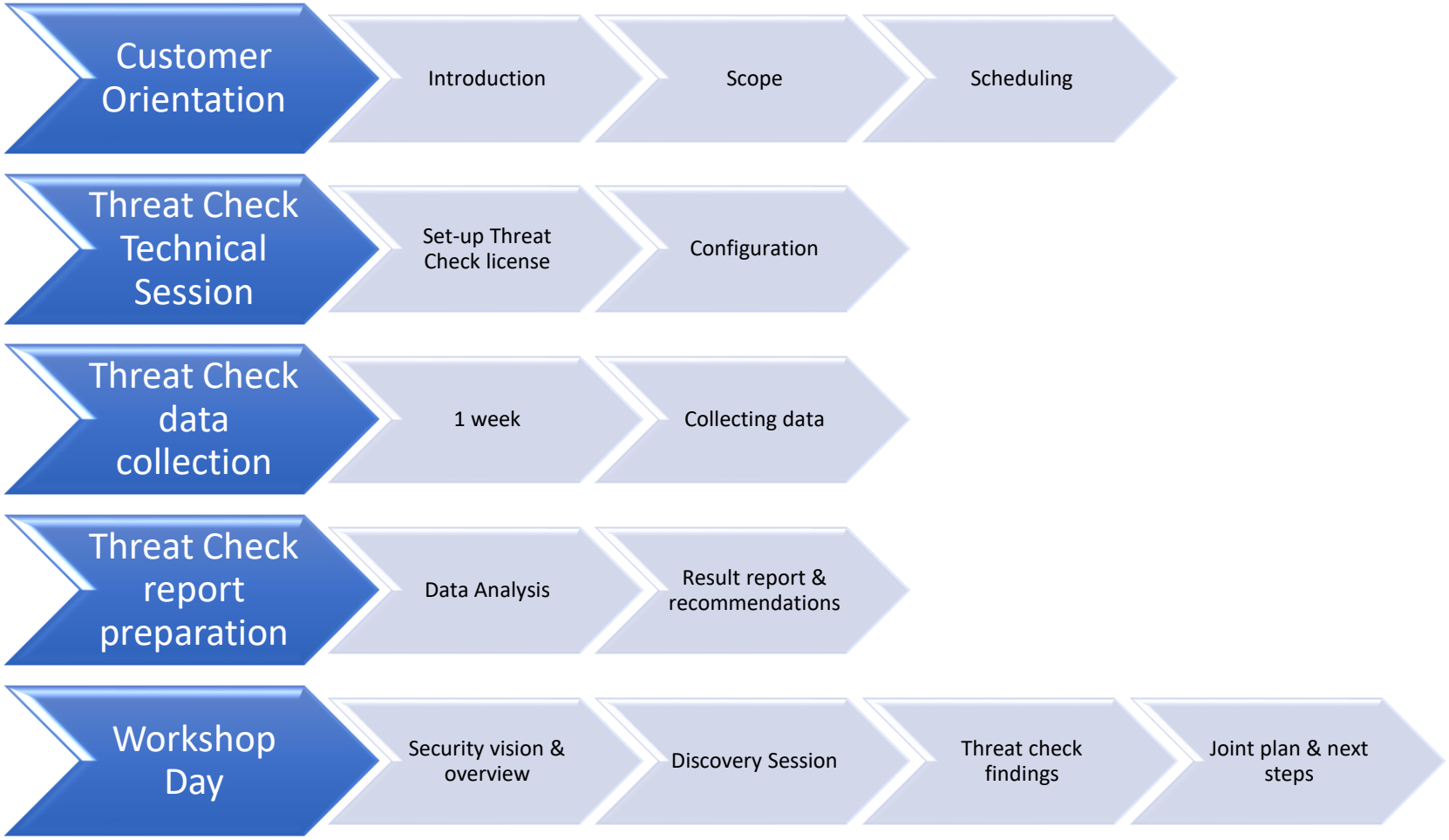
Security Workshop Introduction

Assessment Goals:

- Help customers assess their security landscape
- address their most pressing security goals and challenges
- Provide an immersive experience that brings to life Microsoft's security vision and capabilities
- Run the Threat Check analysis and review the results report & recommendations
- Plan for security next steps

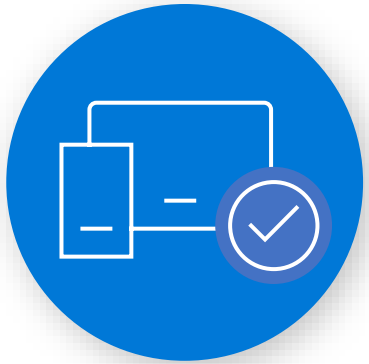
Security Workshop Agenda



Identity and Access management

Secure identities to reach zero trust

Secure Authentication



Conditional Access

Identity Protection

Identity & Access

- Is your end user authentication seamless and secure?
- How much control do you have over access?
- How do you secure identities against current and emerging threats?

Secure Authentication

- Application registration and SSO
  - Manage all application access using one identity
- Multi Factor Authentication:
  - Strengthen your authentication by enforcing the MFA on your organization
- Password-Less:

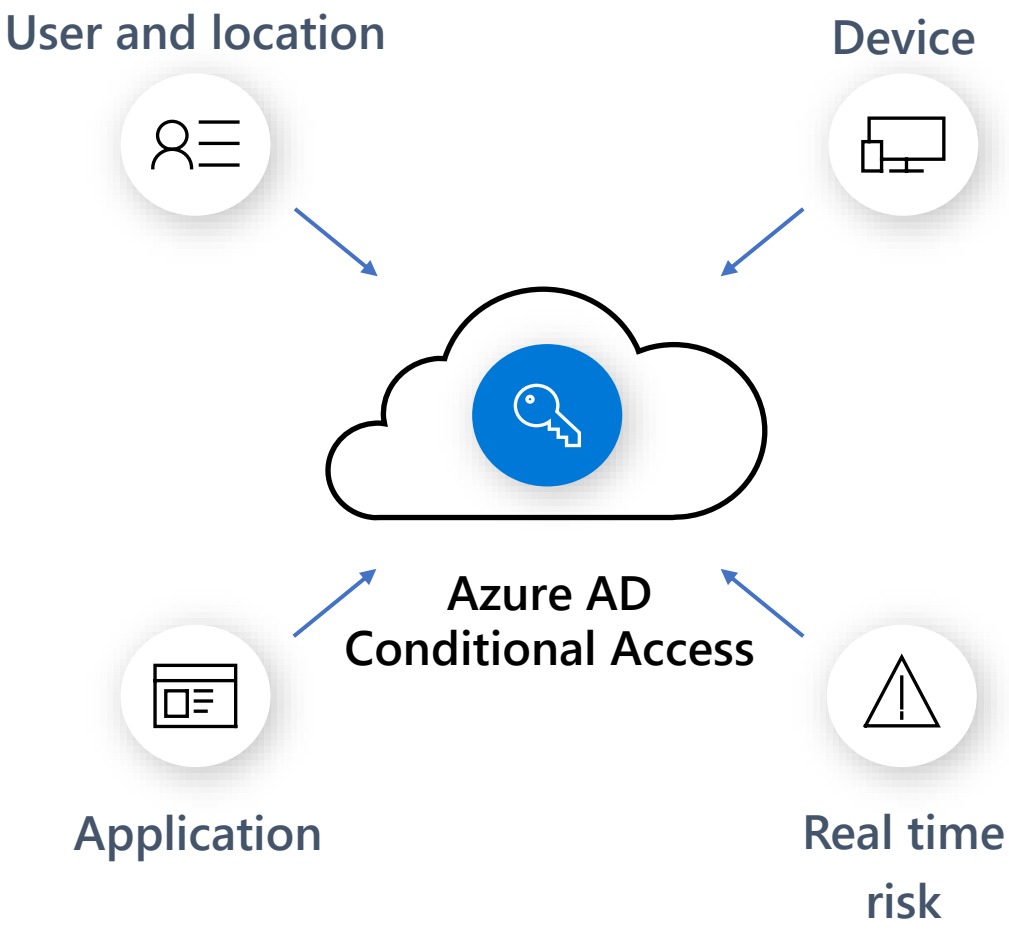
(**Over 82% of the breaches are caused by stolen password**)

Conditional Access

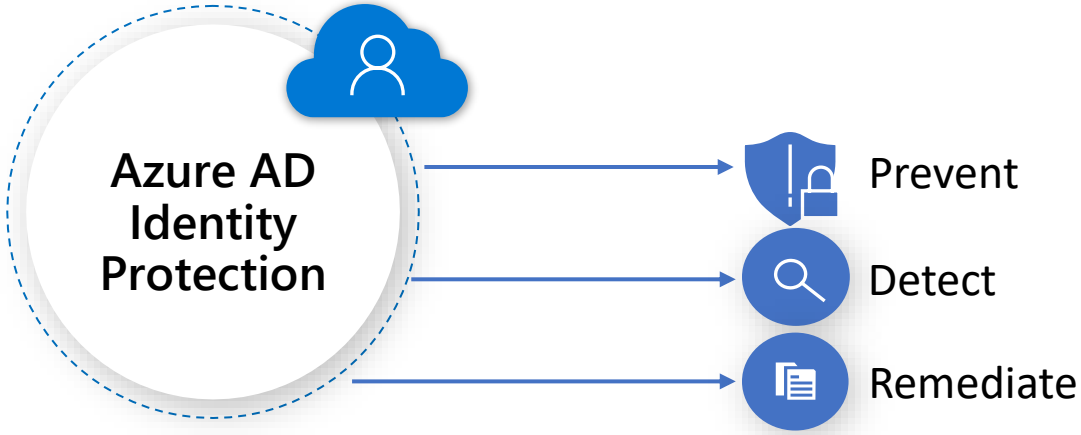
Secure identities to reach zero trust

End to end solution across users, devices, apps and data, using policies and real time signals to determine when to:

- Allow / Block access.
- Require additional proofs like MFA.



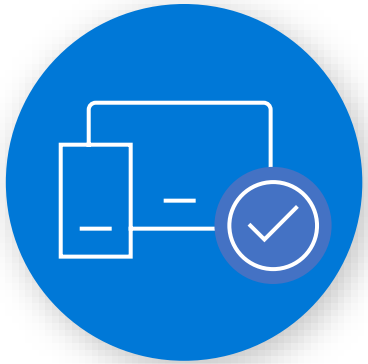
Azure AD Identity Protection



Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

Device Management



Mobile Device Management
MDM

Mobile Application Management
MAM

Intune Main Features

- Device management (enrolling devices, performing software and hardware inventory checks).
- Managing security and compliance policies.
- Managing LOB applications and app store applications supporting Intune SDK (mostly Microsoft)
- Combine with On-Premises SCCM solution to control non-domain-joined devices.
- Deploy policies, configurations and software installations for non-domain joined devices.

Microsoft Threat Protection

Secure your organization against advanced threats!

- Can you detect suspicious activities on your network?
- How do you know if credentials have been compromised?
- How quickly can you remediate advanced threats?
- How do you protect your users from email threats?

Azure Information Protection

Control and help secure email, documents, and sensitive data inside and outside your company walls.

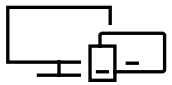
Discover & classify sensitive information

Apply protection based on policy

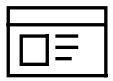
Monitor & remediate

Accelerate Compliance

Across



Devices



Apps

Cloud services

On-premises

Office 365 ATP

Sandbox Safe Attachments

Anti-phishing protection

Threat protection policies: Define threat-protection policies to set the appropriate level of protection for your organization.

Reports: View real-time reports to monitor ATP performance in your organization.

Threat investigation and response capabilities: Use leading-edge tools to investigate, understand, simulate, and prevent threats.

Automated investigation and response capabilities: Save time and effort investigating and mitigating threats.

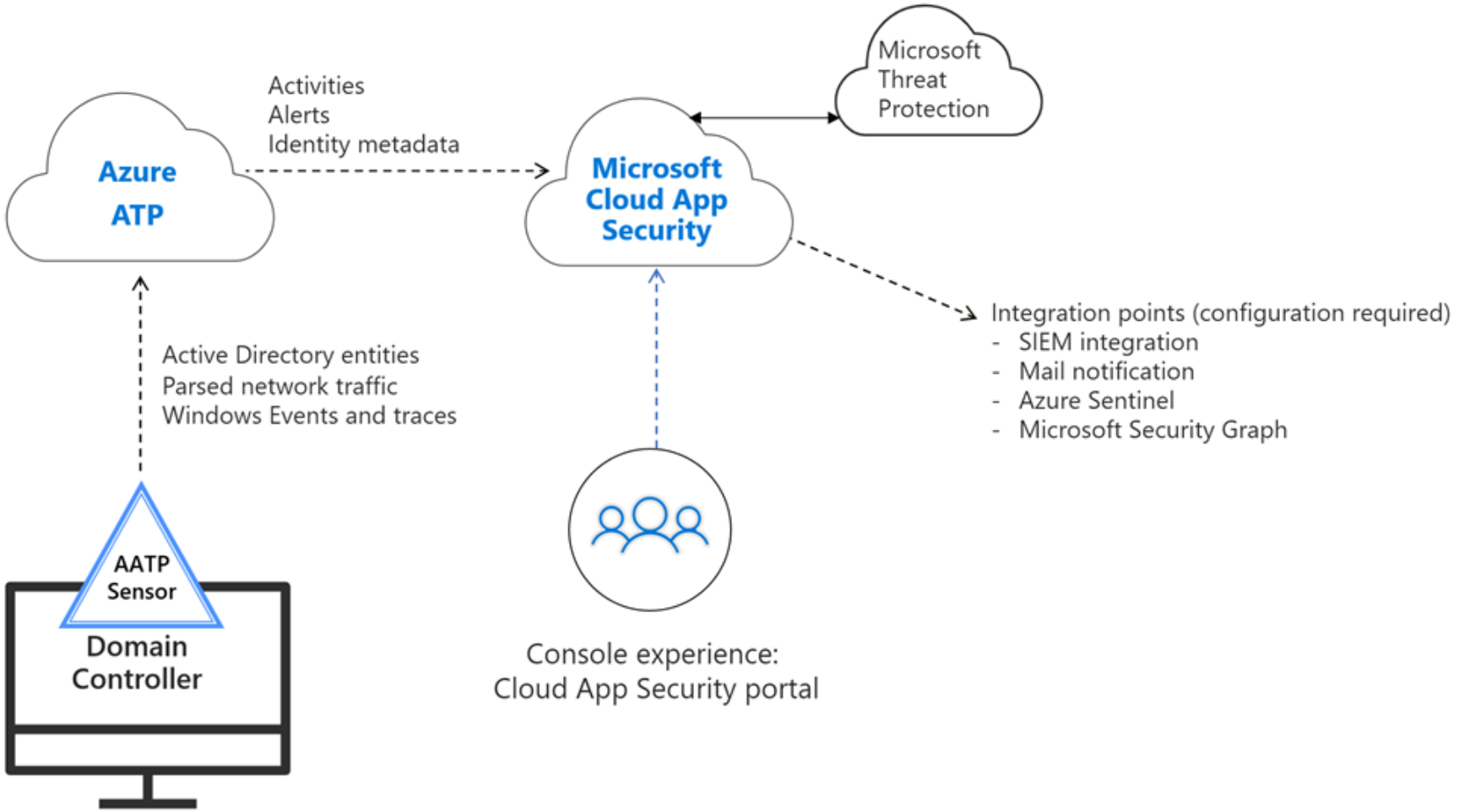
Safe Links Protection

ATP for SFB, ODFB, TFB

Azure ATP

- Monitor users, entity behavior, and activities with learning-based analytics.
- Protect user identities and credentials stored in Active Directory.
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain.
- Provide clear incident information and evidence on a simple timeline for fast control.

Azure ATP Architecture



Defender ATP

Secure score

Automated investigation and remediation

Endpoint detection and response

Endpoint behavioral sensors: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.

Cloud security analytics: Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.

Threat intelligence: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

Threat & Vulnerability Management

Attack surface reduction

Next generation protection

Cloud App Security

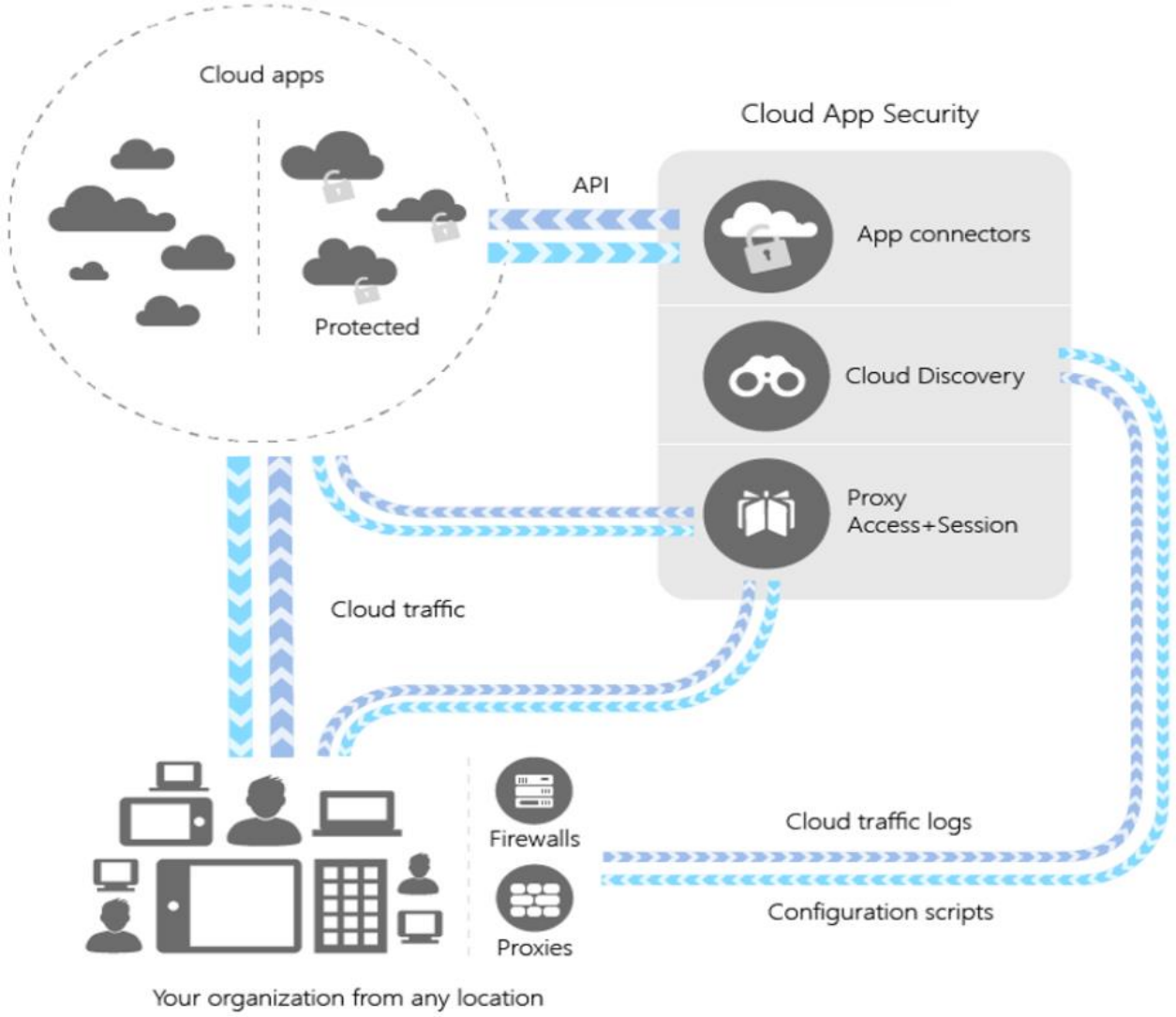
- **Discover and control the use of Shadow IT**: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 16,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.

- **Protect your sensitive information anywhere in the cloud**: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real-time across all your cloud apps.

- **Protect against cyberthreats and anomalies**: Detect unusual behavior across cloud apps to identify ransomware, compromised users or rogue applications, analyze high-risk usage and remediate automatically to limit the risk to your organization.

- **Assess the compliance of your cloud apps**: Assess if your cloud apps meet relevant compliance requirements including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps, and limit access to regulated data.

MCAS Architecture



Protection across the attack kill chain