

# Cybersecurity is a team sport

**Stefano Longo**

Head of Sales CyberSecurity | Compliance | Identity |  
Azure & M365



*“Security is our top priority and we are committed to working with others across the industry to protect our customers.”*

Satya Nadella

*Chief Executive Officer, Microsoft Corporation*

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships



**“comprehensive”**

# Microsoft's Security Strategy

**Diplomacy**



**Disruption**



**Defence**



***Microsoft pursues the most comprehensive cyber security strategy in the industry  
(that spans the three “Ds”)***



# Key Cybersecurity Challenges

## Traditional security approach fails – Lesson Learned

- ❑ Hackers don't break in: they log-in (with *your* credentials)
- ❑ Lack of visibility and correlation - Siloed security tools & datasets
- ❑ Blast radius of the attack is identity constrained
- ❑ Most of the attacks leverage lack of hygiene & technical debt
- ❑ Data explosion and dispersion
- ❑ Shortfall of Cybersecurity professionals
- ❑ Technology Obsolescence



# Kill chain attach

## MS Defender for Office 365

Malware detection, safe links, and safe attachments

## Azure AD Identity Protection

Identity protection & conditional access for SSO Applications  
Conditional Access

Account Compromise in cloud application or VPN

Opens attachment

Clicks on a URL

User browses to a website

Exploitation & Installation

Command & Control

User account compromise & persistence

## Unified Portal - XDR

## MS Defender for Cloud Apps

Extends protection & conditional access to other cloud apps

Exfiltrate data

Attacker collects reconnaissance and configuration data

Attacker accesses sensitive data

Attacker attempts lateral movement

Privileged account compromised

Domain compromise & persistence

## Microsoft Defender for Endpoint

Endpoint Detection and Response (EDR) & End-point Protection (EPP)

## MS Defender for Identity

On Premises Identity protection

Azure



Sentinel

"Intrusion Detection for Active Directory"

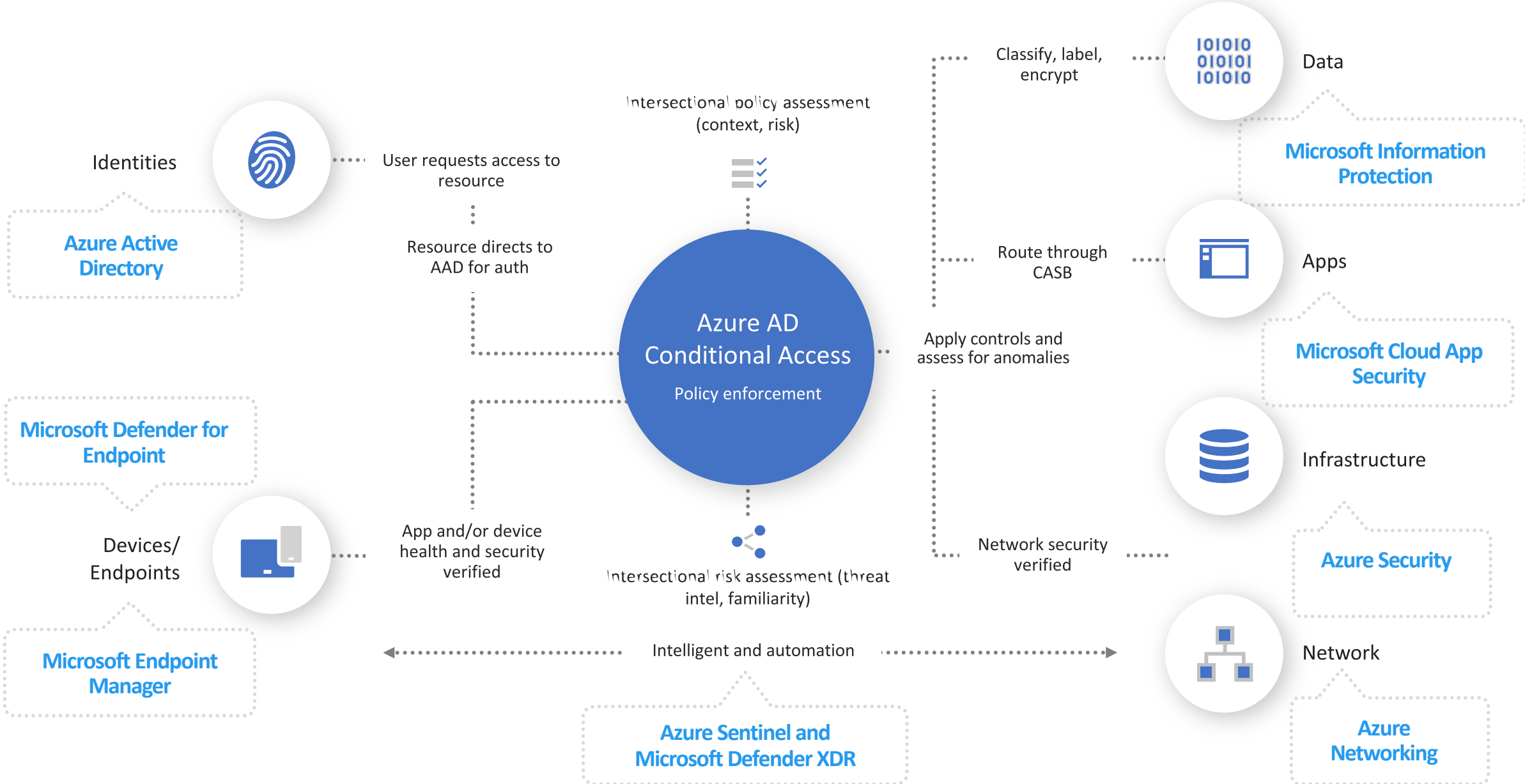
Training/Certification

Support for adoption

Hands-on for SOC

Technical workshop

# Microsoft's Zero Trust enabling technologies



# RiskIQ Evolution and collaborative integrated model





grazie