Microsoft

Implementing Zero Trust Architecture with Microsoft Security Stack

A Modern Security Approach for Hybrid Environments

Presented By:

Alaa Eddine AYEDI

“Cloud Security Intern”

Supervised By:

Mr. Karim ABED

Consultim-IT

The Best of Consulting and IT

2024-2025

Current Security Landscape

The Modern Security Challenge

Rising Cyber Threats

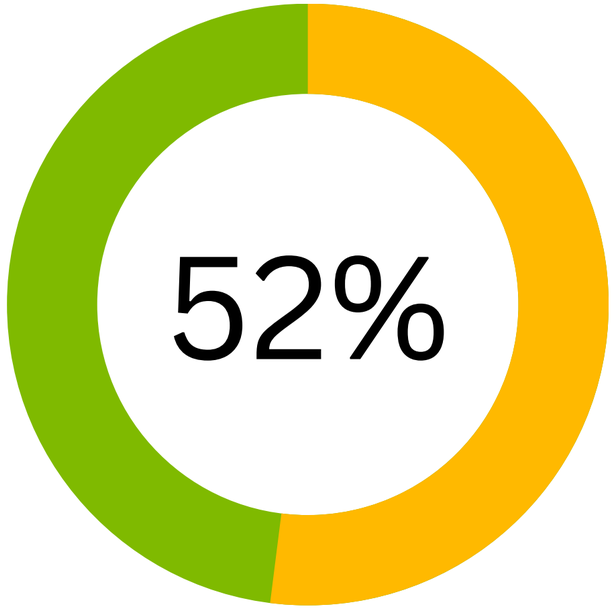
- 80% of organizations have experienced a cloud security incident in the past year.

Financial & Operational Impact

- Ransomware costs organizations an average of $4.54M per attack.

Cloud & Hybrid Security Gaps

- 90% of businesses rely on cloud services, but only 41% have adequate cloud security controls.



of companies have migrated most of their IT to the cloud

The Need for a New Security Approach

key reasons why Zero Trust is essential

Rising Cyber Threats

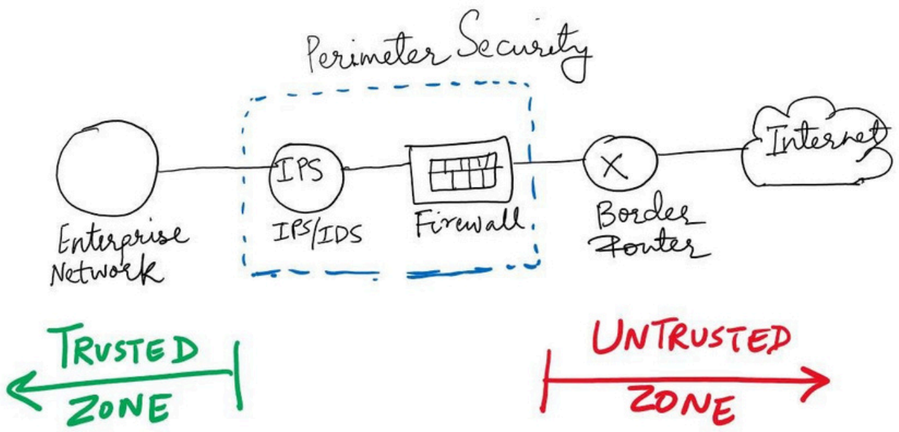
- Increasing sophistication of attacks.

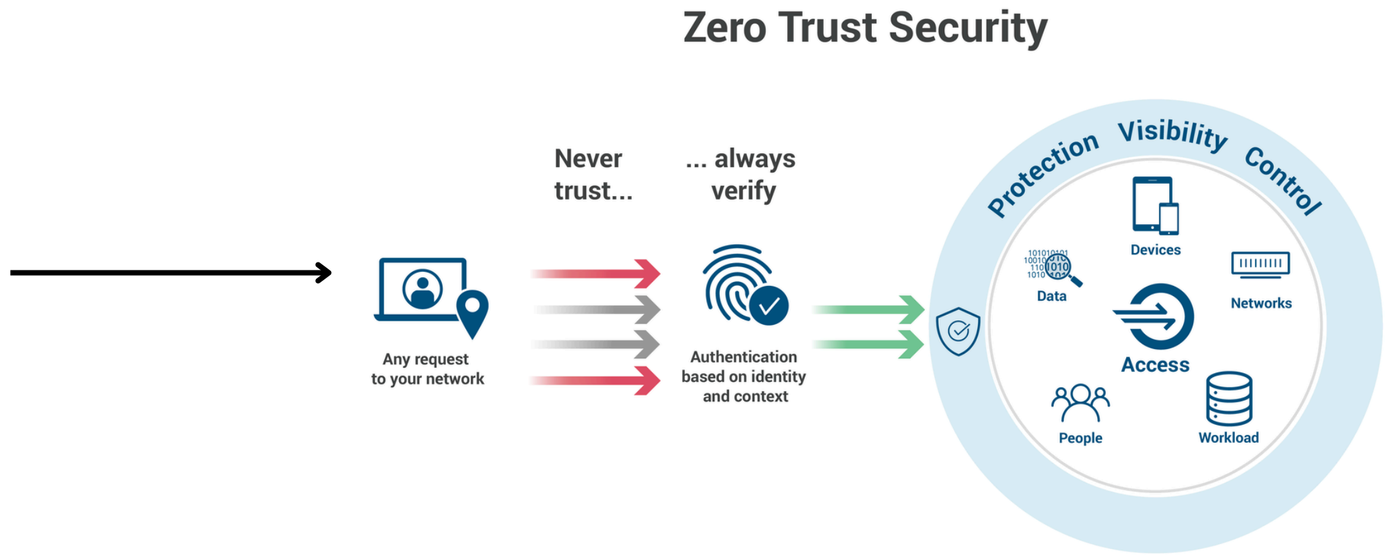
Regulatory Compliance:

- Need for stricter access controls and monitoring

Hybrid Environments

- Complexity of securing both cloud and on-premises resources.





Zero Trust Foundation

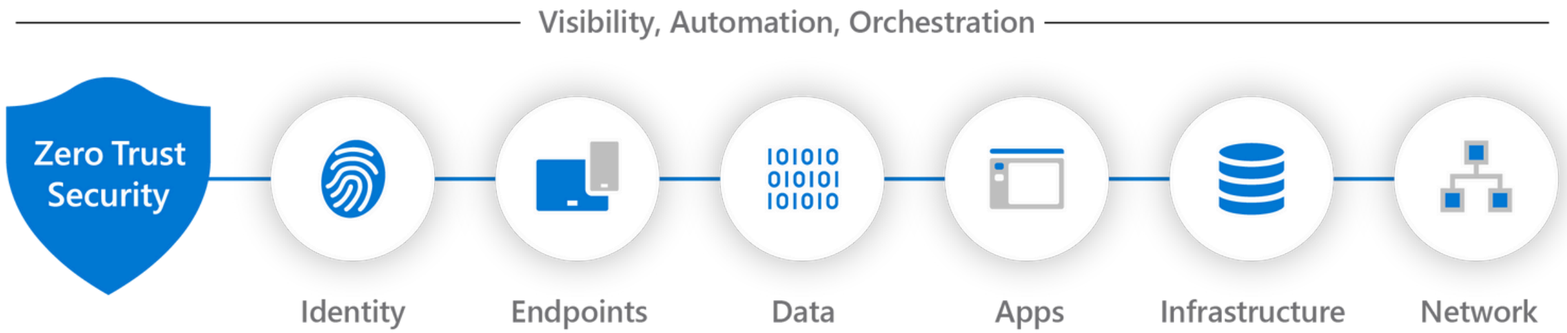
Core Principles

“Never trust, always verify”

Verify Explicitly

Use least privileged access

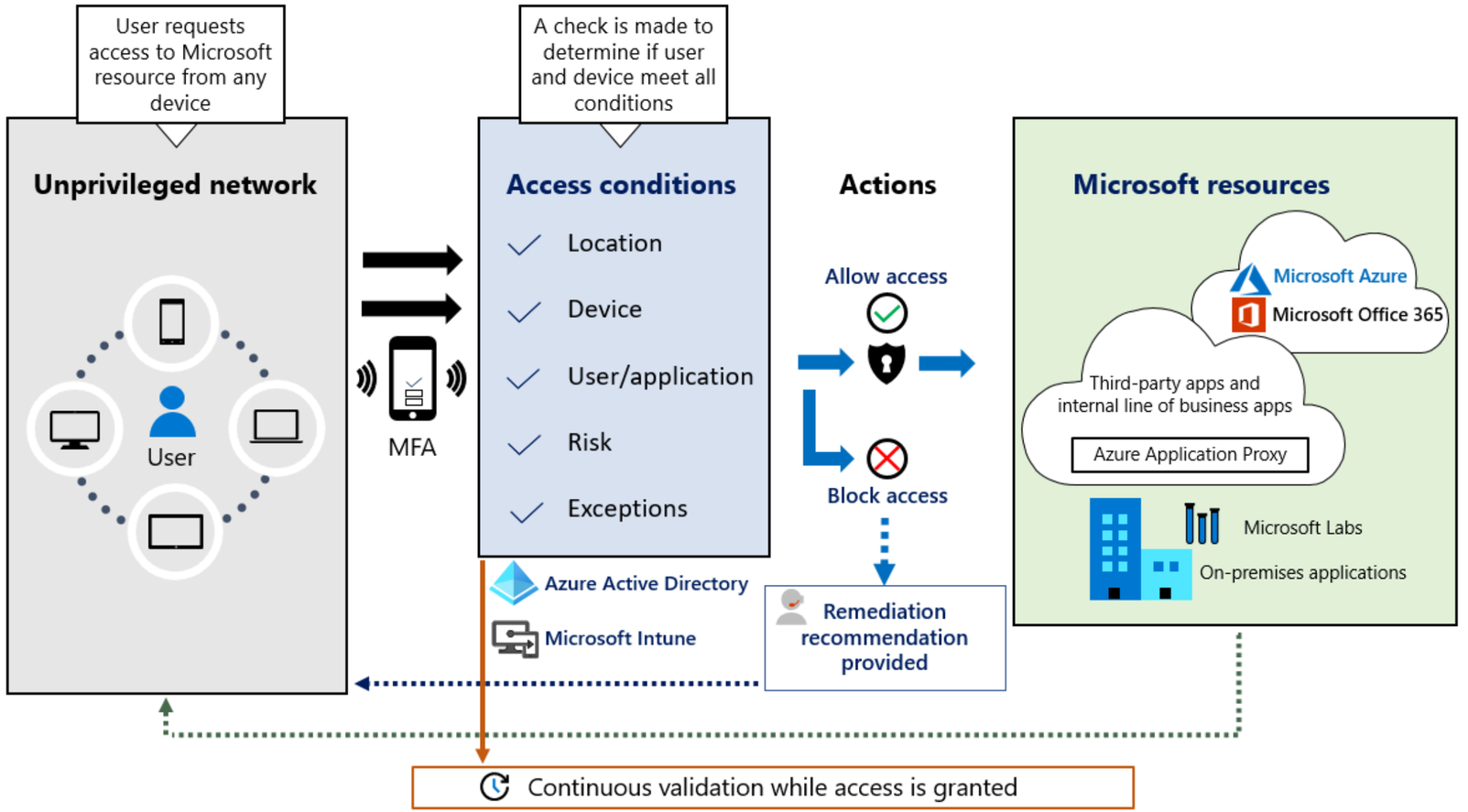
Assume Breach



Zero Trust Foundation

Microsoft's Approach

Microsoft Entra ID

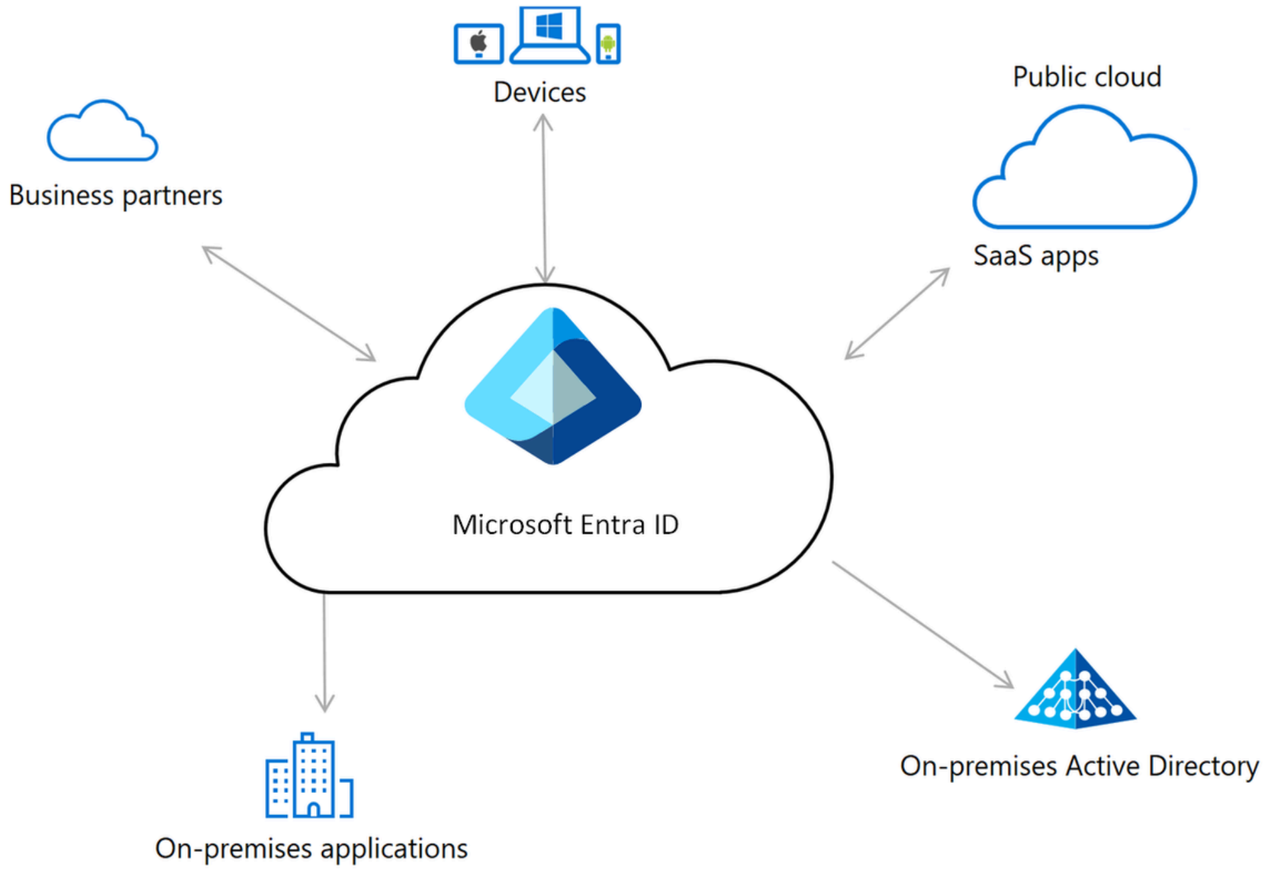


Intune

Microsoft Defender for Endpoints

Microsoft Entra ID

Overview



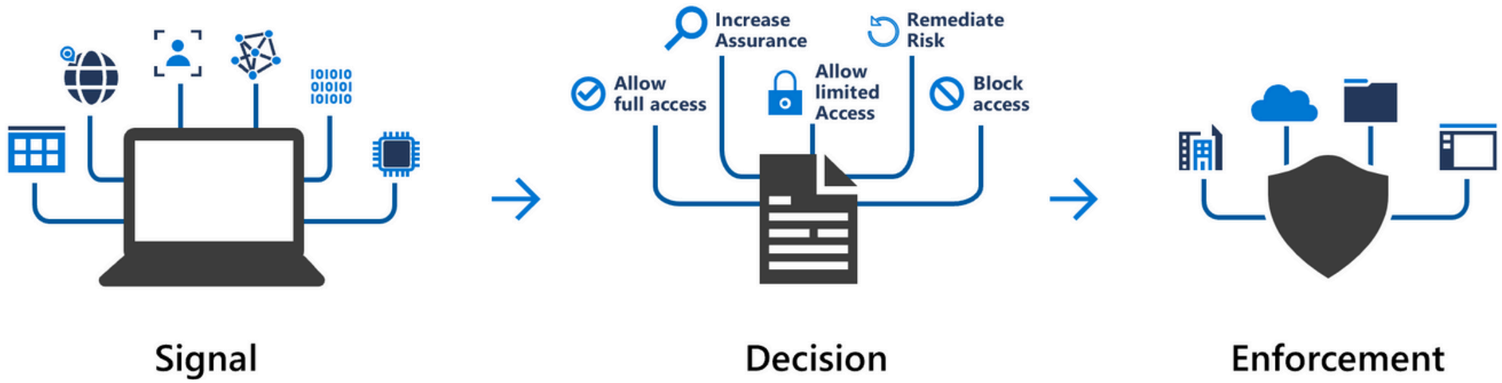
Cloud-based IAM service

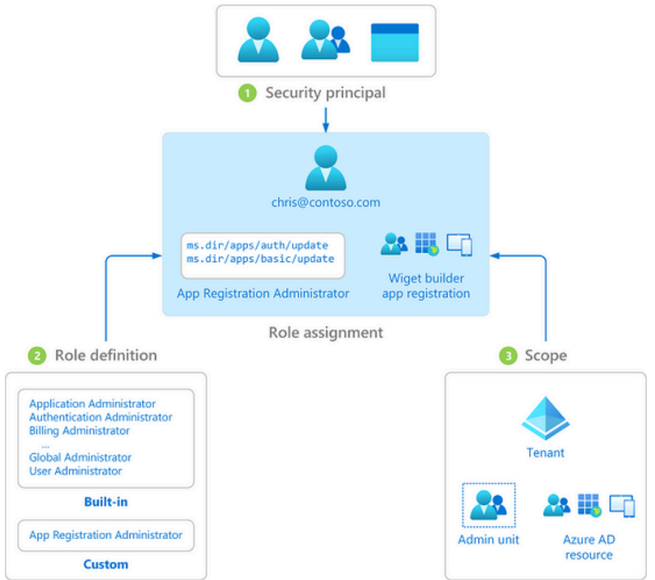
- Manage Identities
- Enforce Access Policies
- Secure Applications and Data in the Cloud and On-prem

Microsoft Entra ID

Key Features

- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)
- Conditional Access
- Privileged Identity Management (PIM)
- Identity Protection
- Hybrid Identity
- Self-Service Password Reset
- Access Reviews
- Application Governance





Microsoft Entra ID

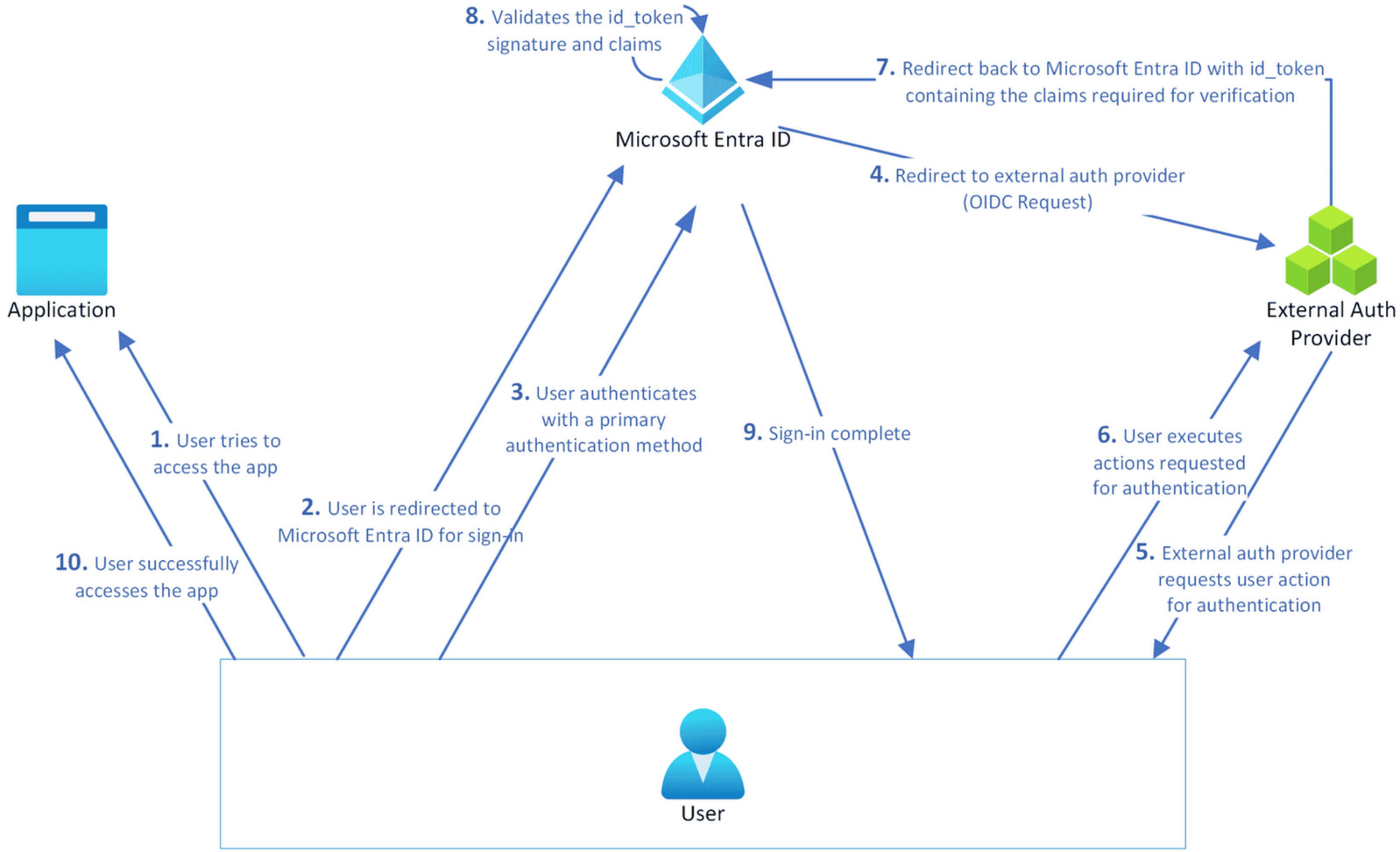
Zero Trust Implementation

Identity Verification

- Continuous Assessment
- Contextual Access

Policy Enforcement

- Granular Controls
- Adaptive Policies

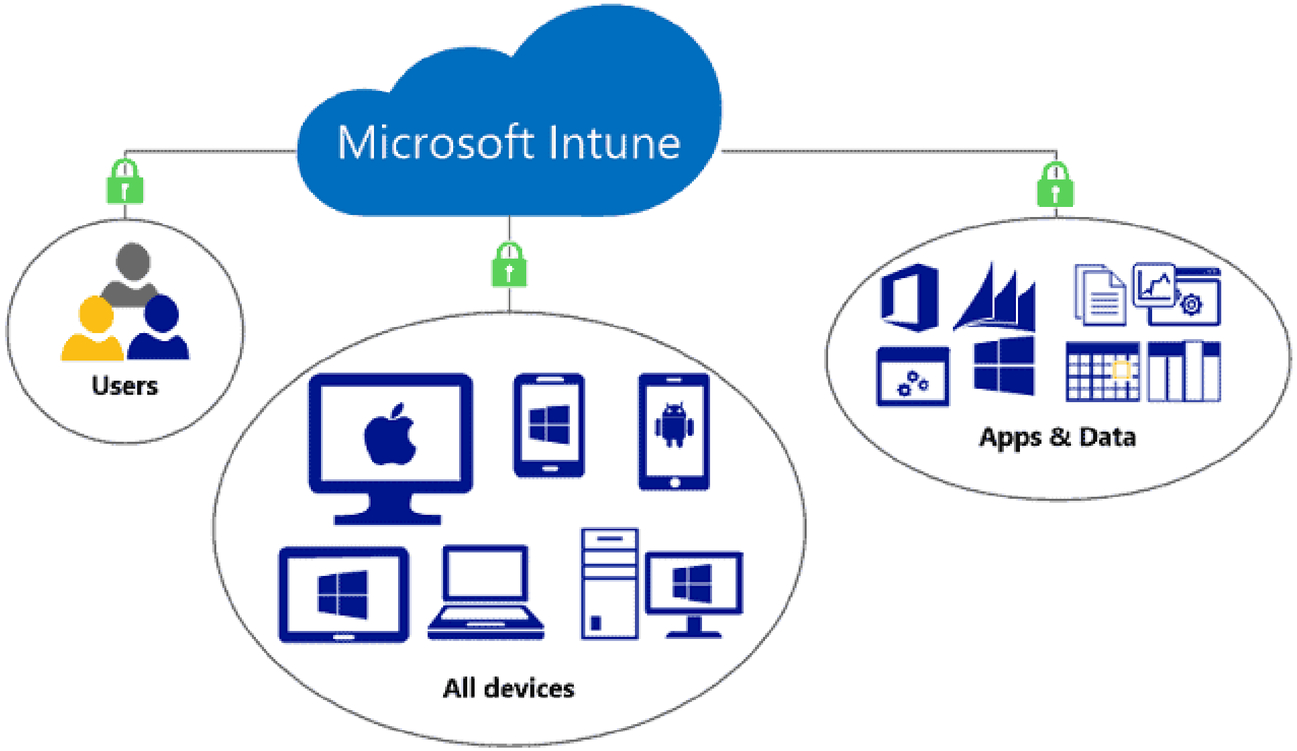


Microsoft Intune

Overview

Cloud-based Endpoint Management Solution

- Enforce Compliance
- Policy Management
- Manage and Secure devices, applications, and data



Microsoft Intune

Key Features

- Unified Endpoint Management
- Device Compliance Policies
- Automated Device Enrollment
- Remote Actions
- Integration with Microsoft Defender for Endpoint
- Mobile Application Management Capabilities
- Endpoint Security
- Cross-platform Compatibility
- Reporting and Analytics
- Conditional Access Integration

Microsoft Intune

Zero Trust Implementation

Device Trust

- Device Health Attestation
- Compliance Verification

Integration Capabilities

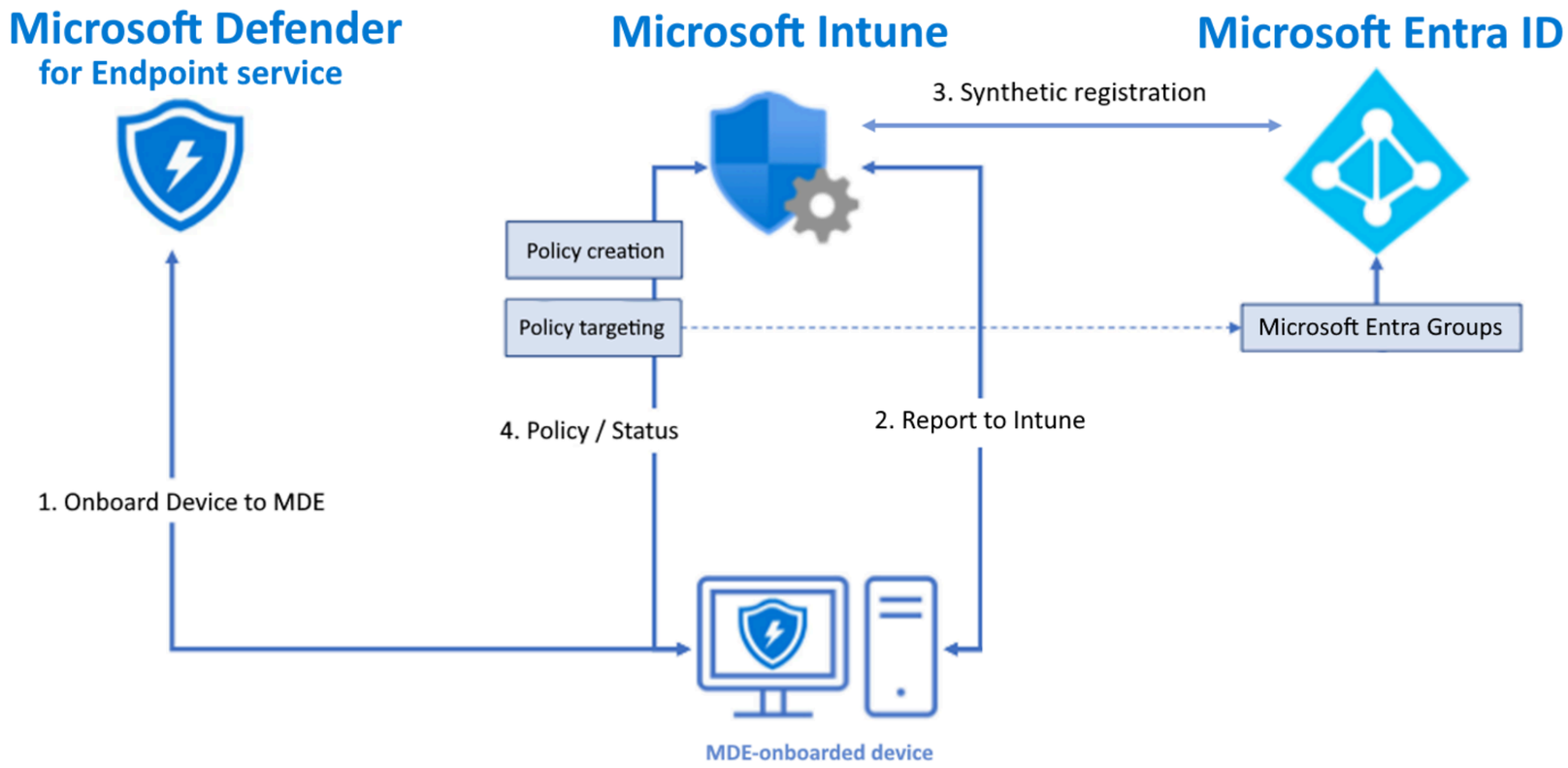
- Third-Party Integration
- Microsoft Services

App Security

- Protected Apps
- App Configuration

Monitoring and Reporting

- Device Monitoring
- Reporting

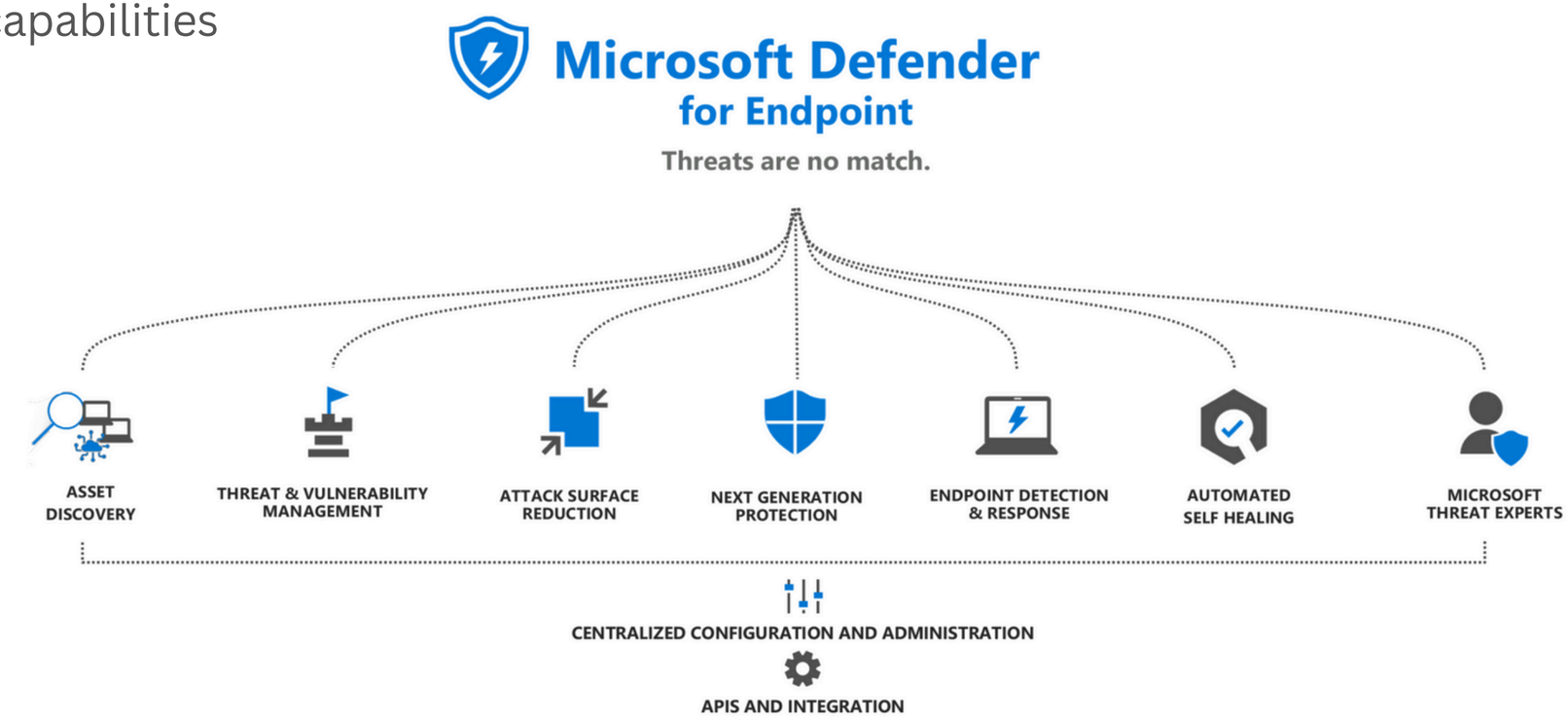


Microsoft Defender for Endpoint

Overview

centralized security control over both cloud and on-prem resources

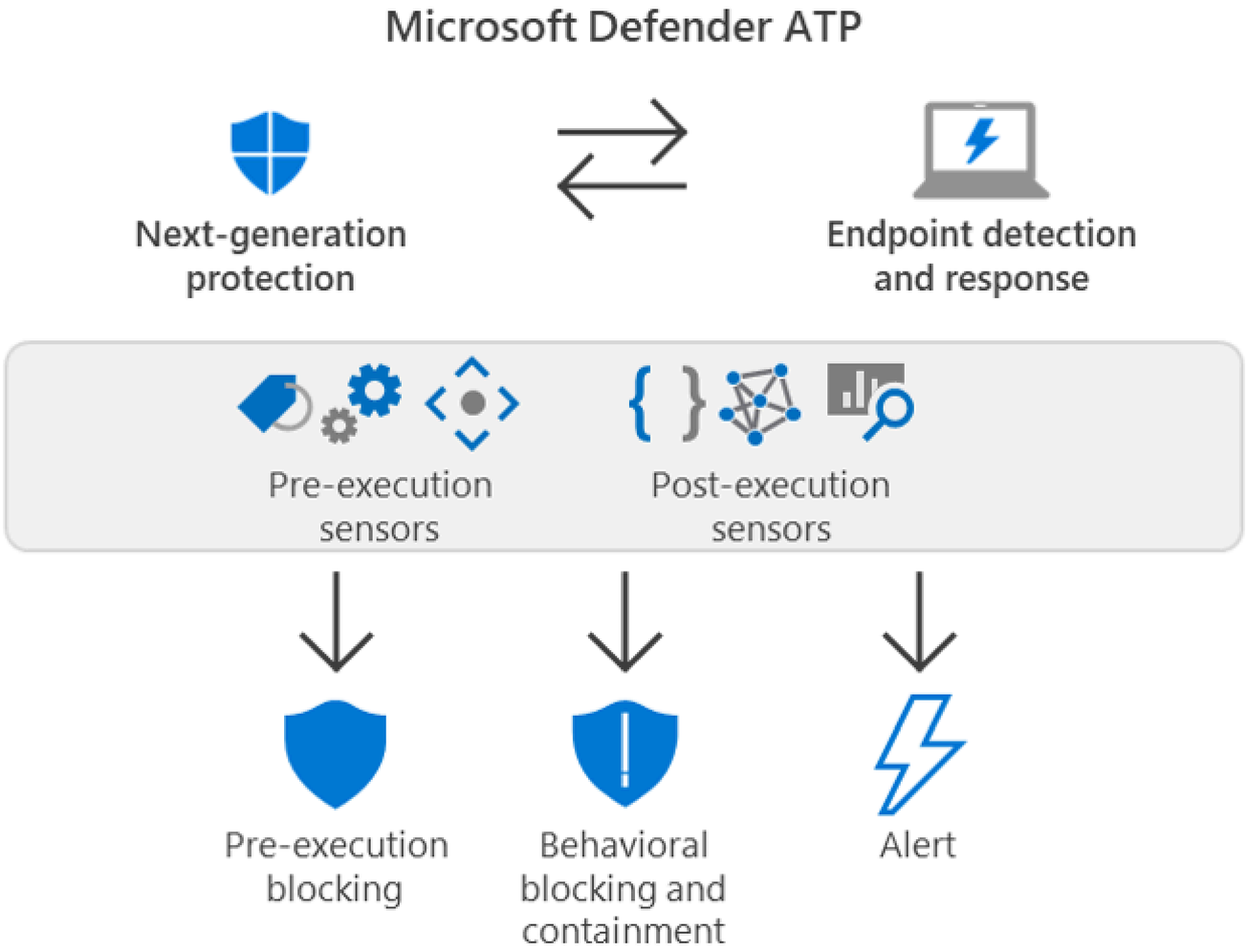
- monitor Microsoft Defender functionalities
- prevent, detect, investigate, and respond to advanced threats
- provide ATP and detection capabilities



Microsoft Defender for Endpoint

Key Features

- Attack Surface Reduction
- Next Generation Protection
- EDR Capabilities
- Third-Party Integration
- Threat Intelligence
- Device Discovery and Management
- Advanced Threat Hunting
- Auto Investigation and Remediation
- Secure Score



Microsoft Defender for Endpoint

Zero Trust Implementation

Device Risk Assessment

- Risk Factors
- Risk-based Access

Continuous Monitoring

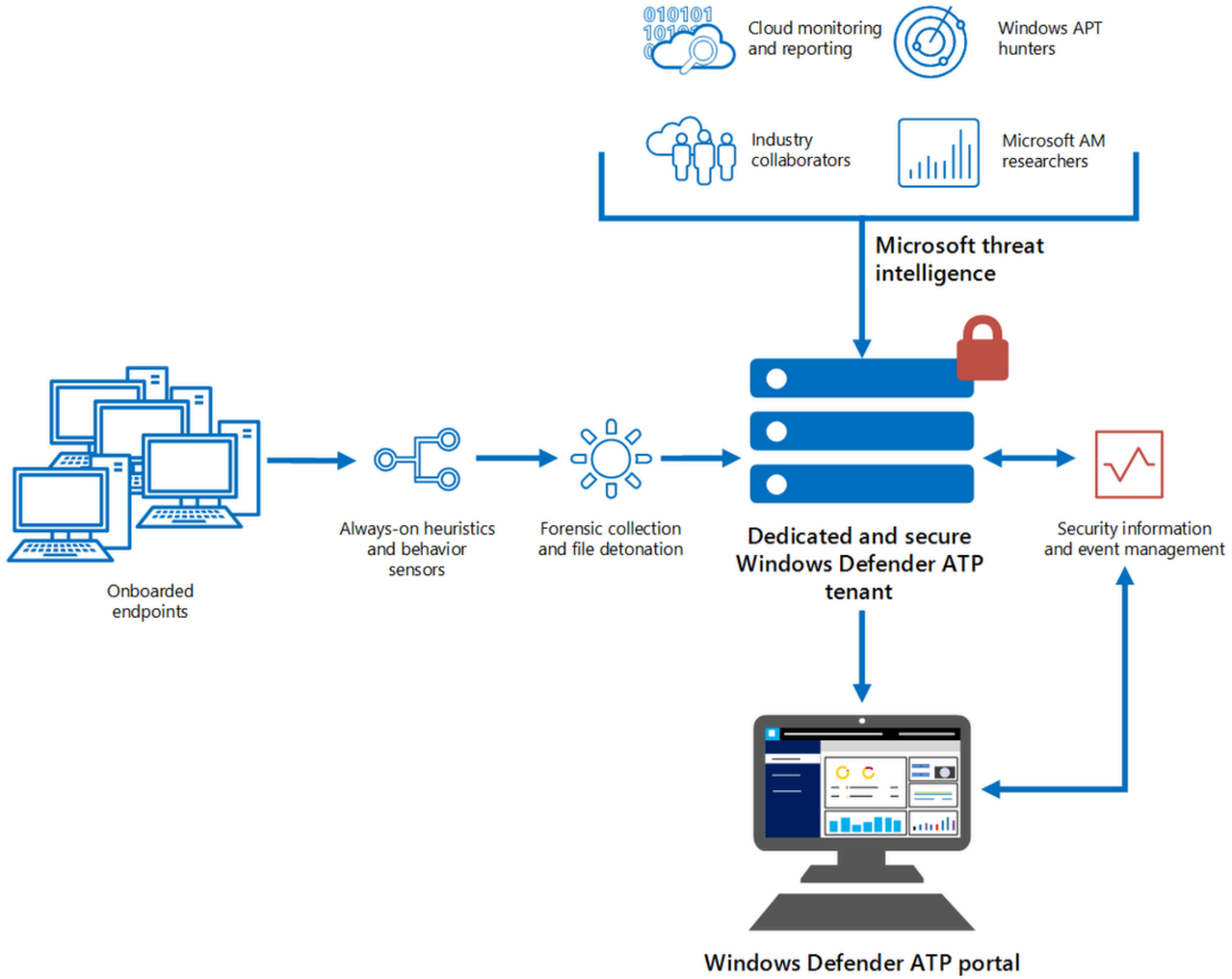
- Security Monitoring
- Response Automation

Security Operations

- Incident Management
- Reporting and Analytics

Specialized Features

- Cloud Protection
- Mobile Threat Defense



Hybrid Environment Integration

Microsoft’s Zero Trust Tech Stack

Unified Identity Management

- Entra ID provides a single identity platform for both cloud and on-premises resources.

Seamless Device Management

- Intune ensures consistent security policies across all devices, regardless of location.

Centralized Threat Protection

- Defender for Endpoint monitors and protects endpoints across hybrid environments.

Interoperability with Third-Party Providers

- Microsoft’s solutions can integrate with other cloud providers (e.g., AWS, Google Cloud) and on-premises systems, ensuring flexibility and scalability.