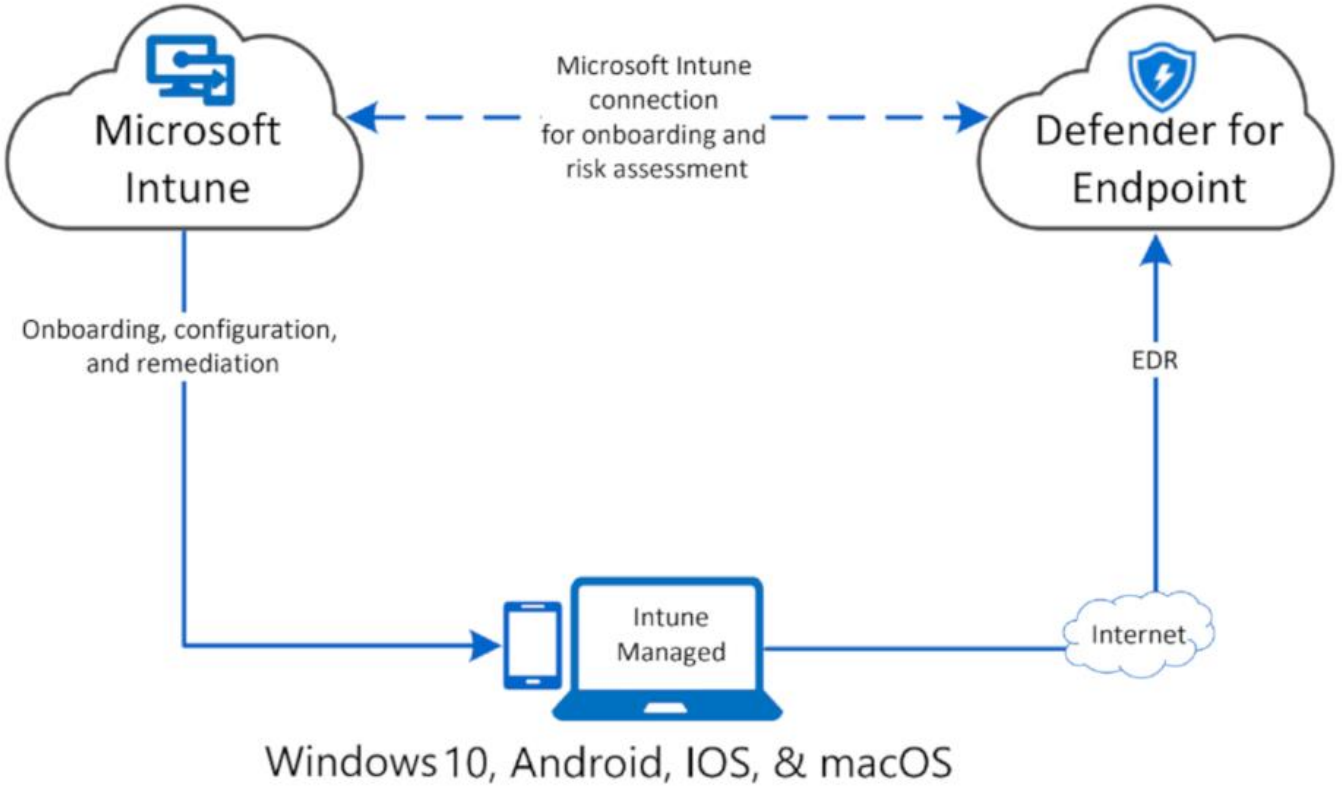
Profile users & entities behavior, identify behavior anomalies

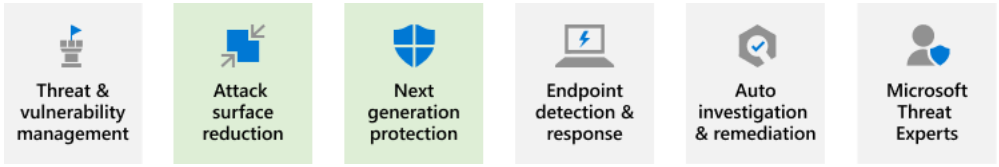
Cloud based real-time detections

Data enrichment and correlation in the cloud, for real time detections

Microsoft Defender for Endpoint

An enterprise endpoint security platform





Microsoft Defender for Cloud Apps

a Cloud Access Security Broker