ZERO TRUST SECURITY

Microsoft 365

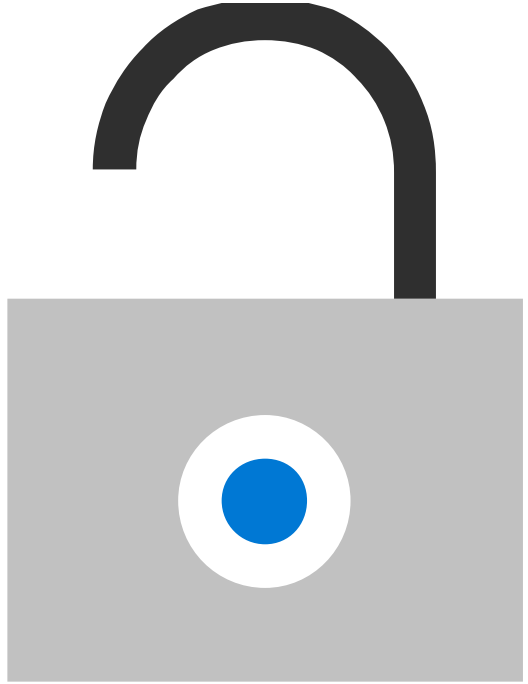
JASCO

Why Security is Relevant to You

- **33%** of Australian Businesses have experienced cybercrime with an average cost of **$276,000** (23 to 51 days to recover). ^

- COVID has resulted in an unprecedented adoption of cloud services – functionality taking precedence over security.

- Many businesses have not addressed the changes to the security landscape.



^ Australian Government – Department of Communications - https://www.communications.gov.au/sites/default/files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf

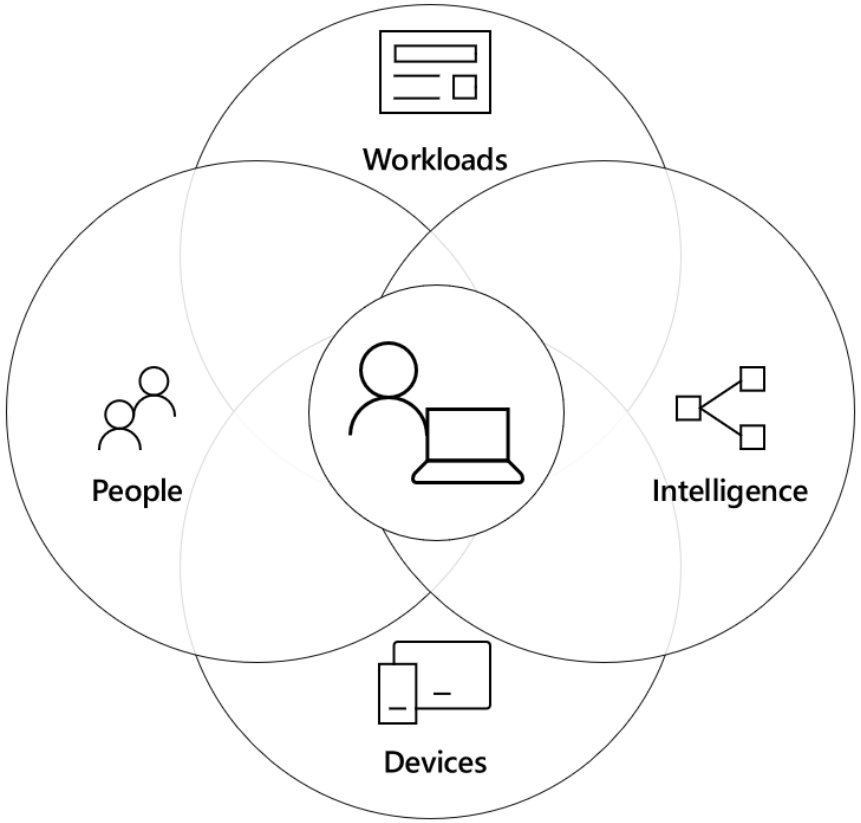
Agenda

Today we will:

- Discuss what Zero Trust is and explore its key components
- Review Microsoft's solutions to these modern threats and challenges
- Present some of Jasco's security offerings powered by the Microsoft engine

MODERN SECURITY

What is Zero Trust?



Principals

- Verify explicitly
- Least privileged access
- Assume breach

Components

- Identity
- Devices
- Applications
- Data
- Infrastructure
- Network

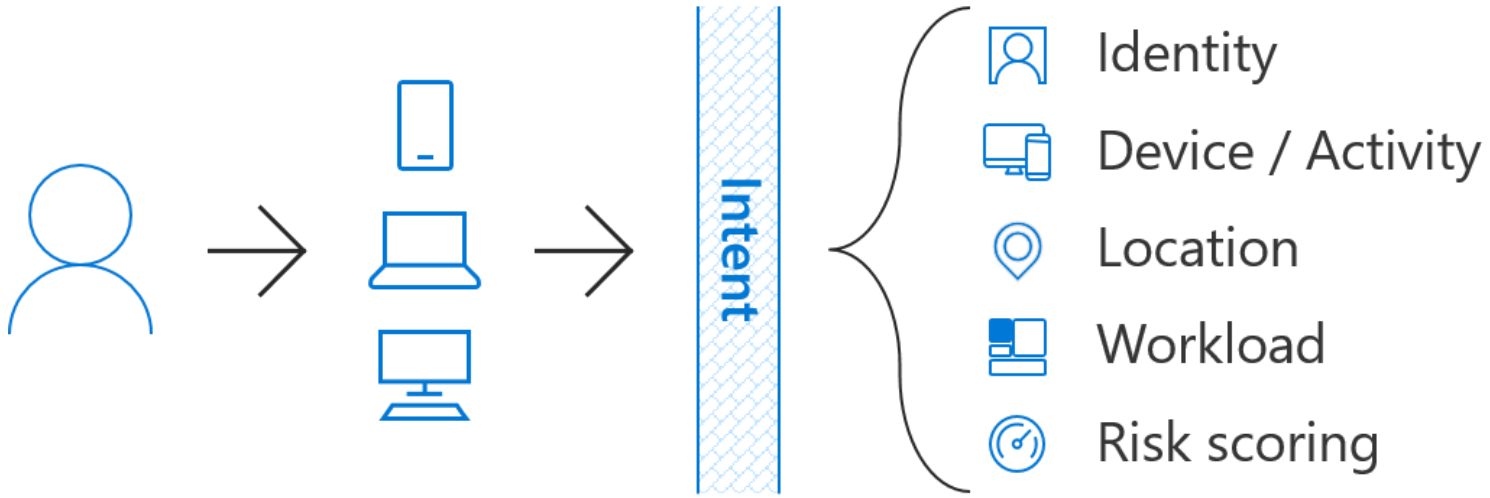
Why is Identity important?

CLOUD!!!

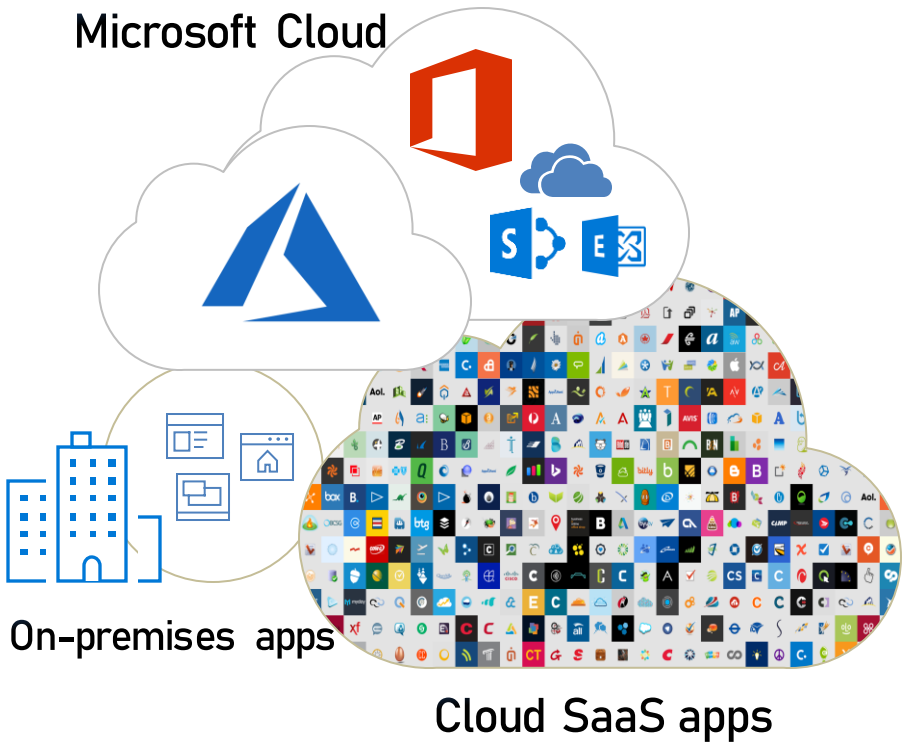
- The security boundary is no longer the firewall
- Is the first line of defence in a cloud first world
- Aligned with every sign-in, application or data transaction, and defines privilege

Devices

- Remote work demands greater levels of control, access, and device management
- Traditional device management solutions do not reach past the (old) security boundary
- Key to facilitating a successful and secure BYOD strategy



Applications



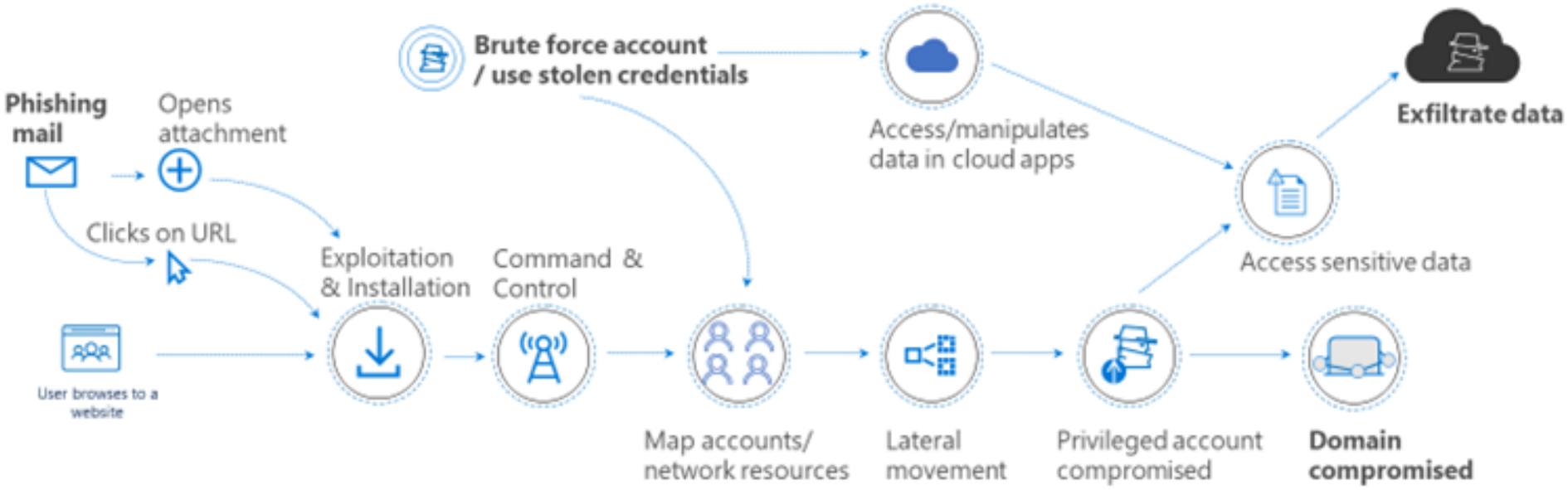
- Shadow IT is often an important but invisible risk to the business
- Unsanctioned apps pass on their own insecurities to the business
- May impact upon regulatory compliance responsibilities

Data

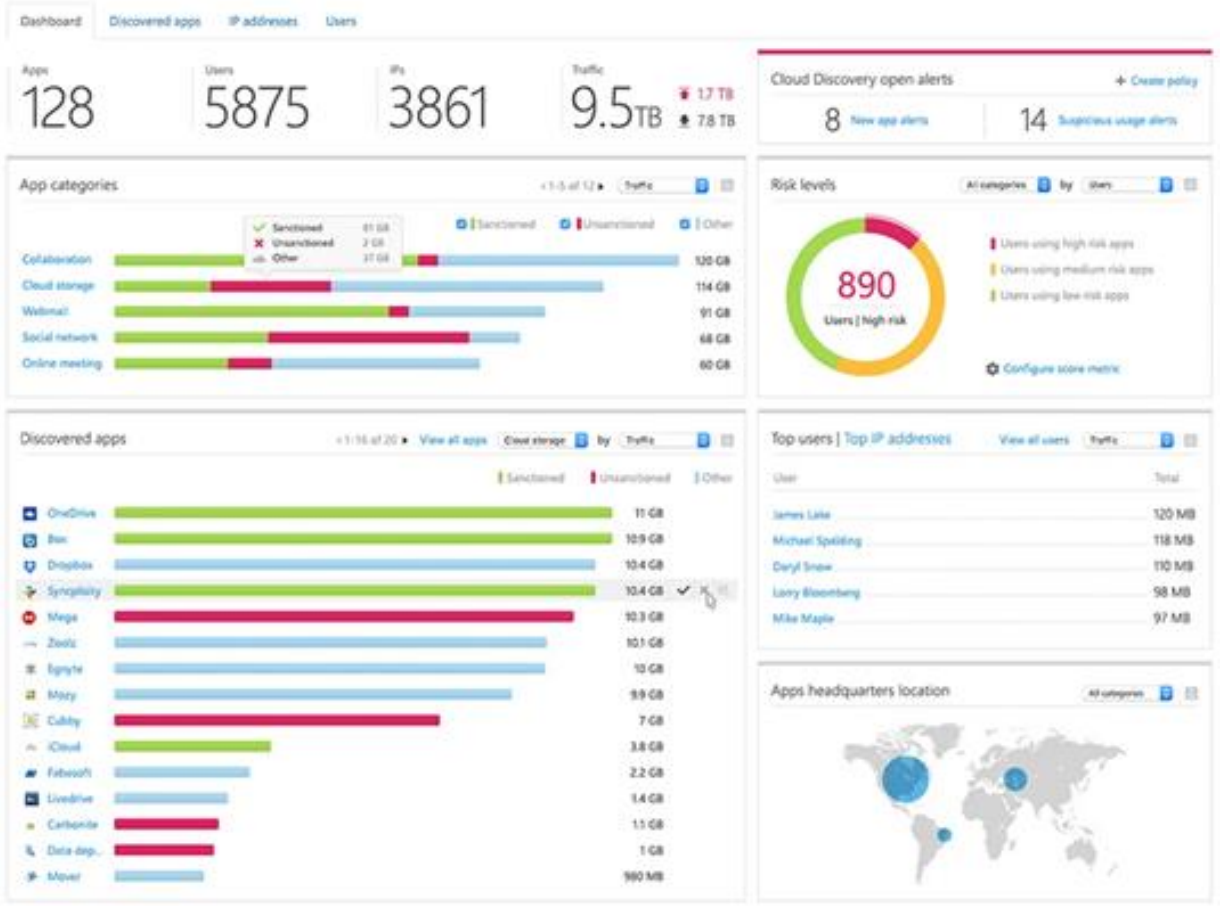
- Corporate data is the life blood of a business
- Leakage of sensitive information may result in stolen IP, fines due to non-compliance, and impact to company brand

External Threats

- Malware
- Email threats
- Credential theft and infiltration
- Ransomware



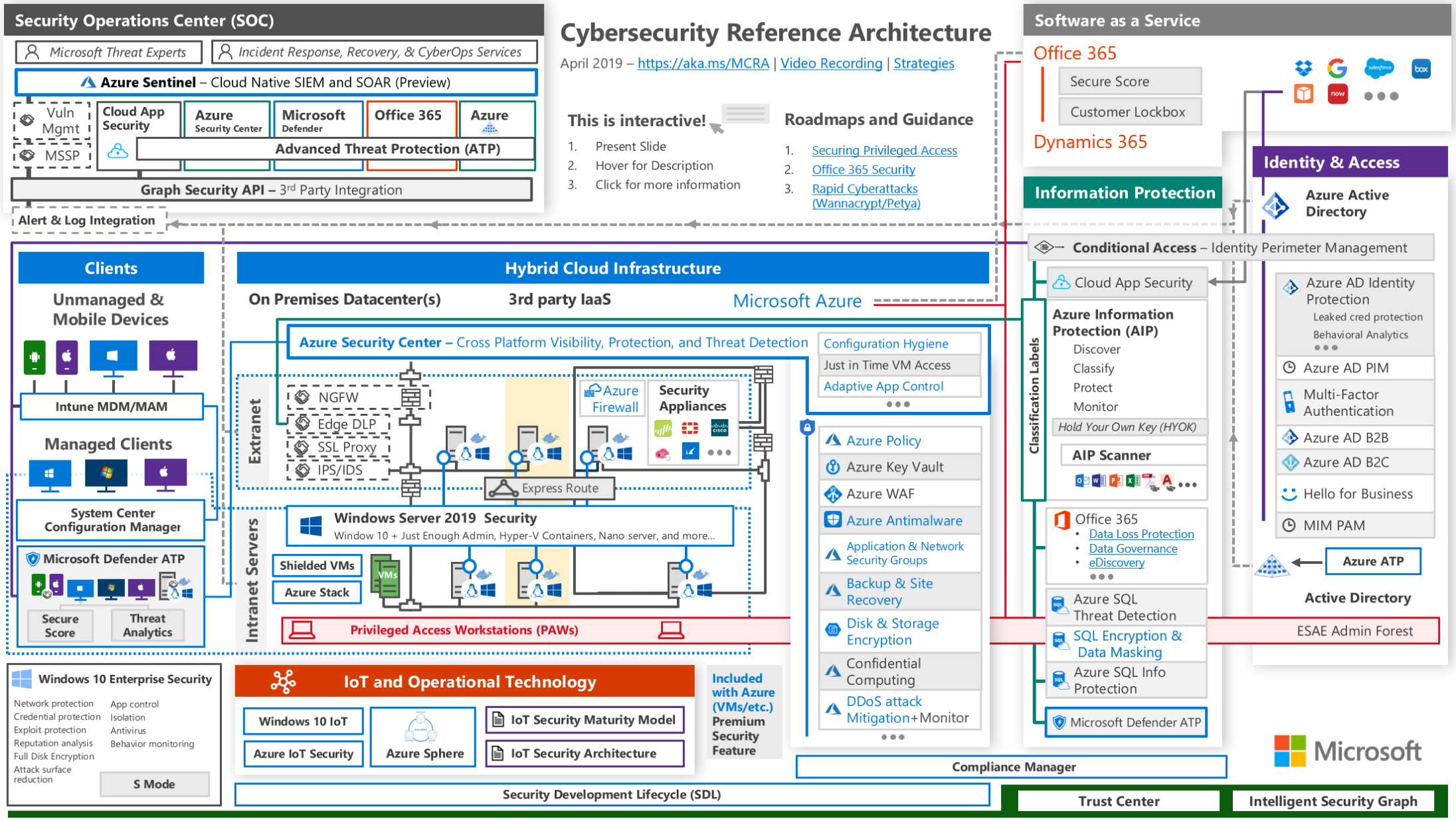
Internal Threats



- Data and IP Leakage
- Malicious insiders
- Shadow IT
- Unsecure Devices

MICROSOFT SOLUTIONS

Microsoft's Security Architecture



Azure Active Directory (AAD)

- Single sign-on simplifies access to your apps from anywhere
- A single identity platform lets you engage with internal and external users more securely
- Gartner recognised access management leader in 2020 ^

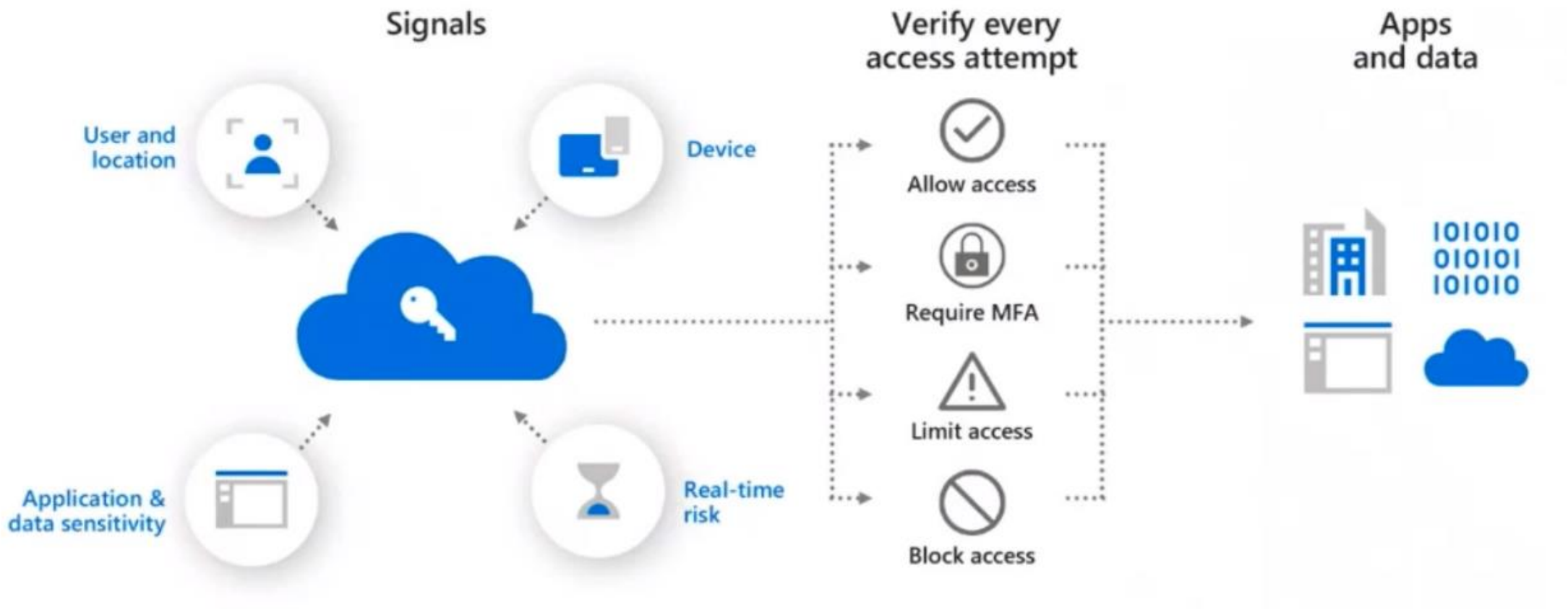
^ Gartner - https://www.gartner.com/doc/reprints?id=1-24F36V24&ct=201021&st=sb

Multi Factor Authentication

- Remove the insecurities of outdated password management processes.
- MFA (or 2FA) secured accounts are 99.9% less likely to be compromised. ^
- Protect access to resources using three key principles

^ Microsoft Corporation - https://www.microsoft.com/en-au/security/business/identity/mfa

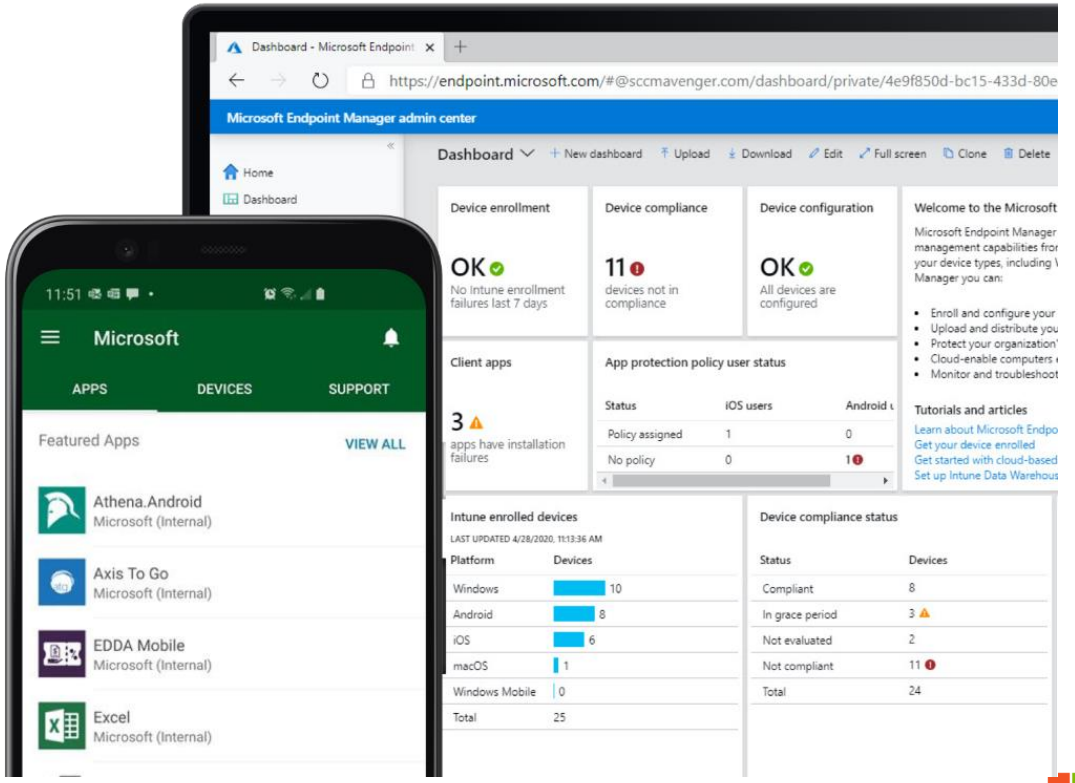
Conditional Access



Microsoft Endpoint Manager

Formerly known as Intune

- Centrally manage your fleet of workstations and mobile devices regardless of their locations
- Extend on-premises Configuration Manager capabilities to the cloud
- Provision new corporate devices from anywhere
- Introduce a BYOD strategy securely

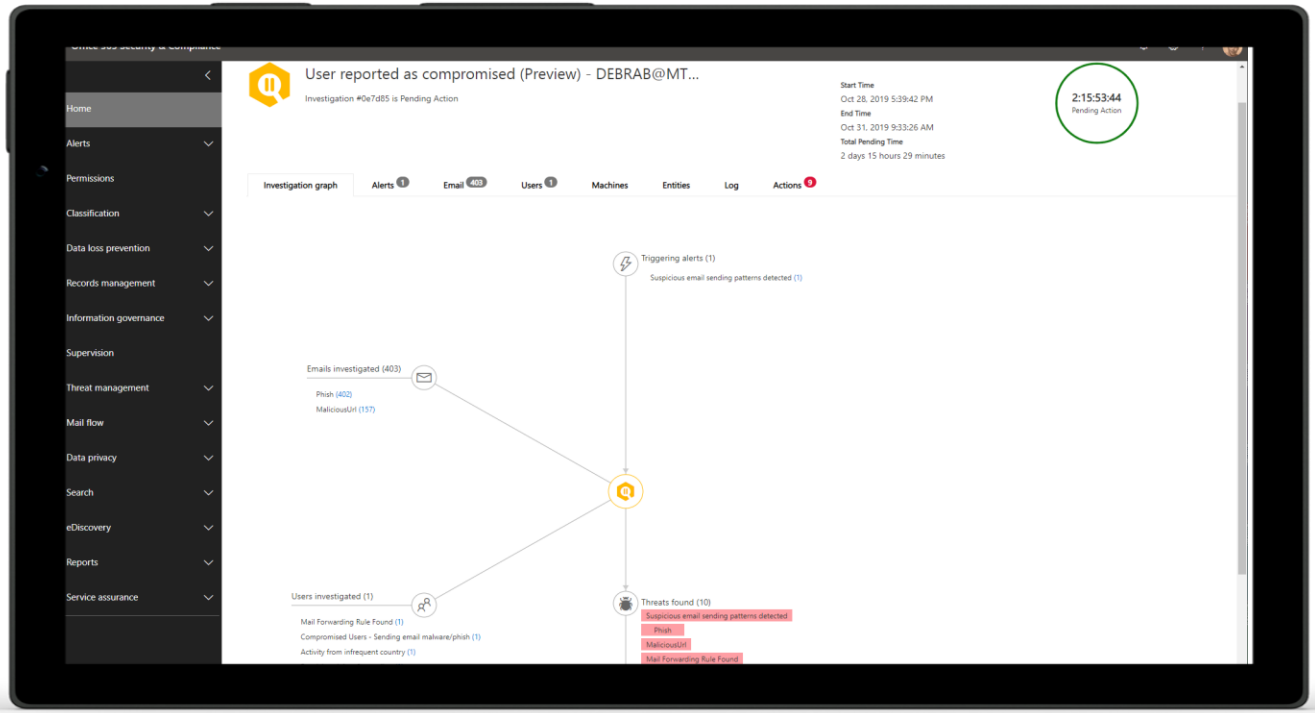


Exchange Online Protection

- Reputation Filtering
- Spam and Spoof protection
- Anti-Malware
- Content Filtering
- Zero Hour Auto-purge

Microsoft Defender for Office 365 (MDO)

Formerly Office 365 Advanced Threat Detection (O365 ATP)

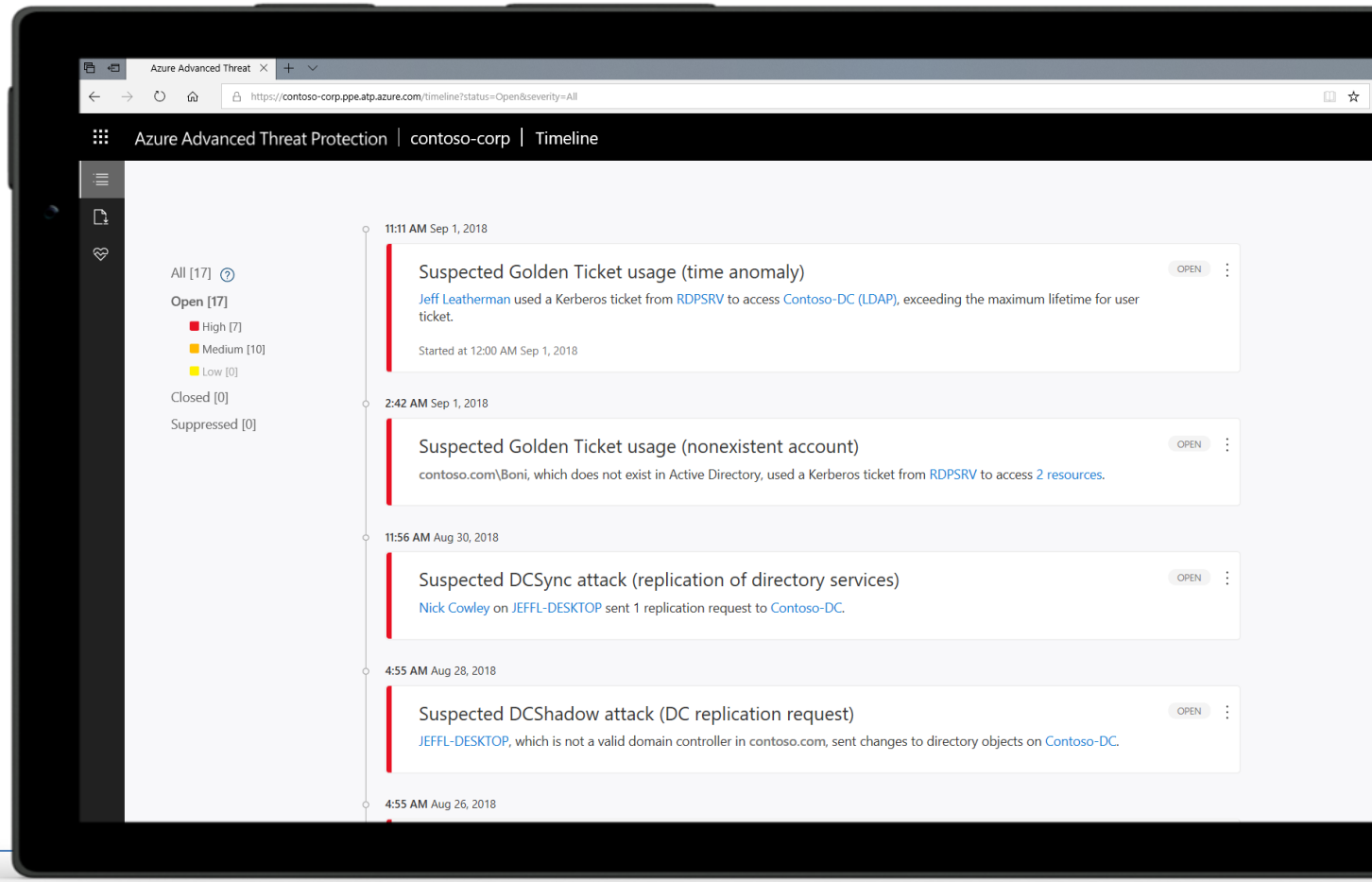


- Exchange Online Protection features.
- Zero Day attack defence.
- Content Filtering and Anti-Malware for Teams, SharePoint, and OneDrive.
- Email and Password Attack Simulation.

Microsoft Defender for Identity (MDI)

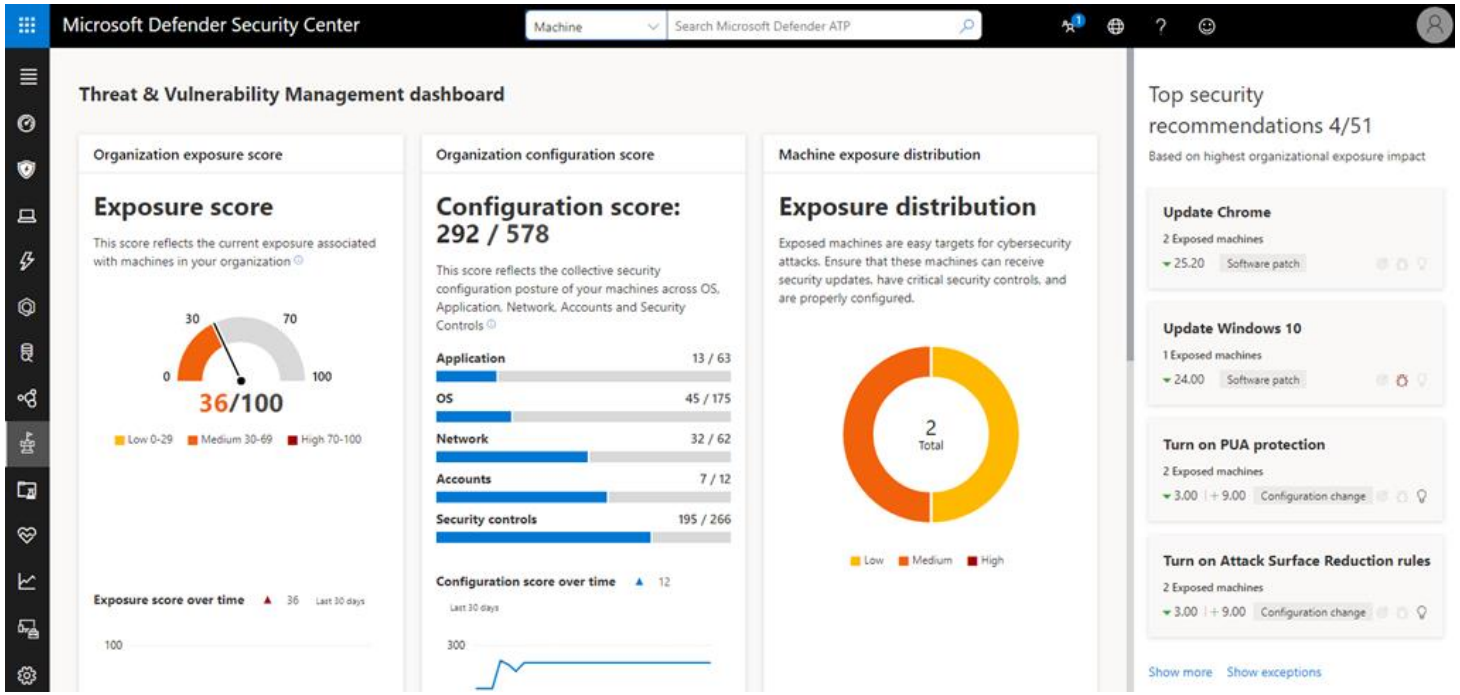
Formerly Azure Advanced Threat Detection (Azure ATP)

- Protect against identity compromise
- Prioritised information to focus on real threats
- Identify vulnerabilities before attacks happen



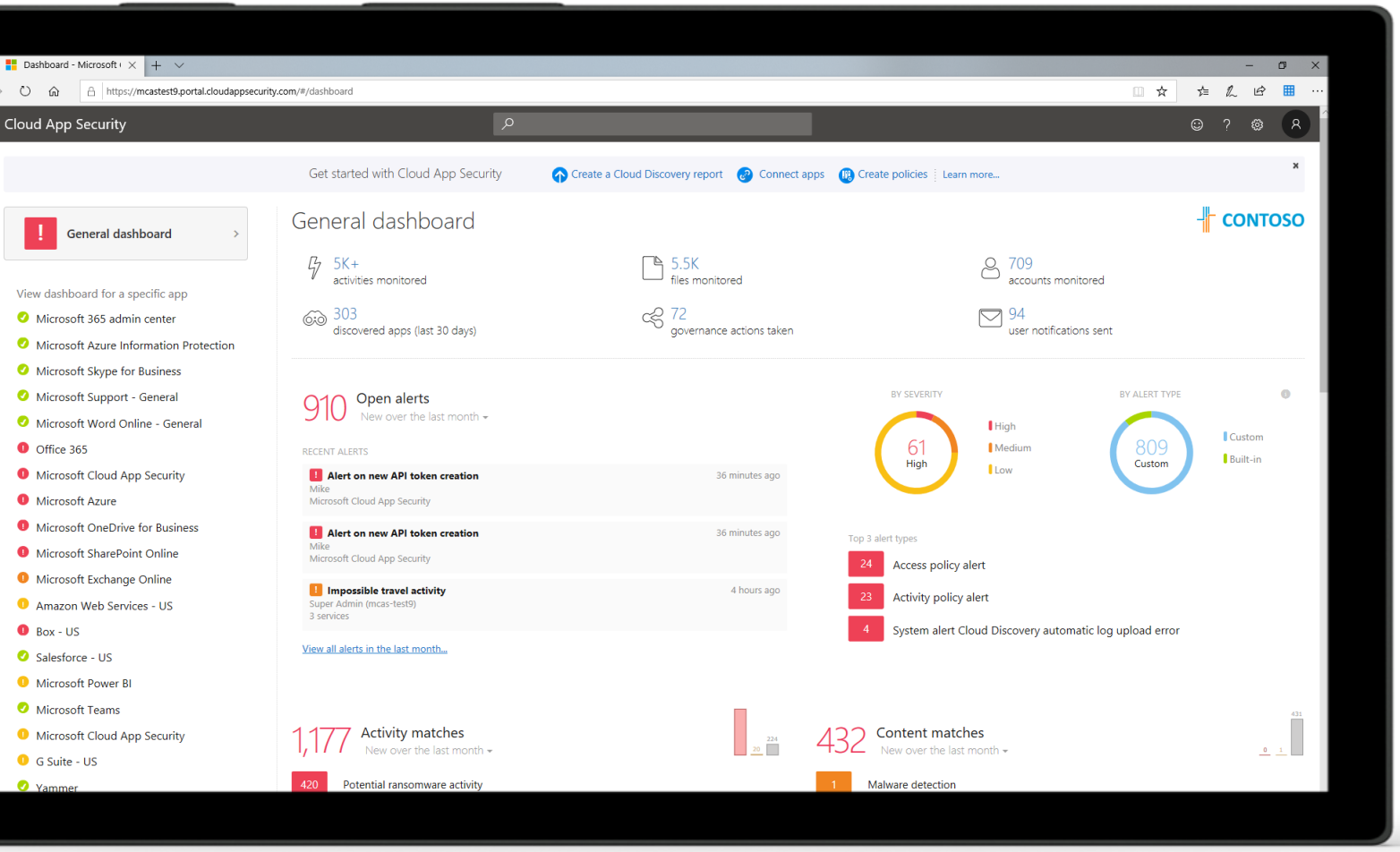
Microsoft Defender for Endpoint (MDE)

Formerly Windows Defender Advanced Threat Detection (Windows ATP)



- Endpoint detection and response
- Threat and vulnerability management
- Automated investigation and remediation
- Next generation protection and attack surface reduction

Microsoft Cloud App Security (CAS)

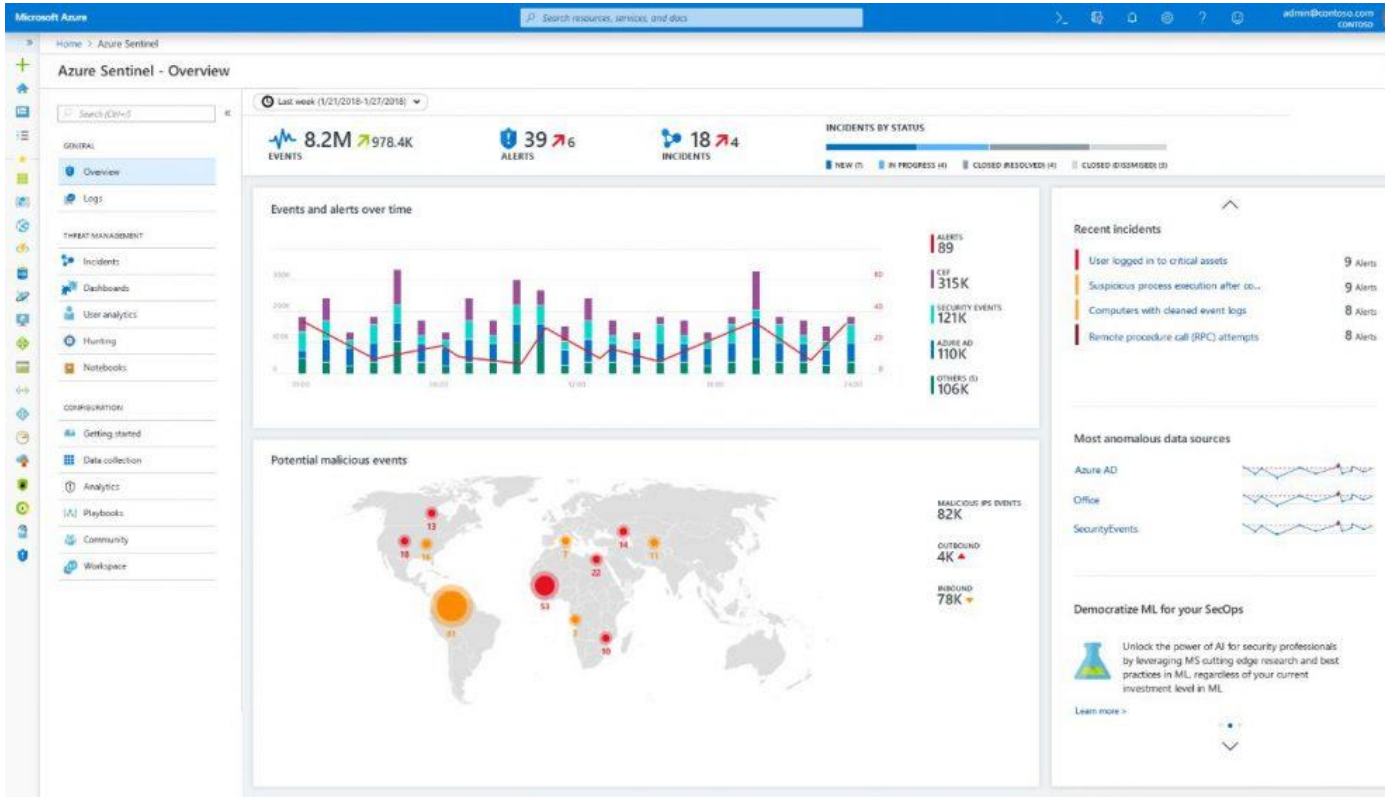


- Centralize and control cloud app activity
- Discover Shadow IT and enforce policies to manage cloud usage.
- Protect your sensitive information anywhere in the cloud.
- Assess the compliance of your cloud apps.

Microsoft Sentinel

Security Event and Incident Management (SEIM) and Security Orchestration and Response (SOAR)

- Gathers security events across multiple platforms
- Related events are collated into incidents for review and correction
- Uses configured policies and machine learning to automate corrective action



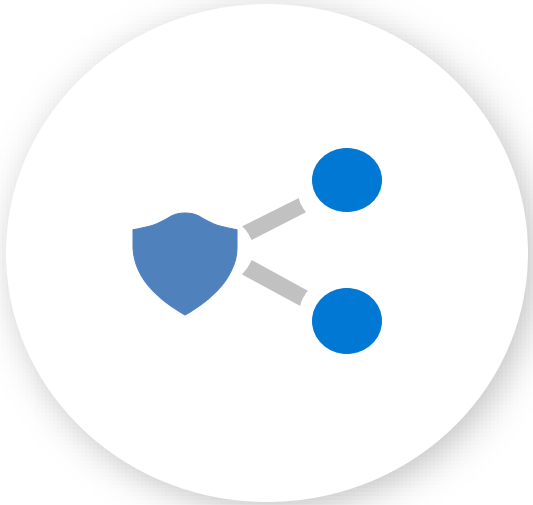
JASCO OFFERINGS

Jasco's Flexible Approach

- Not every Business is the same
- Tiered offerings to address customers of multiple profiles
- Consultancy and Tailoring!!!

Tier 1 – Security Essentials

Providing visibility for Identities, Users, and Devices without borders



Objectives

- Protect against common external threats.
- Ruin Attacker's Return on Investment (AROI).
- Provide visibility of your security standing and security events.

Components

- Modern Authentication - Multi Factor Authentication and Conditional Access
- Device management and security - Windows Defender, Log Analytics, Endpoint Manager
- Spam, Phishing, and Malware protection - Exchange Online Protection
- Office 365 Access Control and Reporting – Conditional Access App Enforced Restrictions

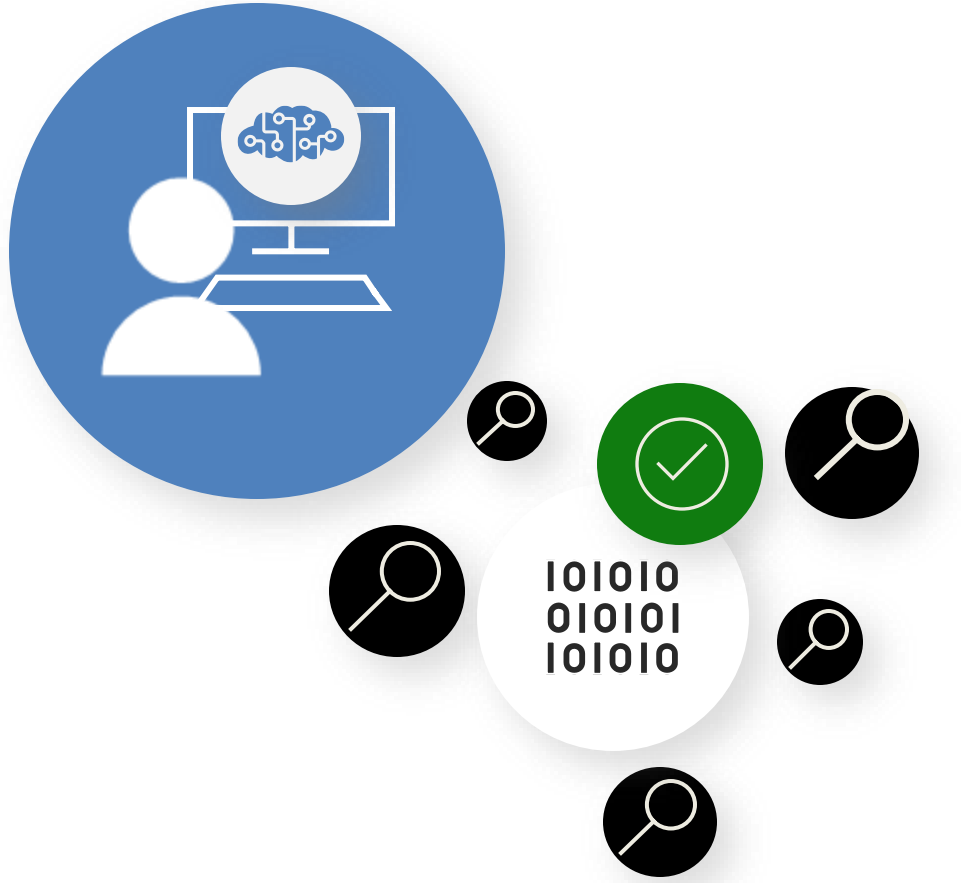
Tier 2 – Security Enhanced

Adding enhanced Visibility, Protection, and Insider Risk Management

Objectives

In addition to Security Essentials:

- Protect email against zero-day attacks and educate staff on how to identify phishing attempts – Microsoft Defender for Office 365
- Track and understand non-standard behaviours using Heuristics and Machine Learning – Microsoft Defender for Identity
- Track, Isolate, and Automate compromise remediation – Microsoft Defender for Endpoint
- Remove Shadow IT risks – Microsoft Cloud App Security



Thank You