

Advanced Security

Michele Sensalari

Overnet Education

Trainer, Speaker, Consultant

michele.sensalari@overneteducation.it

michele@sensalari.com

Twitter: @ilsensa7

Linkedin: <https://www.linkedin.com/in/michele-sensalari-4988b7/>

Agenda

- Cybersecurity
- Identity Protection and Access Management
- Device Management and Protection
- Information Protection
- GDPR in M365
- Microsoft 365 Security & Compliance platform

Cybersecurity

Phishing

Account Breach

Elevation of Privilege

AgID

GDPR

Data Exfiltration

ISO 27001

Data Deletion

Spam & Malware

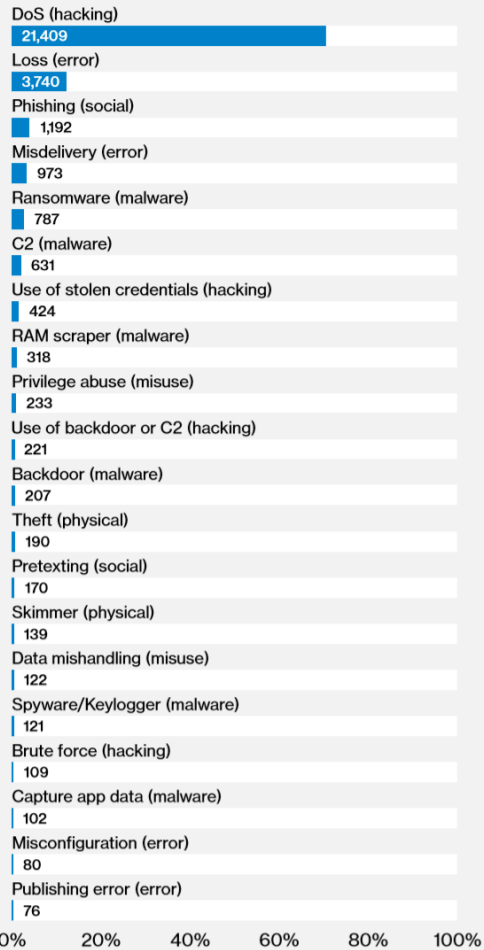
Ransomware

Data Spillage

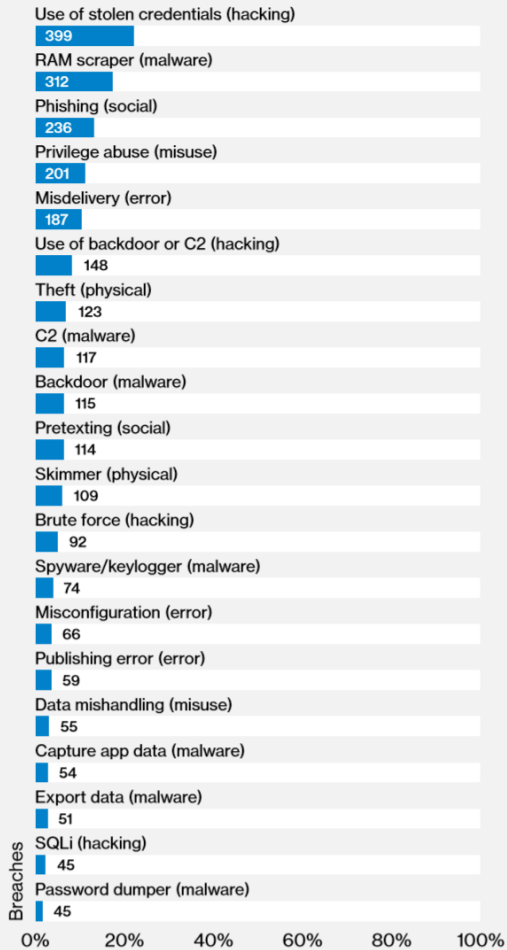
Cryptolocker

Cybersecurity Statistics

Top 20 action varieties in incidents



Top 20 action varieties in breaches



81% of hacking-related breaches leveraged either stolen and/or weak passwords.

32% of breaches involved phishing

66% of malware was installed via malicious email attachments.

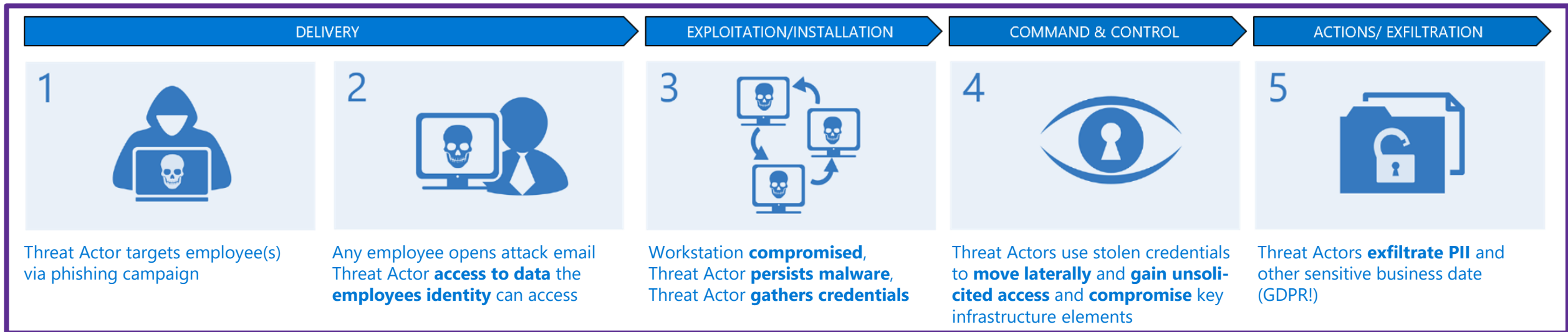
68% of breaches took months or longer to discover

58% of victims are categorized as small businesses

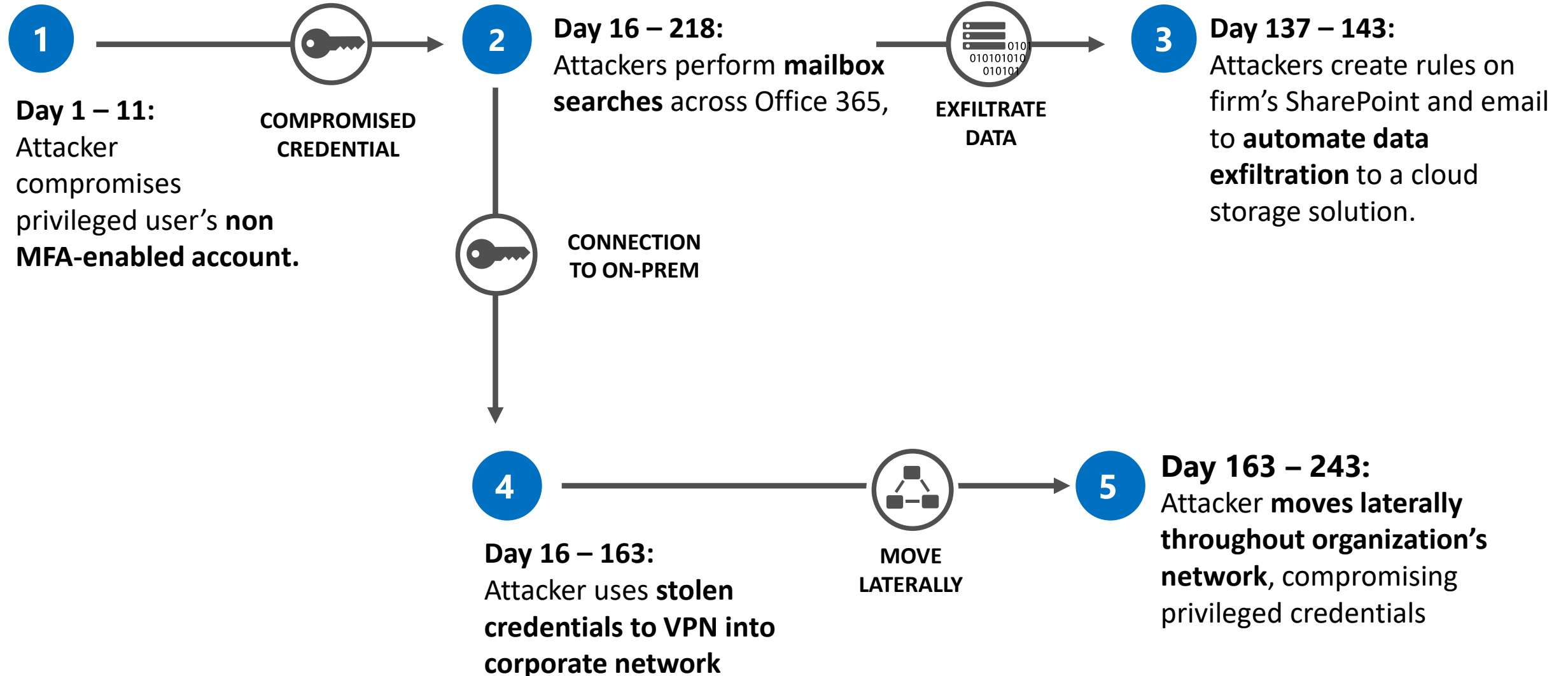
71% of breaches were financially motivated

Disrupting the Common Attack Playbook

Killchain Attack



Attack Timeline



Microsoft 365

Windows 10 + Office 365 + EMS

Enterprise Plans

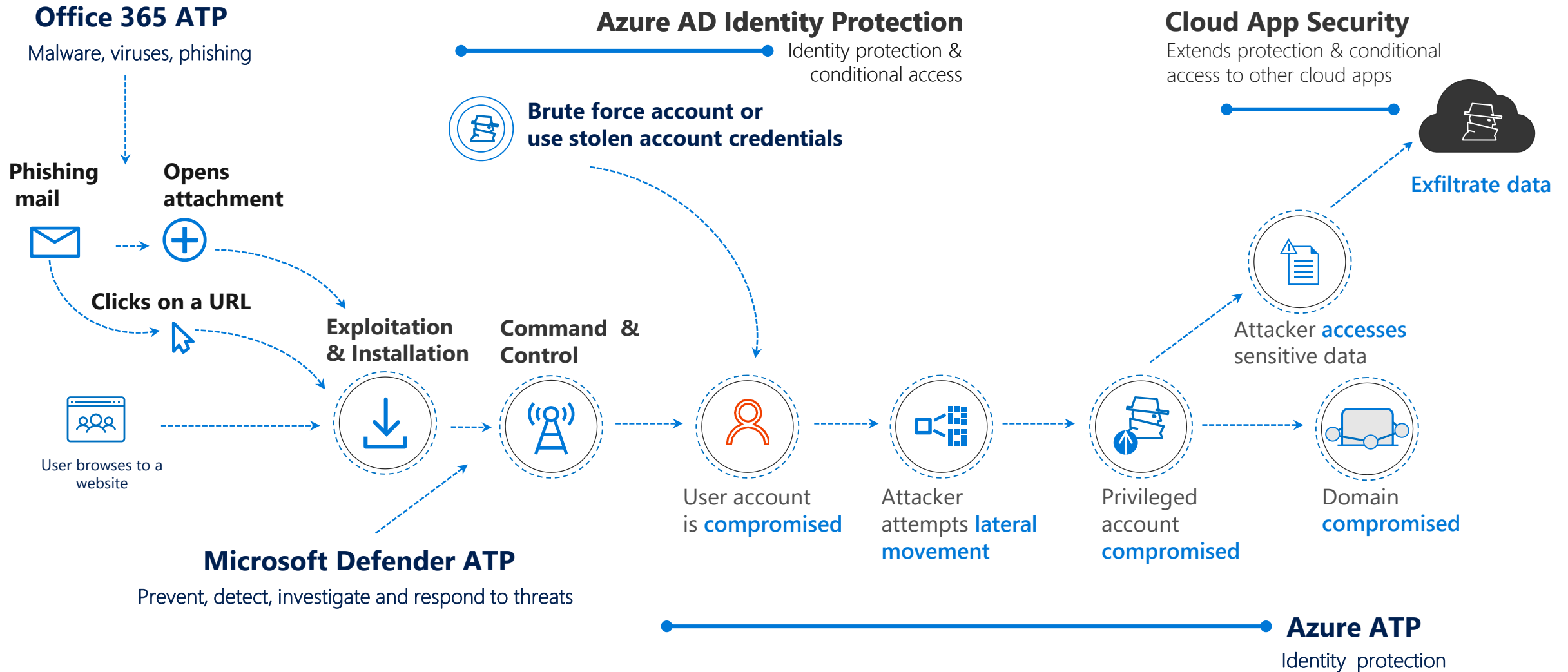
Microsoft 365 E3		
	Office 365 E3	EMS E3
Windows 10 Enterprise E3 Per User	Office Pro Plus for O365 SharePoint Online Plan 2 Exchange Online Plan 2 Skype for Business Online Plan 2 Yammer Office Online (Web Apps) OneDrive	Microsoft Intune Azure Active Directory Premium Plan 1 Azure Information Protection Premium Plan 1 Microsoft Identity Manager CAL Advanced Threat Analytics Windows Server CAL equivalency
Microsoft 365 E5		
<i>Contains everything in Microsoft 365 E3 and adds:</i>		
	Office 365 E5 Additive Features	EMS E5 Additive Features
Windows Defender ATP	Threat Intelligence Advanced Threat Protection Advanced Security Management Advanced Compliance (Advanced eDiscovery, Customer Lockbox, Advanced Data Governance) Audio Conferencing Phone System Power BI Pro MyAnalytics	Cloud App Security Azure Active Directory Premium Plan 2 Azure Information Protection Premium Plan 2

SMB Plan

Microsoft 365 Business

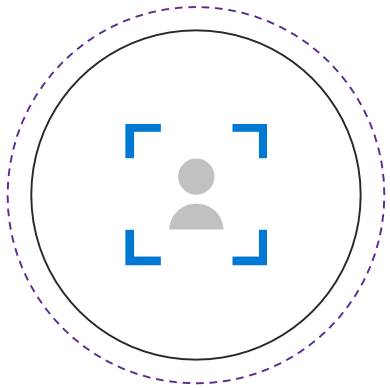
- Office 365 Business
- Azure AD P1 (only some feature): MFA (Multi Factor Authentication, SSPR (Self Service Password Reset), Conditional Access
- Windows 10 Professional (only upgrade from 7, 8.1 Professional)
- Office 365 ATP
- Data Loss Prevention
- Exchange Online Archiving (eDiscovery, Litigation Hold, Retention Policy)
- Azure Information Protection
- Intune (Windows 10, iOS, Android)

Maximize detection during attack stages



Microsoft Threat Protection

Protect, detect, respond



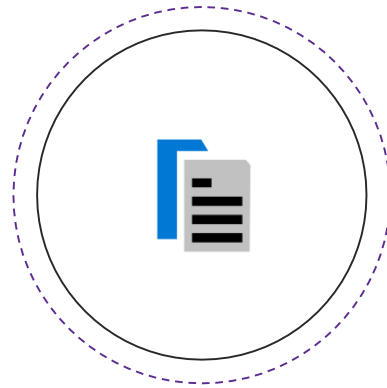
Identities

Users and Admins



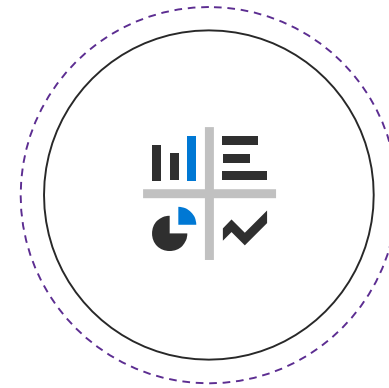
Endpoints

Devices and Sensors



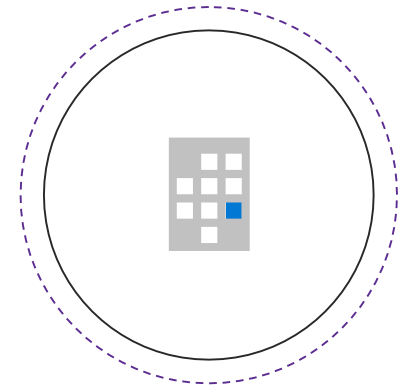
User Data

Email messages and documents



Cloud Apps

SaaS Applications and Data Stores

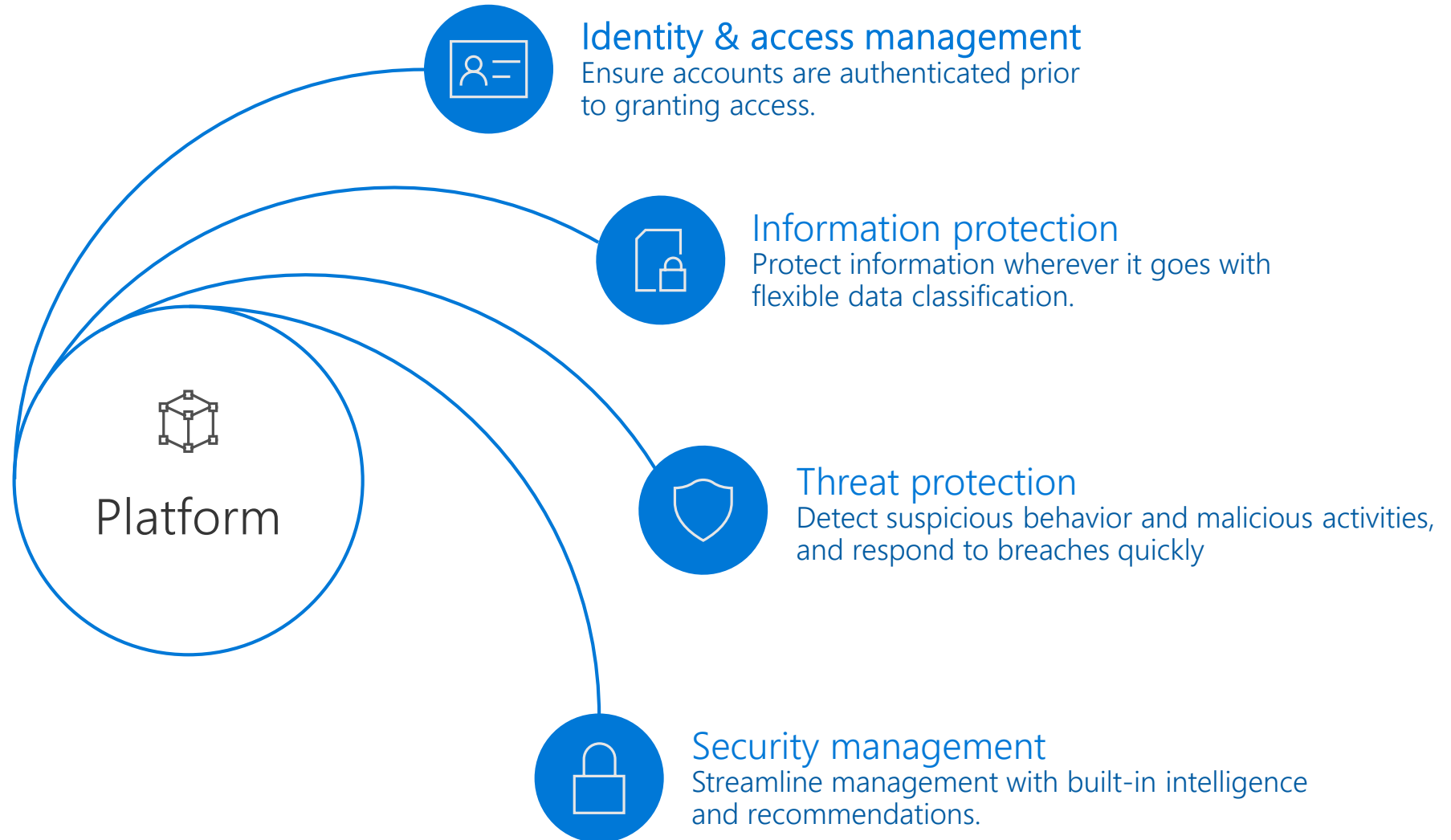


Infrastructure

Servers, Virtual Machines, Databases, Networks

Intelligent Security Graph | 6.5 TRILLION signals per day

Built in security in Microsoft 365

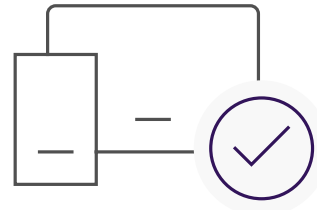


Identity & Access Management

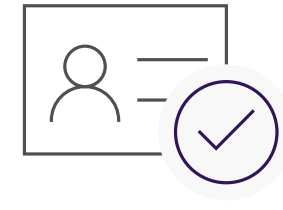
Prove users are authenticated, authorized and secure before granting access to apps, data, and devices



Password-less Authentication



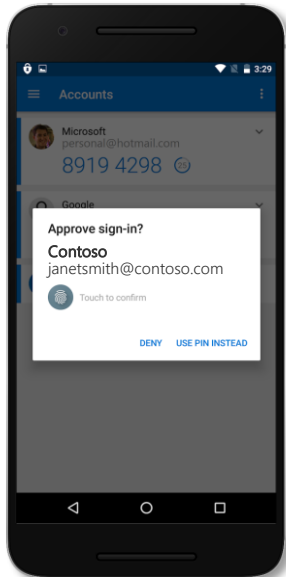
Conditional Access



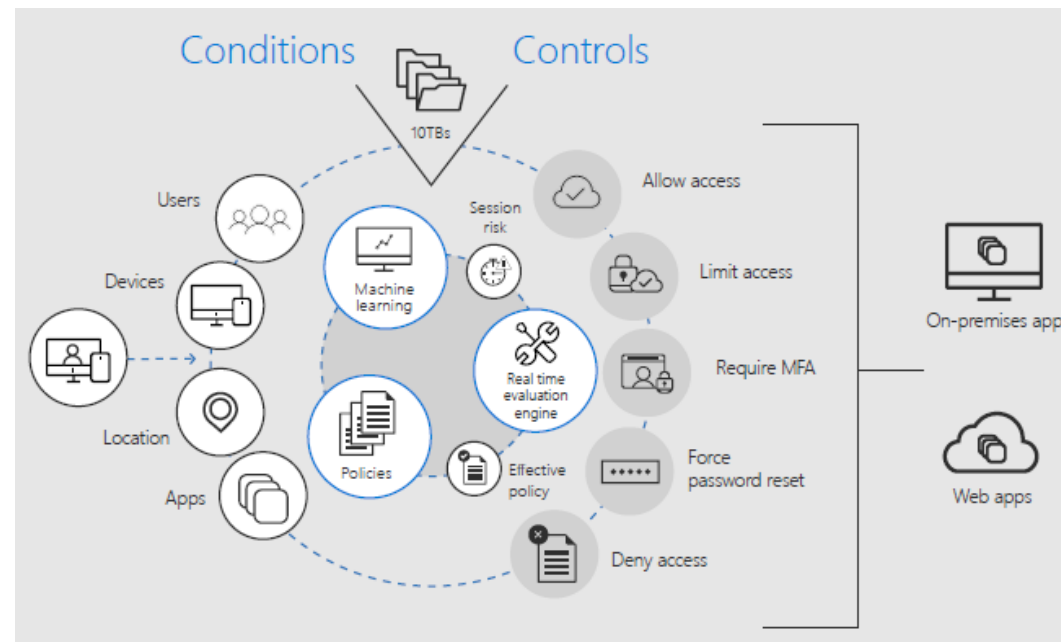
Identity Protection



Windows Hello



MS Authenticator



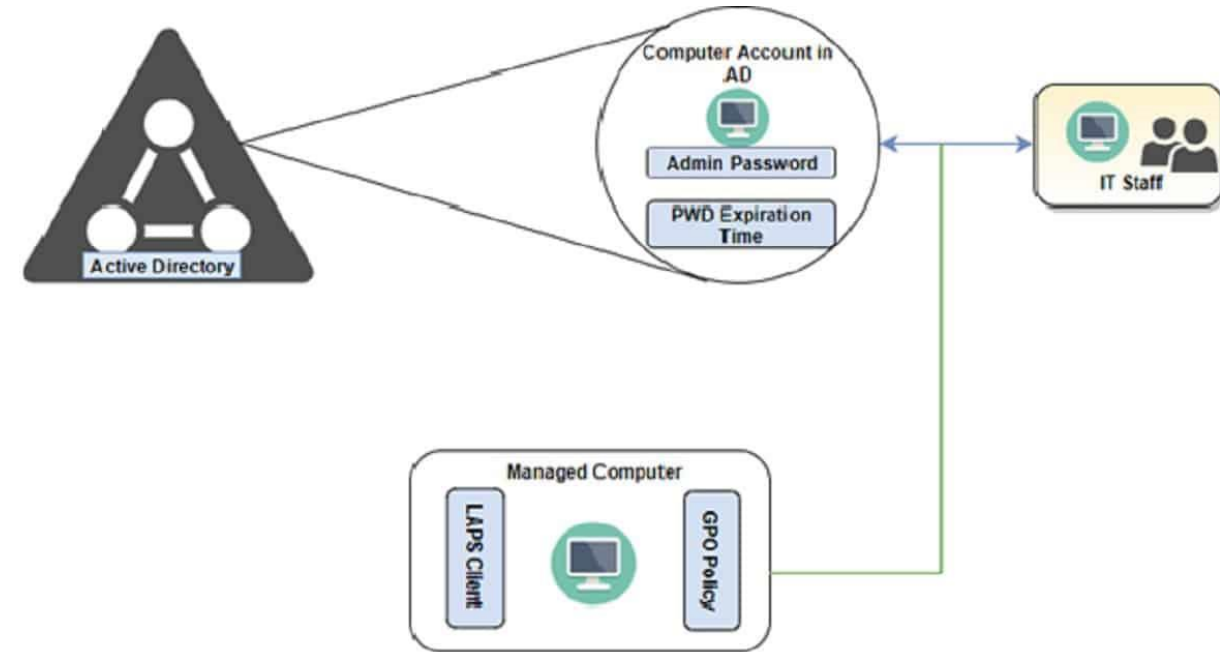
Safeguard credentials when they are used in an OS or application session



Local Administrator Password Solution

Microsoft Local Administrator Password Solution (LAPS) is a free password manager tool that utilizes Active Directory to manage passwords for local administrator account across all of your Windows clients and servers.

LAPS is a mitigation tool against lateral movement and privilege escalation, by forcing all local administrator account to have unique, complex passwords, so an attacker compromising local administrator account can't move laterally to other endpoints that may share that same password



General	Operating System	Member Of	Delegation	Password Replication	
Location	Managed By	Object	Security	Dial-in	Attribute Editor
Attributes:					
Attribute	Value				
msImaging-HashAlgorithm	<not set>				
msImaging-ThumbprintHash	<not set>				
ms-Mcs-AdmPwd	j09jX\ubt\u1.R				
ms-Mcs-AdmPwdExpirationTime	130797069158476163				
mSMQDigests	<not set>				
mSMQDigestsMig	<not set>				
mSMQSignCertificates	<not set>				
mSMQSignCertificatesMig	<not set>				
msNPAllowDialin	<not set>				
msNPCallingStationID	<not set>				
msNPSavedCallingStationID	<not set>				
msPKIAccountCredentials	<not set>				
msPKI-CredentialRoamingTokens	<not set>				
msPKIDPAPIMasterKeys	<not set>				

The screenshot shows the LAPS UI with the following fields and values:

- ComputerName: [text box]
- Password: [text box]
- Password expires: 15/10/2016 12:00:43
- New expiration time: 22 September 2016 23:17:33

Buttons: Search, Set, Exit

Windows Defender Credential Guard

WDCG is a security feature in Windows 10 Enterprise and Windows Server 2016/2019 that uses virtualization-based security to protect your credentials usually stored in LSASS cache memory. With Credential Guard enabled, only trusted, privileged applications and processes are allowed to access user secrets, or credentials

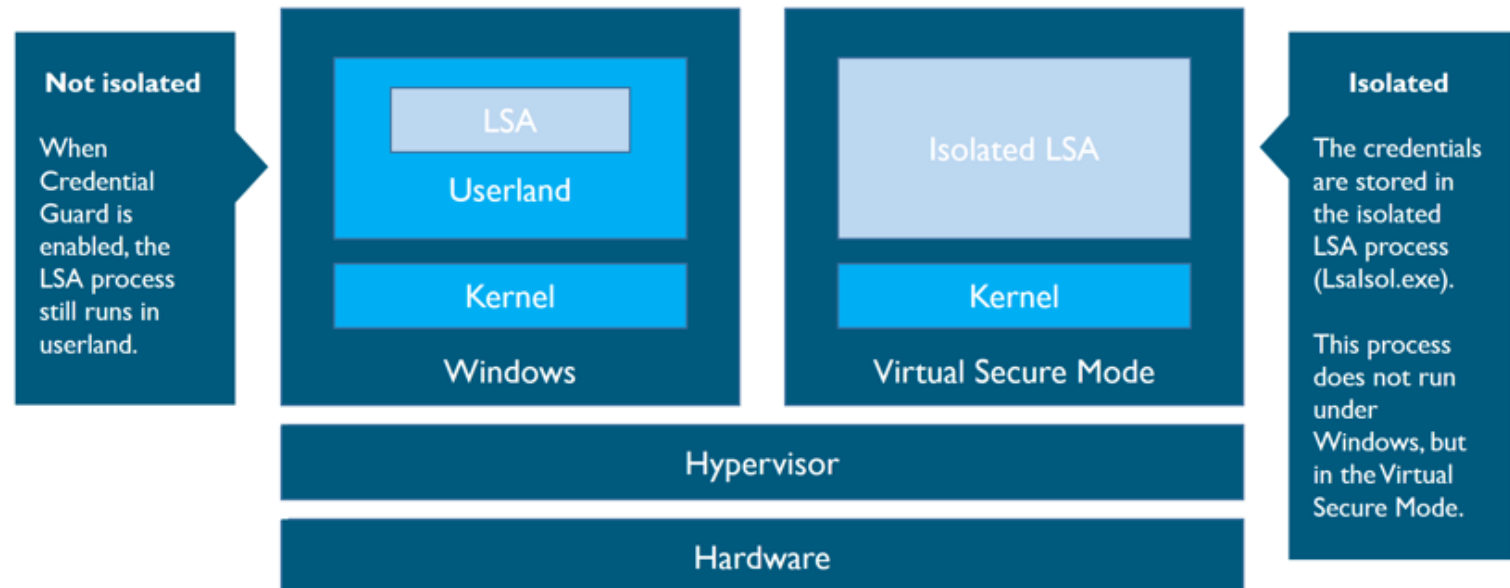
```
Authentication Id : 0 ; 233728 (00000000:00039100)
Session          : Interactive from 1
User Name       : administrator
Domain         : CONTOSO
Logon Server    : DC
Logon Time      : 5/24/2017 1:18:59 AM
SID            : S-1-5-21-1469689841-4213604591-3442953207-500

msv :
[00000003] Primary
 * Username : Administrator
 * Domain   : CONTOSO
 * NTLM     : eaa4bb35b0e582b247335bcbb5dea412
 * SHA1     : e3d927ff20f3b587df63b8388122d49b59d1b36e
 * DPAPI    : 1e19849f813cebb2e907762030a999b2

tspkg :
wdigest :
 * Username : Administrator
 * Domain   : CONTOSO
 * Password : (null)

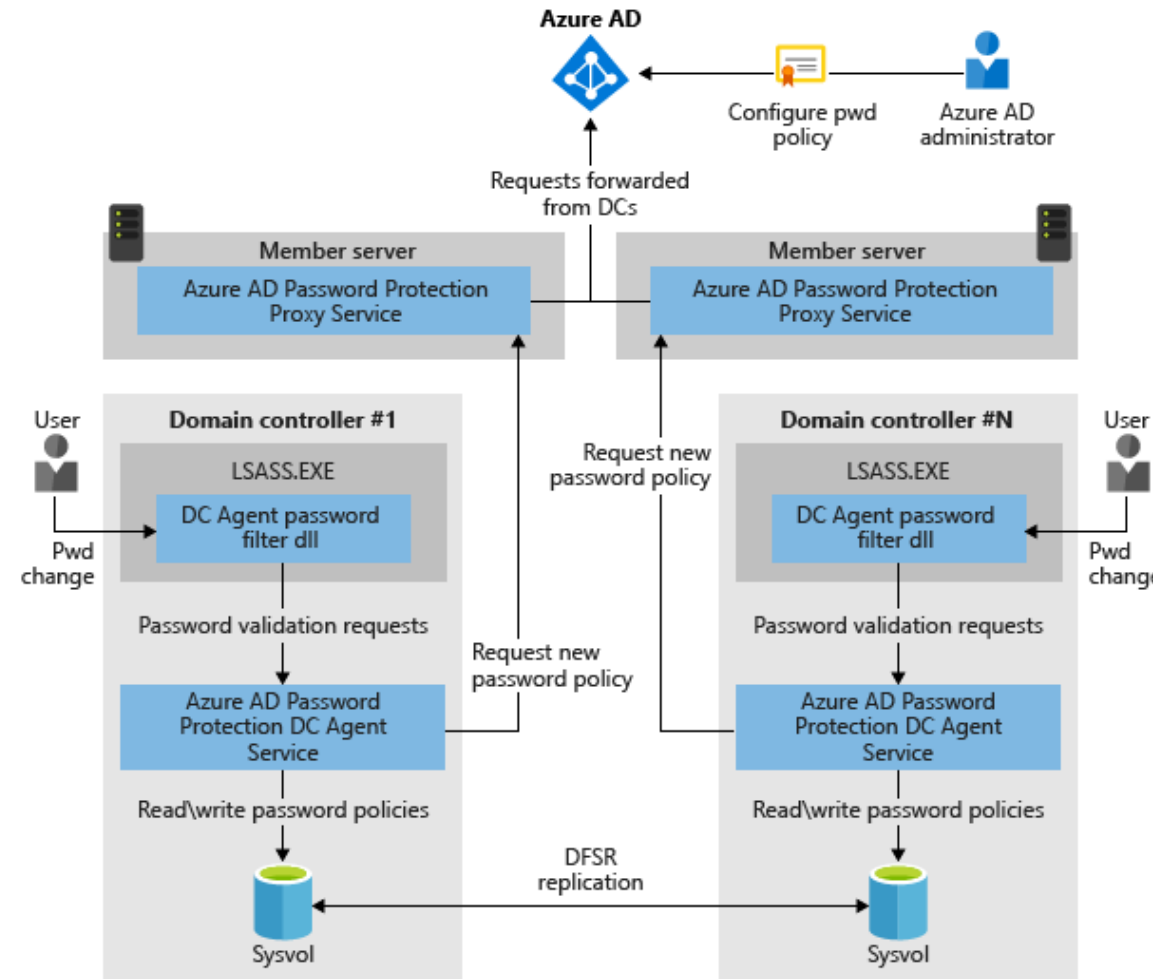
kerberos :
 * Username : Administrator
 * Domain   : CONTOSO.COM
 * Password : (null)

ssp :
credman :
```



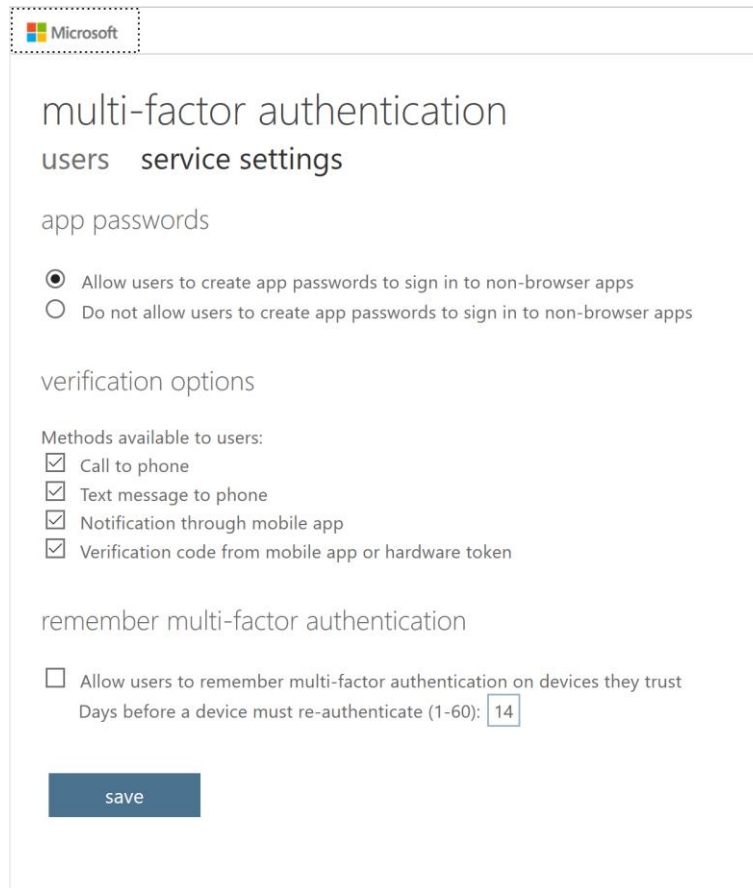
Azure AD Password Protection

- ✓ Hackers use brute force techniques like password spray attacks to discover and compromise accounts with common passwords.
- ✓ Azure AD Password Protection helps you eliminate easily guessed passwords from your environment, which can dramatically lower the risk of being compromised by a password spray attack
- ✓ Azure AD Password Protection also provides an integrated admin experience to control checks for passwords in your organization, in Azure and on-premises.
- ✓ Azure AD Premium Password Protection is an Azure AD Premium 1 feature
- ✓ Required: Azure AD password protection for Windows Server Active Directory



Multi-Factor Authentication

- ✓ Multi-factor Authentication (MFA) helps increase security by requesting users to provide a username and a password while signing in and then use a second authentication method.
- ✓ The second authentication method might be acknowledging a phone call, text message, or an app notification on their smartphone
- ✓ You can also enable users who authenticate from a federated, on-premises directory for multi-factor authentication.
- ✓ The tenant administrator enables MFA in the Microsoft 365 admin center



Microsoft

multi-factor authentication
users service settings

app passwords

Allow users to create app passwords to sign in to non-browser apps
 Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

Call to phone
 Text message to phone
 Notification through mobile app
 Verification code from mobile app or hardware token

remember multi-factor authentication

Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60):


save


You can reduce your odds of being compromised by up to 99.9% by implementing multi-factor authentication (MFA).


Source: Microsoft 2018 Security Research


MFA – Authentication Methods

Verify your identity

 Approve a request on my Microsoft Authenticator app

 Use a verification code from my mobile app

 Text +X XXXXXXXX40

 Call +X XXXXXXXX40

[More information](#)

Cancel

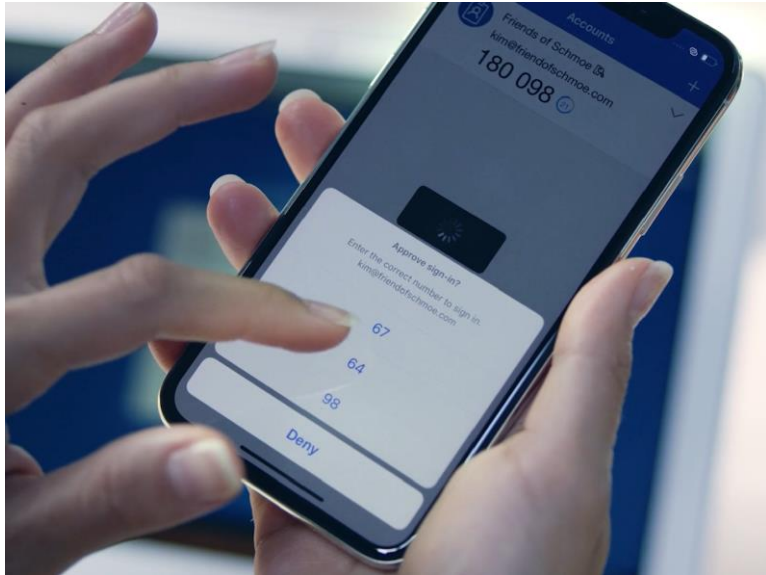
✓ MFA with Smartphone: SMS / CALL / Microsoft Authenticator APP

✓ MFA without Smartphones: OATH-certified hardware tokens

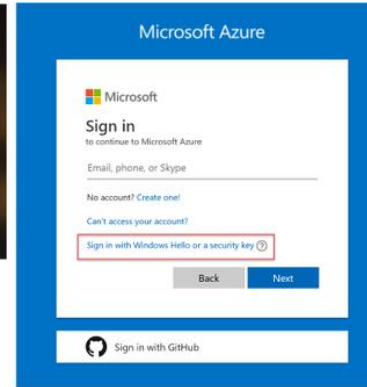
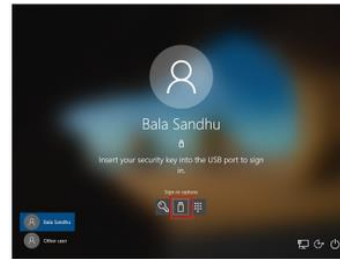
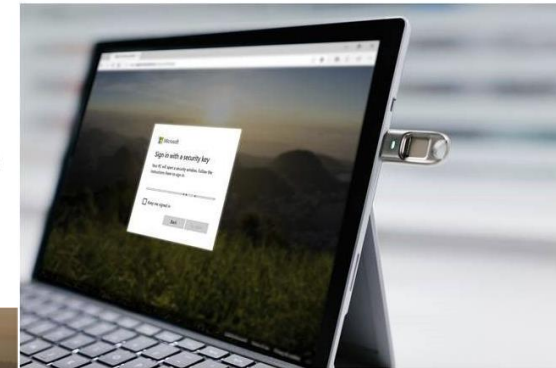


MFA: Password-less Authentication

Microsoft Authenticator passwordless signin



Fido2 Security Hardware



1. Send challenge
2. Provide user verification
User Auth Gestures
3. Sign and return challenge
FIDO2 Authenticator
4. Verify signed challenge
RP Server



Windows Hello for Business

✓ No passwords!

- ✓ Password-less, strong authentication
- ✓ On devices with TPM, multi-factor authentication
- ✓ Device with or without fingerprint reader or 3D camera

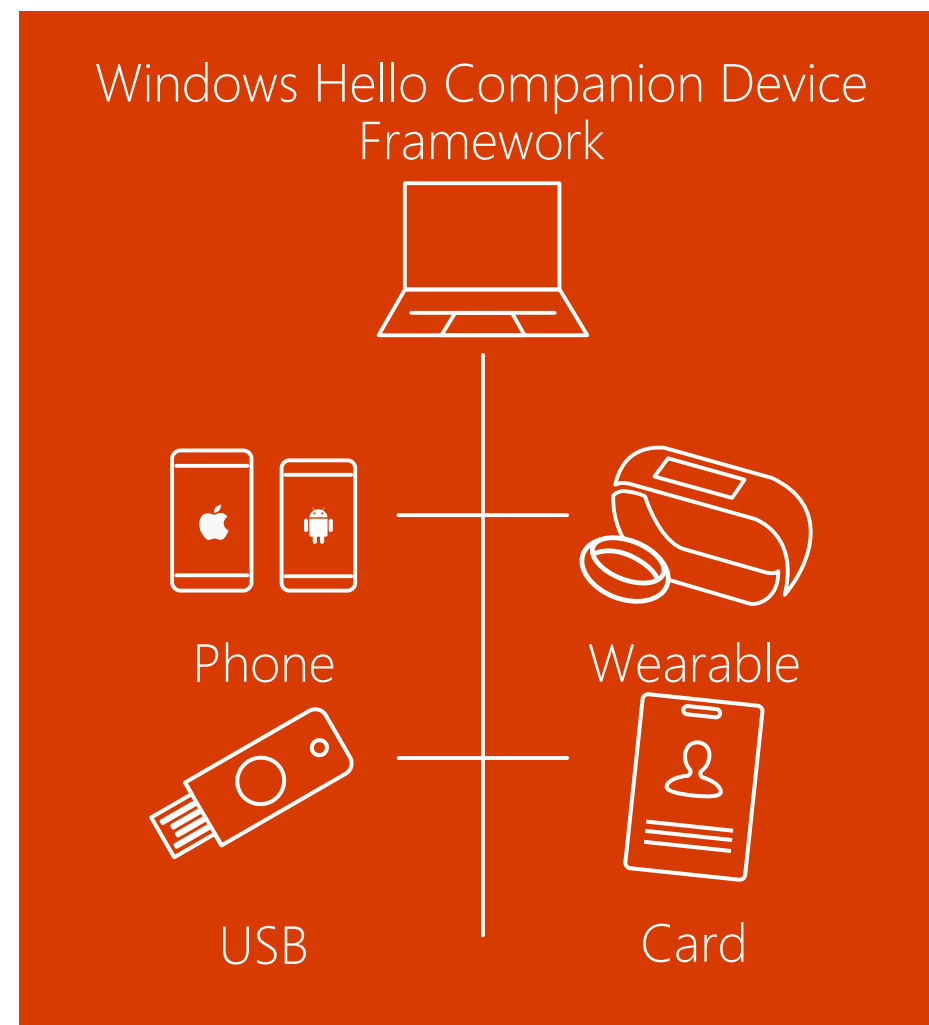
✓ Available for Windows 10

✓ Secure

- ✓ Credentials are protected by hardware

✓ Extensible

- ✓ The Windows Hello Companion Device Framework
- ✓ Possibilities for a wide array of devices



Azure AD Identity Protection

Azure AD Identity Protection introduces automatic, risk-based, conditional access to help protect users against suspicious logins and compromised credentials

- ✓ **Detection: Vulnerability and risky accounts are detected by:**
 - ✓ Highlighting vulnerability and providing custom recommendations
 - ✓ Calculating sign-in and user risk level
- ✓ **Investigation: Risk events are investigated are solved by:**
 - ✓ Notifications
 - ✓ The provision of relevant and contextual information
 - ✓ Basic workflows used in tracking
 - ✓ Easy access to remediation actions
- ✓ **Risk-based conditional access**
 - ✓ Risk-mitigation, such as blocking sign-ins or requesting multi-factor authentication
 - ✓ Blocking or security risky user accounts
 - ✓ Asking users to register for Azure MFA

Azure AD Identity Protection - Vulnerabilities

Sensalari Lab

RISK LEVEL	COUNT	VULNERABILITY
Medium		Users without multi-factor authentication registration (explore via Identity Secure Score)
Medium	2	Potential stale accounts in a privileged role (Preview)
Low	2	Administrators aren't using their privileged roles
Low	5	There are too many global administrators

GENERAL

- Overview
- Getting started

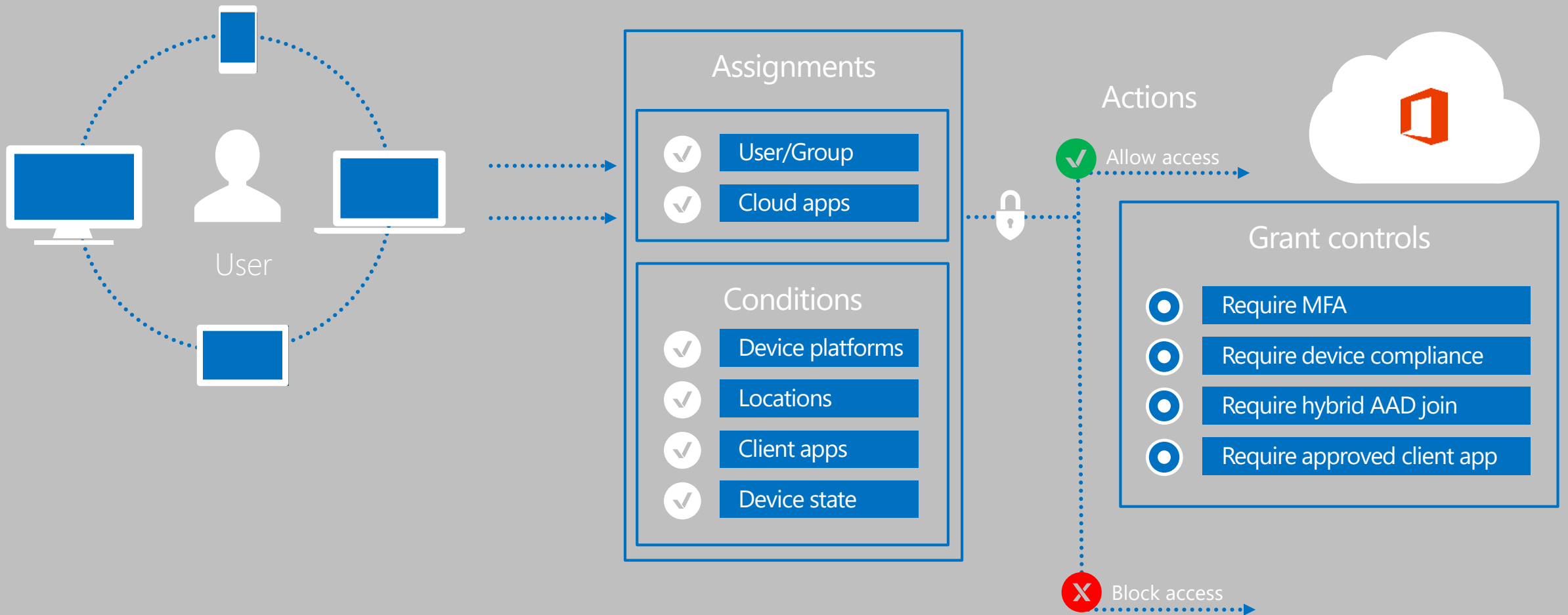
INVESTIGATE

- Risky users (Users flagged for ri...
- Risky sign-ins (Preview)
- Risk Detections (Risk events)
- Vulnerabilities**

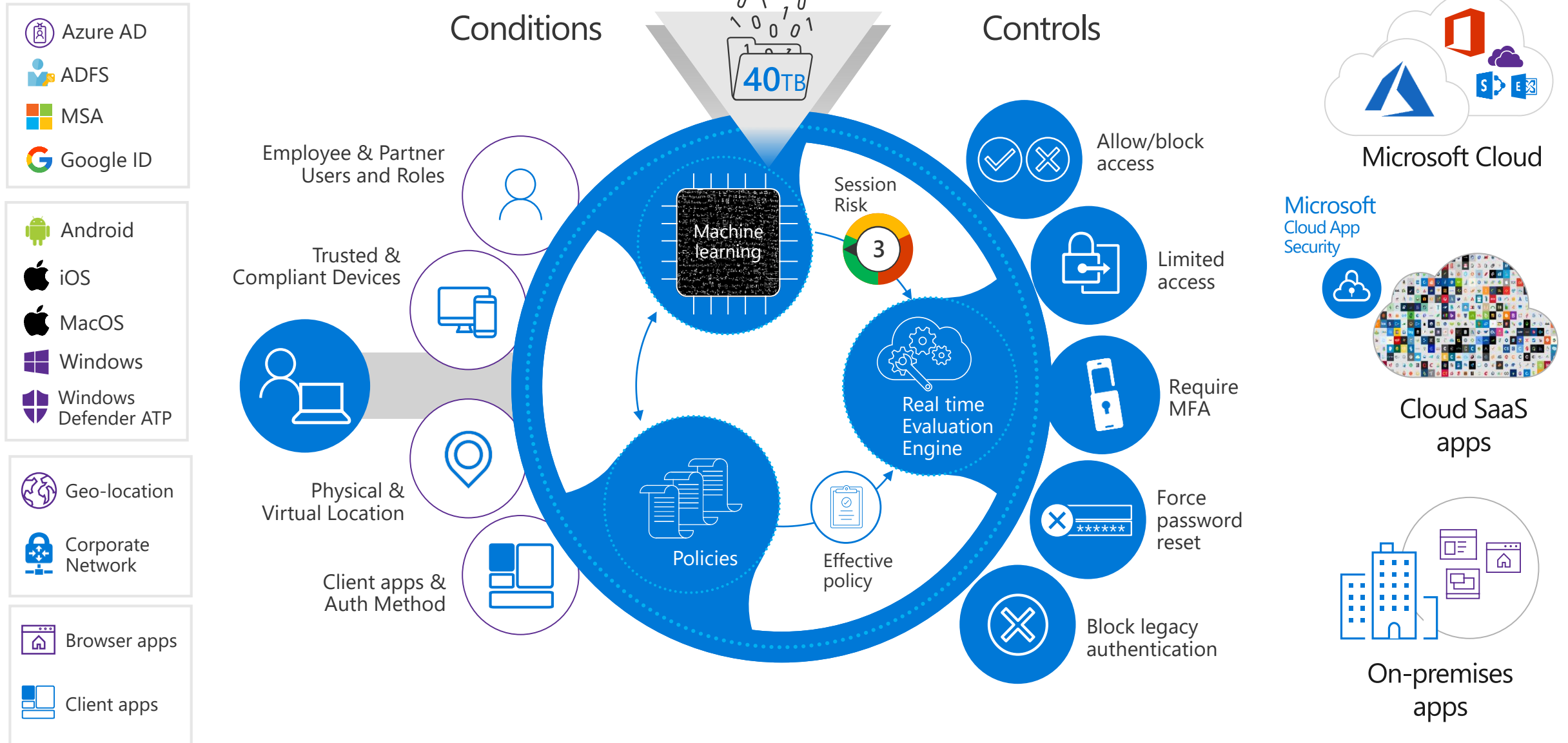
CONFIGURE

- MFA registration
- User risk policy
- Sign-in risk policy

Azure AD Conditional Access



Azure AD Identity Protection Conditional Access



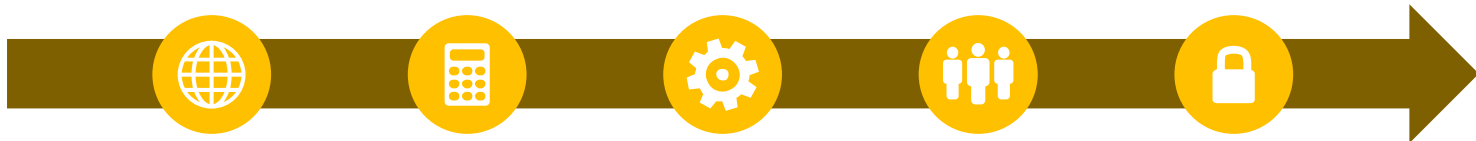
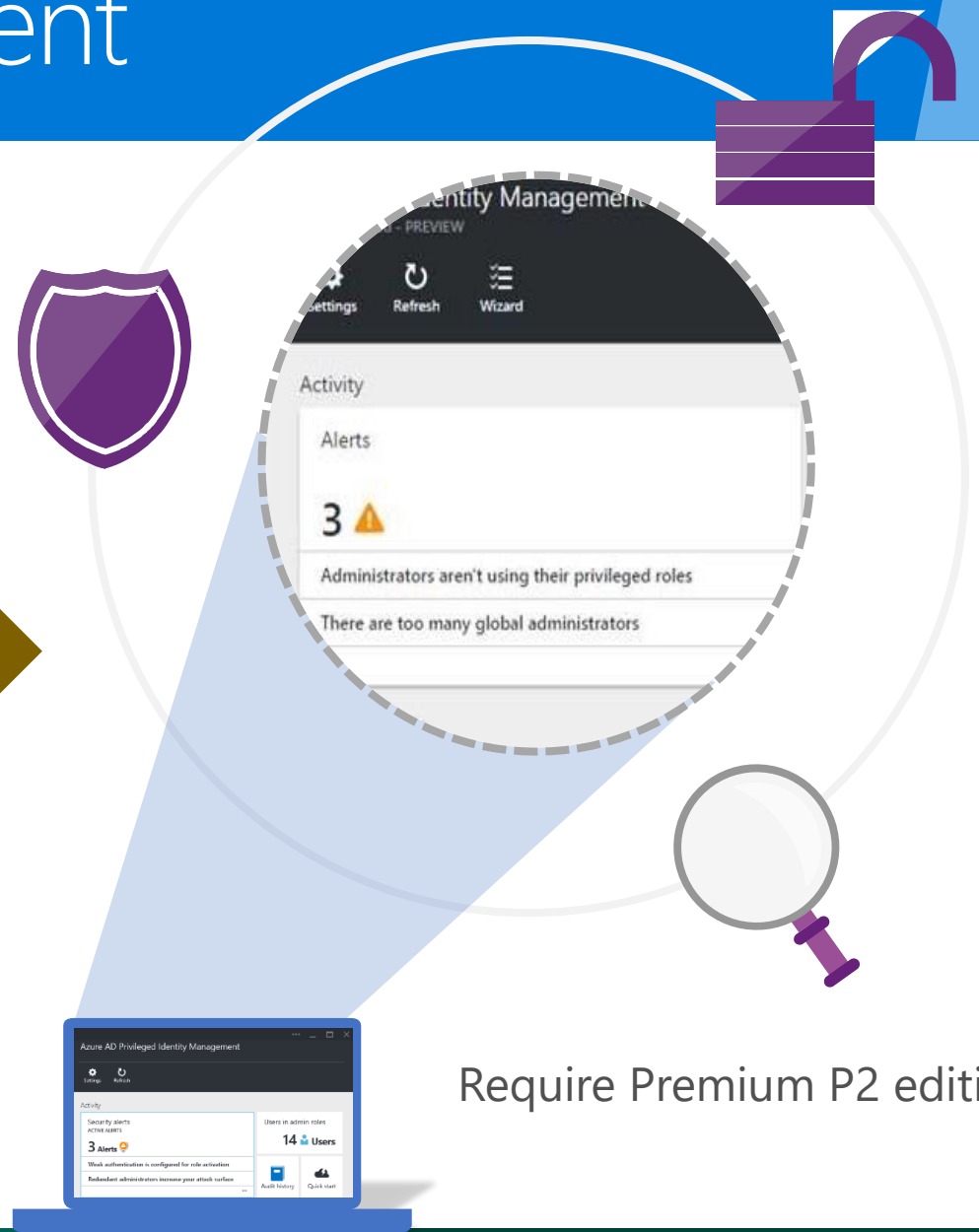
Privileged Identity Management

Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Manage access to resources in Azure AD, Azure Resources (Preview), and other Microsoft Online Services like Office 365 or Microsoft Intune

Provides more visibility through alerts, audit reports and access reviews



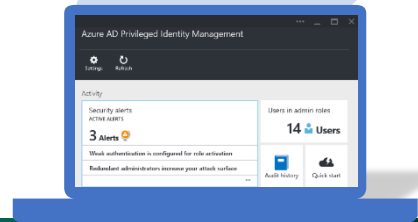
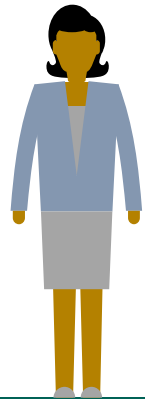
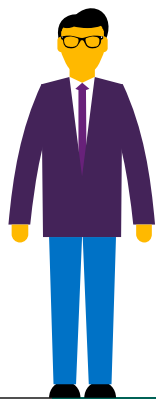
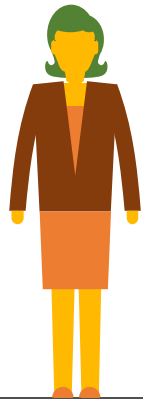
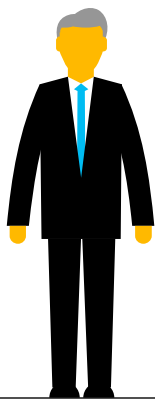
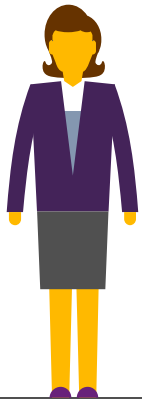
Global Administrator

Billing Administrator

Exchange Administrator

User Administrator

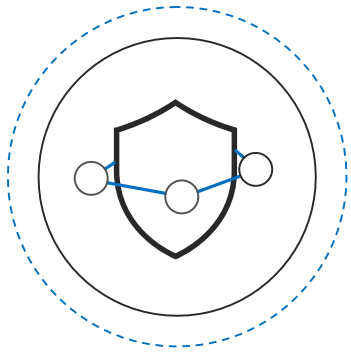
Password Administrator



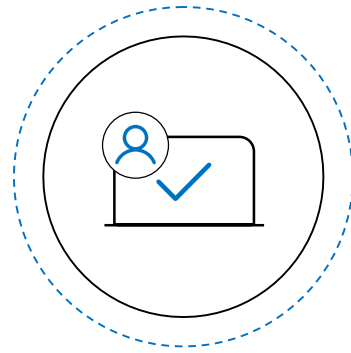
Require Premium P2 edition

Azure Advanced Threat Protection

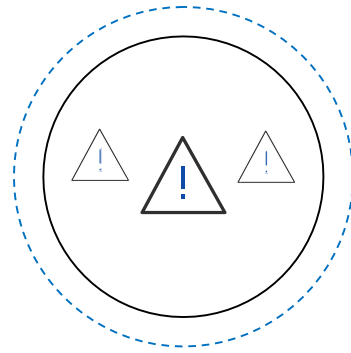
Detect and **investigate** advanced attacks, compromised identities, and insider threats



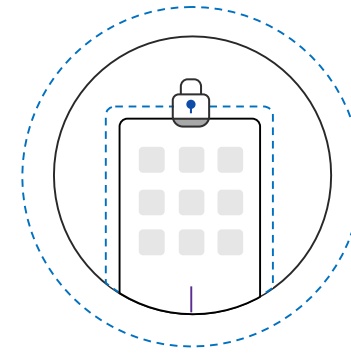
Detect threats fast
with Behavioral
Analytics



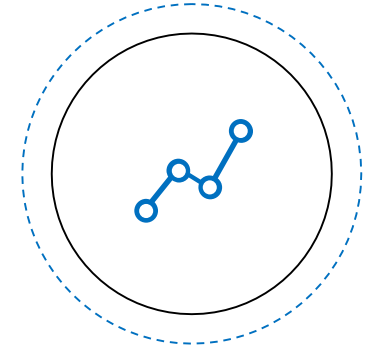
**Focus on what is
important** using
attack timeline



**Reduce the
fatigue** of false
positives

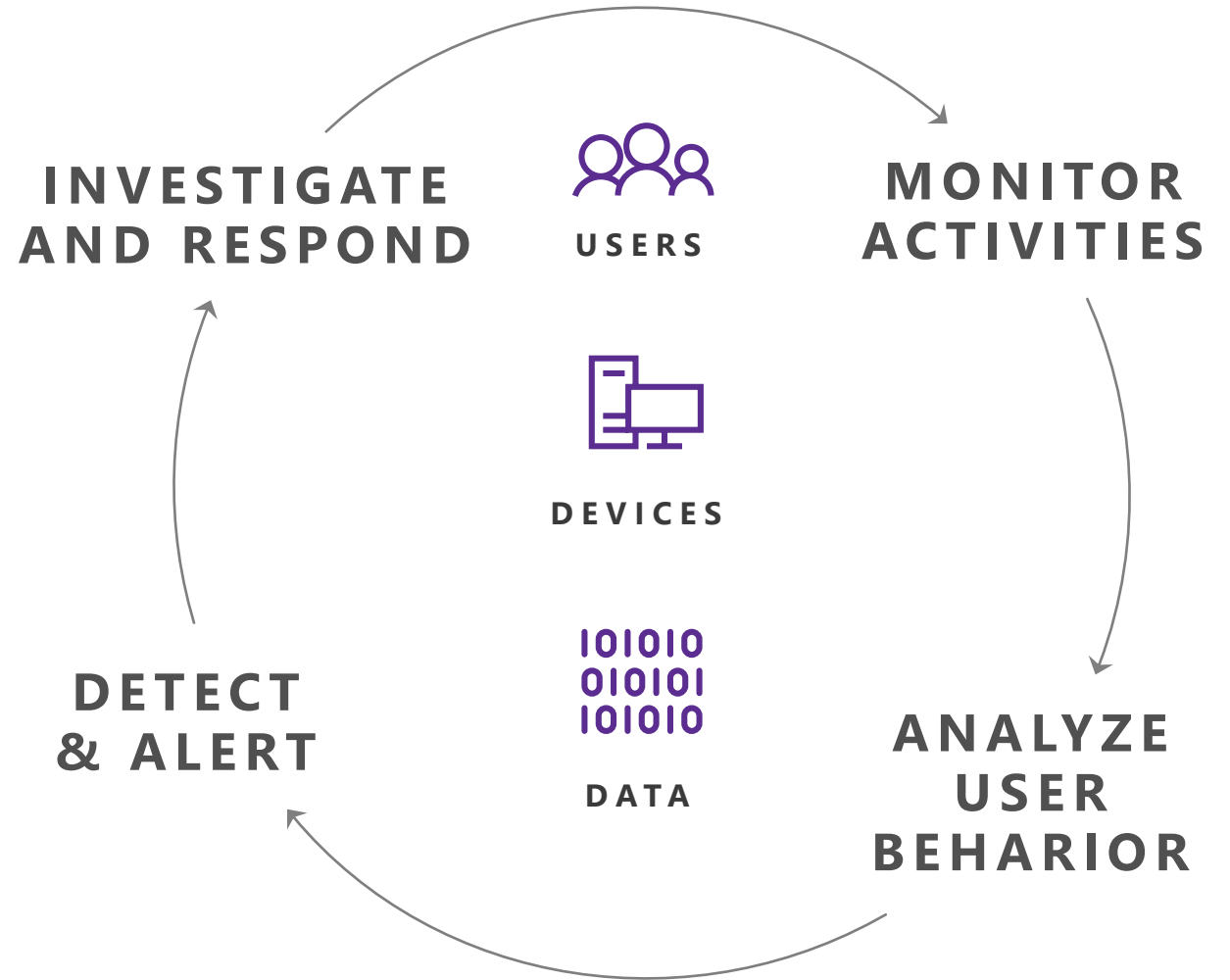
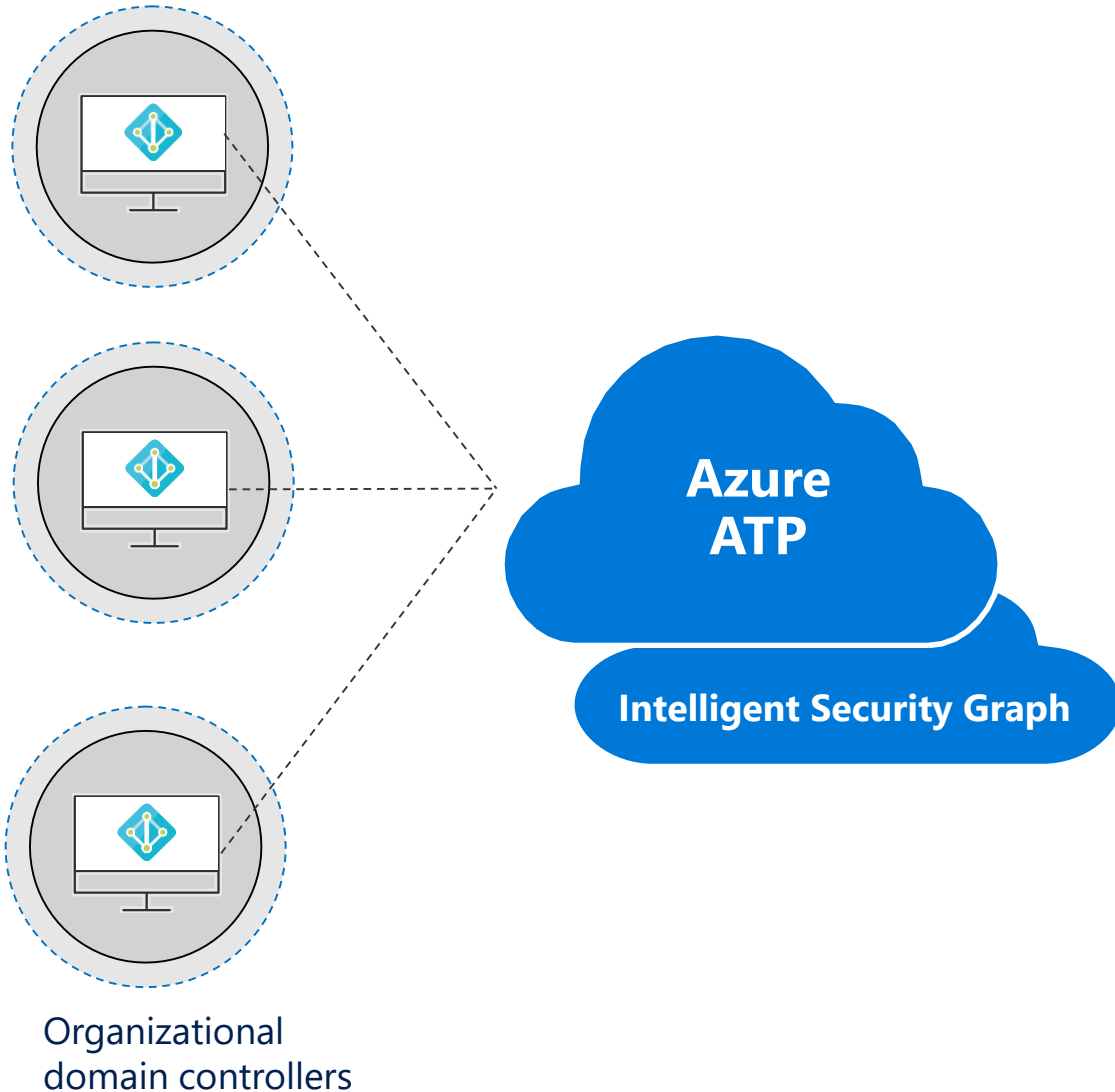


Protect at scale
with the power of
the cloud



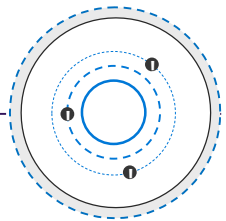
Best-in-class security
powered by the
Intelligent Security
Graph

How Azure ATP Works



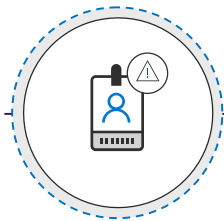
Azure ATP Suspicious Activities

Account enumeration
Users group membership enumeration
Users & IP address enumeration
Hosts & server name enumeration (DNS)



Reconnaissance

Compromised
Credential



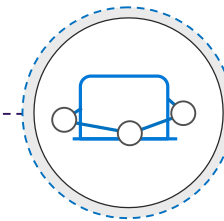
Brute force attempts
Suspicious VPN connection
Suspicious groups membership modifications
Honey Token account suspicious activities

Lateral
Movement



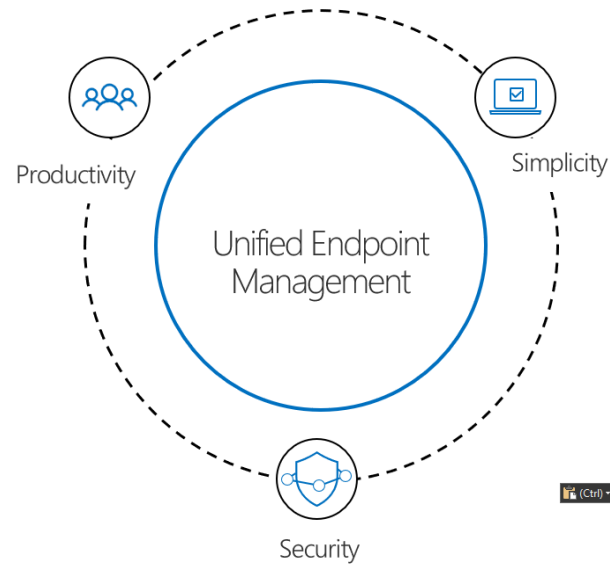
Pass-the-Ticket
Pass-the-Hash
Overpass-the-Hash

Golden ticket attack
DCShadow
Skeleton Key
Remote code execution on DC
Service creation on DC

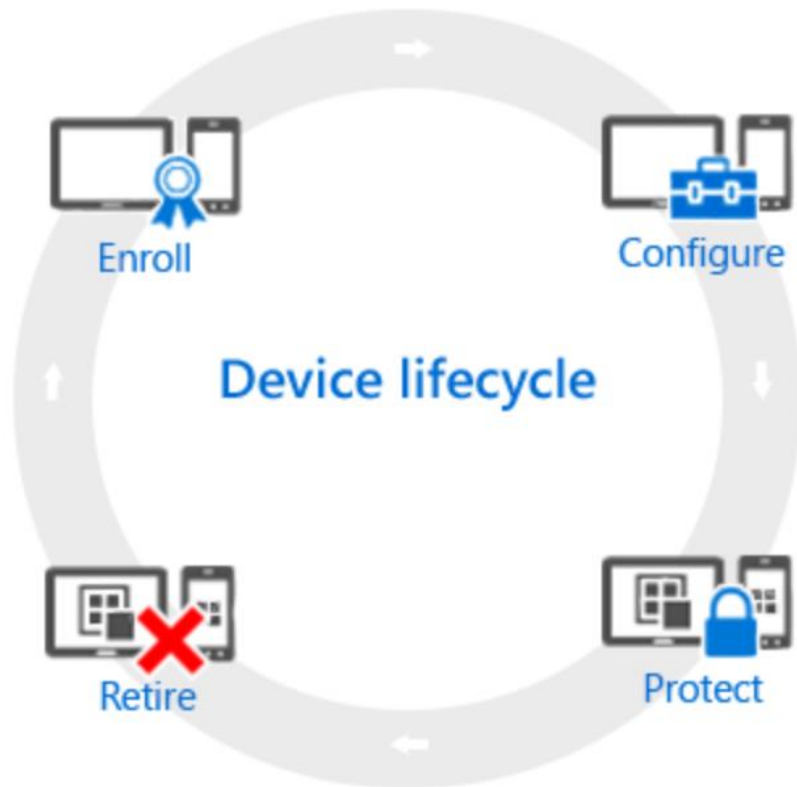


Domain
Dominance

Device management and protection



Microsoft Intune: Mobile Device Management (MDM)



- ✓ Enrolling devices into management so your IT department has an inventory of devices that are accessing corporate services
- ✓ Configuring devices to ensure they meet company security and health standards
- ✓ Providing certificates and Wi-Fi/VPN profiles to access corporate services
- ✓ Reporting on and measuring device compliance to corporate standards
- ✓ Removing corporate data from managed devices
- ✓ Retire Device
- ✓ Intune manage iOS, Android, Windows, and macOS

The most complete way to manage devices and secure data



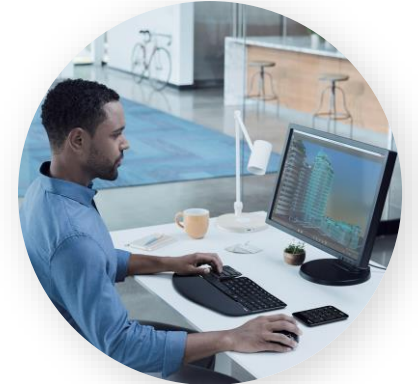
Mobile device
management



Mobile application
management



PC desktop
management



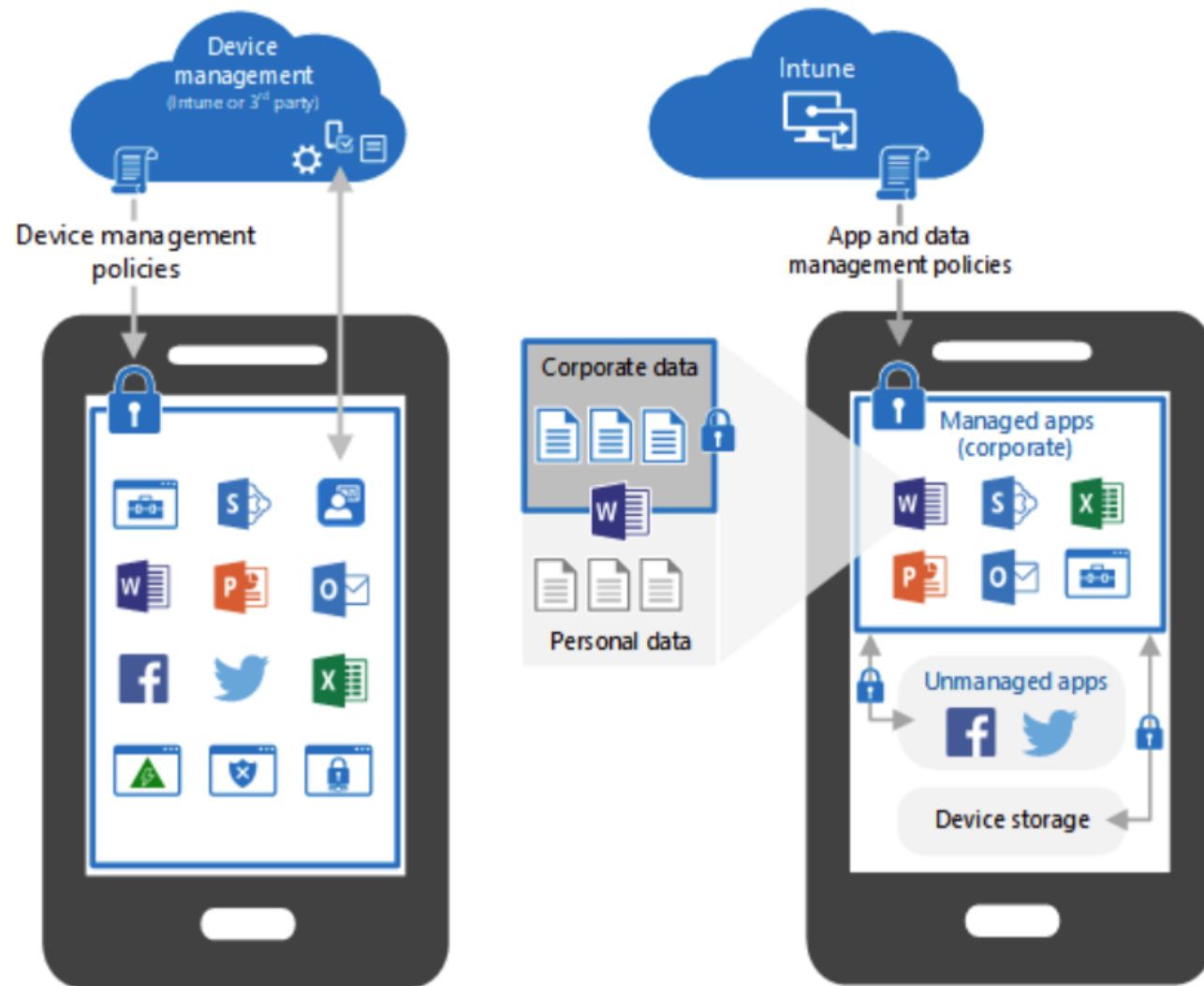
Enable
your users



Protect
your data

**Microsoft
Intune**

Corporate & BYOD | Device and Apps



MDM – Windows 10 Management

Home > Microsoft Intune > Device configuration - Profiles > Create profile

Create profile

* Name
Windows 10 Configuration ✓

Description
Enter a description... ✓

* Platform
Windows 10 and later

* Profile type
Select a configuration type

- Administrative Templates
- Device restrictions
- Device restrictions (Windows 10 Team)
- Delivery Optimization
- Domain Join (preview)
- Edition upgrade and mode switch
- Email
- Endpoint protection
- Identity protection
- Kiosk
- Network boundary
- Trusted certificate
- SCEP certificate
- PKCS certificate
- PKCS imported certificate
- VPN
- Microsoft Defender ATP (Windows 10 Des...)
- Wi-Fi
- Secure assessment (Education)
- Shared multi-user device

Device restrictions

Windows 10 and later

Select a category to configure settings.

- App Store
14 settings available
- Cellular and connectivity
16 settings available
- Cloud and Storage
4 settings available
- Cloud Printer
6 settings available
- Control Panel and Settings
16 settings available
- Display
2 settings available
- General
25 settings available
- Locked Screen Experience
7 settings available
- Messaging
3 settings available
- Microsoft Edge Browser
5 settings available
- Network proxy
8 settings available

Endpoint protection

Windows 10 and later

Select a category to configure settings.

- Windows Defender Application Gu...
10 settings available
- Windows Defender Firewall
44 settings available
- Windows Defender SmartScreen
2 settings available
- Windows Encryption
38 settings available
- Windows Defender Exploit Guard
21 settings available
- Windows Defender Application Co...
2 settings available
- Windows Defender Credential Gua...
1 setting available
- Windows Defender Security Center
17 settings available
- Local device security options
46 settings available
- Xbox services
5 settings available

Windows Hello for Business

Windows 10 and later

Configure Windows Hello for Business: ⓘ Enable

Minimum PIN length: ⓘ Not configured

Maximum PIN length: ⓘ Not configured

Lowercase letters in PIN: ⓘ Not allowed

Uppercase letters in PIN: ⓘ Not allowed

Special characters in PIN: ⓘ Not allowed

PIN expiration (days): ⓘ Not configured

Remember PIN history: ⓘ Not configured

Enable PIN recovery: ⓘ Enable Not configured

Use a Trusted Platform Module (TPM): ⓘ Enable Not configured

Allow biometric authentication: ⓘ Enable Not configured

Use enhanced anti-spoofing, when available: ⓘ Enable Not configured

Certificate for on-premise resources: ⓘ Enable Not configured

Use security keys for sign-in: ⓘ Enable Not configured

OK

MDM – Compliance

Home > Microsoft Intune > Device compliance - Policies > Create Policy > Windows 10 compliance p

Create Policy

* Name
Windows 10 Compliance ✓

Description
Enter a description... ✓

* Platform
Windows 10 and later

Settings
Configure >

Actions for noncompliance
1 configured >

Scope (Tags)
0 scope(s) selected >

Windows 10 compliance p...

Windows 10 and later

Select a category to configure settings.

- Device Health > 3 settings available
- Device Properties > 5 settings available
- Configuration Manager Compliance > 1 setting available
- System Security > 17 settings available
- Microsoft Defender ATP > 1 setting available

Create Policy

* Name
Android Compliance Policy ✓

Description
Enter a description... ✓

* Platform
Android Enterprise

* Profile type
Work profile

Settings
Configure >

Actions for noncompliance
1 configured >

Scope (Tags)
0 scope(s) selected >

Work profile

Android Enterprise

Select a category to configure settings.

- Device Health > 5 settings available
- Device Properties > 2 settings available
- System Security > 9 settings available

Home > Microsoft Intune > Device compliance - Policies > Create Policy > iOS compliance policy

Create Policy

* Name
iOS Compliance Policy ✓

Description
Enter a description... ✓

* Platform
iOS

Settings
Configure >

Actions for noncompliance
1 configured >

Scope (Tags)
0 scope(s) selected >

iOS compliance policy

iOS

Select a category to configure settings.

- Email > 1 setting available
- Device Health > 2 settings available
- Device Properties > 4 settings available
- System Security > 10 settings available

Permit access to Company Resource from Compliance Device with Azure AD Conditional Access

Intune – Mobile Application Management

Client apps - App protection

Microsoft Intune

Search (Ctrl+/)

Overview

Manage

Apps

App protection policies

App configuration policies

App selective wipe

iOS app provisioning profiles

Monitor

App licenses

Data protection

Teams on Android MAM

Save Discard

Data Transfer

Backup Org data to Android backup services Allow Block

Send Org data to other apps

Select apps to exempt

Receive data from other apps

Save copies of Org data Allow Block

Allow user to save copies to selected services

Restrict cut, copy and paste between other apps

Cut and copy character limit for any app

Screen capture and Google Assistant Enable Disable

Encryption

Encrypt Org data Require Not required

Encrypt Org data on enrolled devices Require Not required

Functionality

Sync app with native contacts app Enable Disable

Printing Org data Enable Disable

Restrict web content transfer with other apps

Unmanaged Browser ID

Unmanaged Browser Name

Access requirements

Teams on Android MAM

Save Discard

PIN for access

PIN type Numeric Passcode

Simple PIN Allow Block

Select minimum PIN length

Fingerprint instead of PIN for access (Android 6.0+) Allow Block

Override fingerprint with PIN after timeout Require Not required

Timeout (minutes of inactivity)

PIN reset after number of days Yes No

Number of days

App PIN when device PIN is set Enable Disable

Work or school account credentials for access Require Not required

Recheck the access requirements after (minutes of inactivity)

Android deployment scenarios with Intune

BYOD

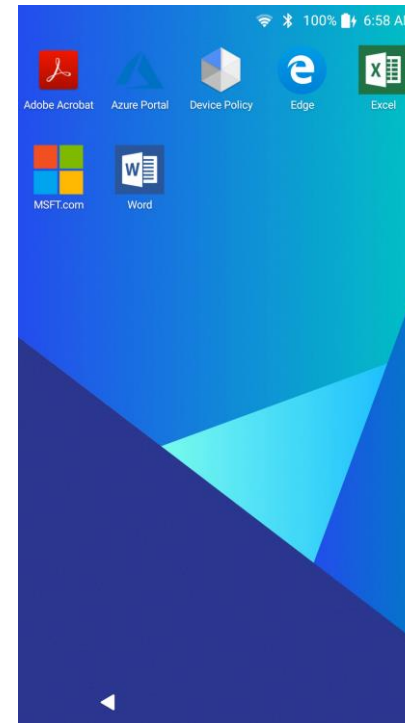
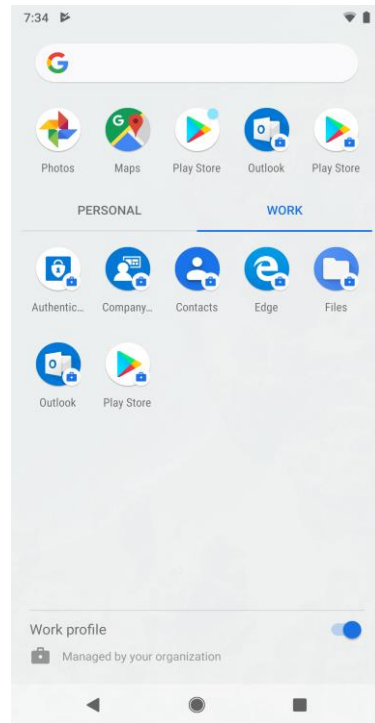
Corp Owned

Android App
Managed

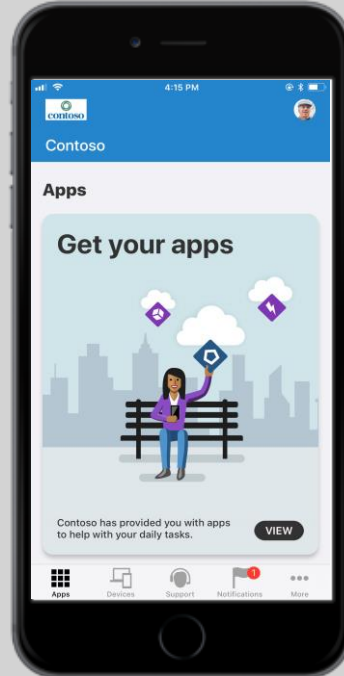
AE Work Profile

AE Dedicated
(kiosk)

AE Fully managed



iOS deployment scenarios



BYOD

CORP OWNED

iOS app managed

iOS device managed

Supervised

- Data protection at the app level
- App protection without full device management

- User-based enrollment via Company Portal
- Push Apps (VPP, standard or store) and policies
- Device based Compliance

- Apple Corporate programs like VPP+DEP/ASM
- Secure locked down devices: Kiosk, Classroom
- Lock management profile to a device

Windows Defender ATP product services

Prevent, detect, investigate,
and respond to advanced
threats



Microsoft Defender ATP

Endpoint behavioural sensors
Cloud security analytics
Threat intelligence

Built-in. Cloud-powered.



THREAT & VULNERABILITY

Detect endpoint vulnerability and misconfiguration



ATTACK SURFACE REDUCTION

Resist attacks and exploitations



NEXT GENERATION PROTECTION

Protect against all types of emerging threats



ENDPOINT DETECTION & RESPONSE

Detect, investigate, and respond to advanced attacks



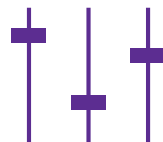
AUTO INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



SECURITY SCORE

Track and improve your organization security posture



SECURITY MANAGEMENT

Centralized configuration and administration

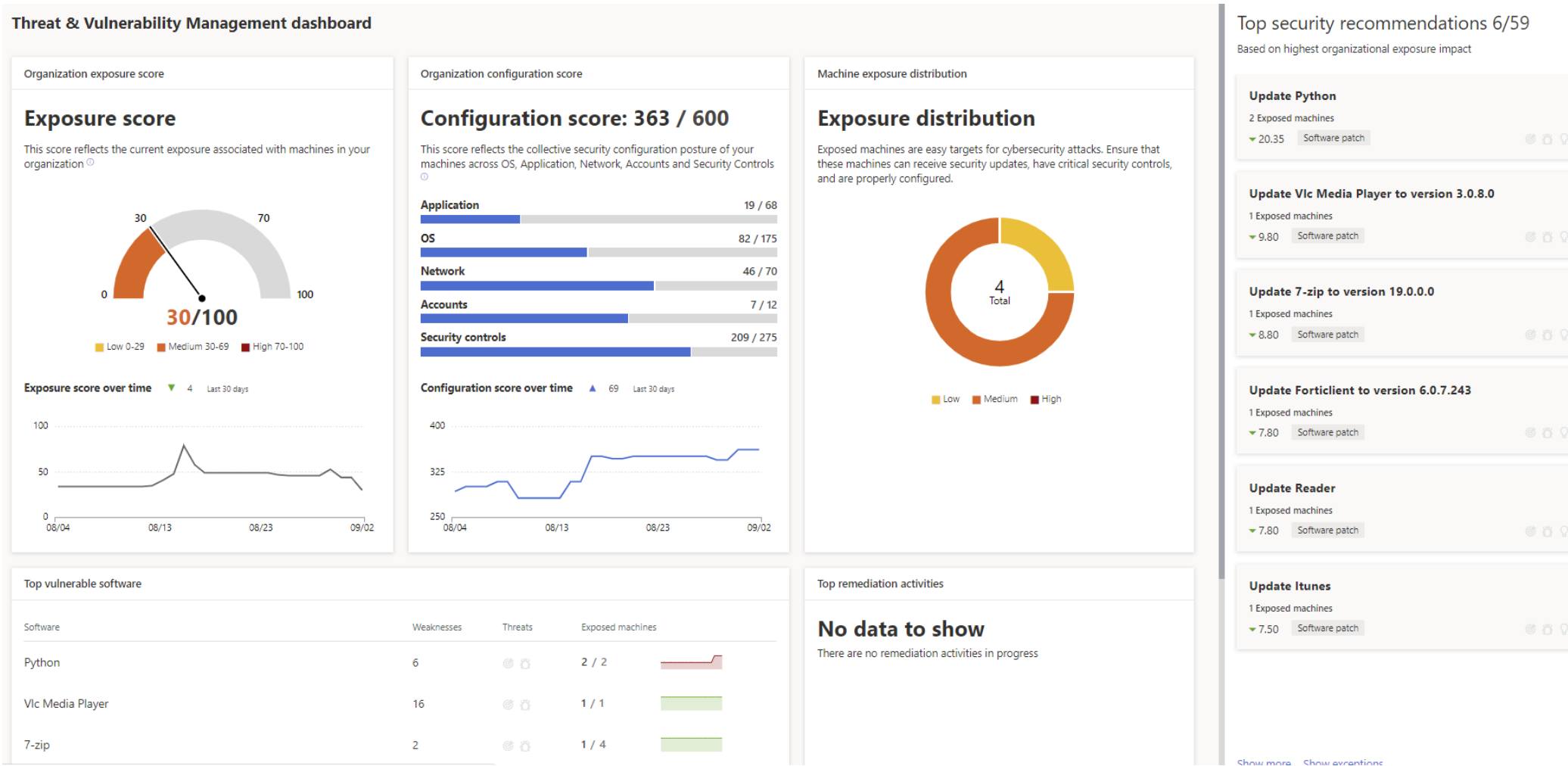
Attack surface reduction protect the devices and applications from new and emerging threats: solutions



Windows 10 Enterprise Features:

- ✓ Microsoft Defender Application Guard
 - ✓ Hardware based isolation
- ✓ Microsoft Defender Application Control
 - ✓ Application control
- ✓ Microsoft Defender Exploit Guard
 - ✓ Exploit protection
 - ✓ Network protection
 - ✓ Controlled folder access /Ransomware Protection
 - ✓ Attack Surface reduction
- ✓ Microsoft Defender Firewall

Threat and Vulnerability Management



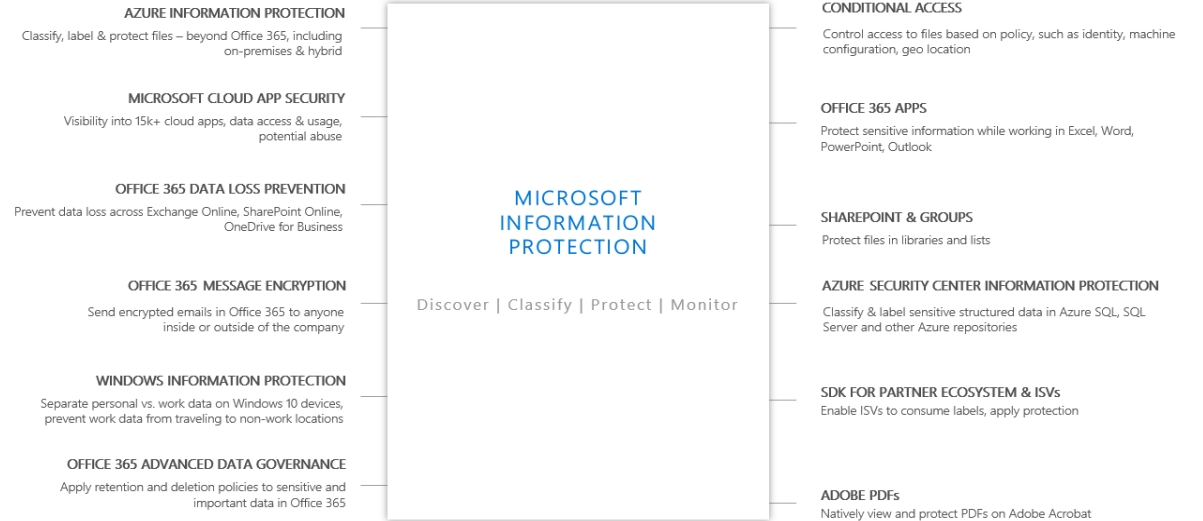
Periodic scanning of vulnerability

Lack of priority on patch management

Manual remediation of misconfiguration

Information Protection

Microsoft information protection solutions



Sensitive data is at risk: solutions

80 % of employees use non-approved SaaS apps at work

58 % Have accidentally sent sensitive information to the wrong person

88 % of organizations no longer have confidence to detect and prevent loss of sensitive data

85 % of enterprise organizations keep sensitive information in the cloud

DEVICE PROTECTION

Protect system and data when device is lost or stolen

DATA SEPARATION

Containment
Data separation

LEAK PROTECTION

Prevent unauthorized users and apps from accessing and leaking data

SHARING PROTECTION

Protect data when shared with others, or shared outside of organizational devices and control

Your information protection needs

DEVICE PROTECTION

BitLocker

DATA SEPARATION

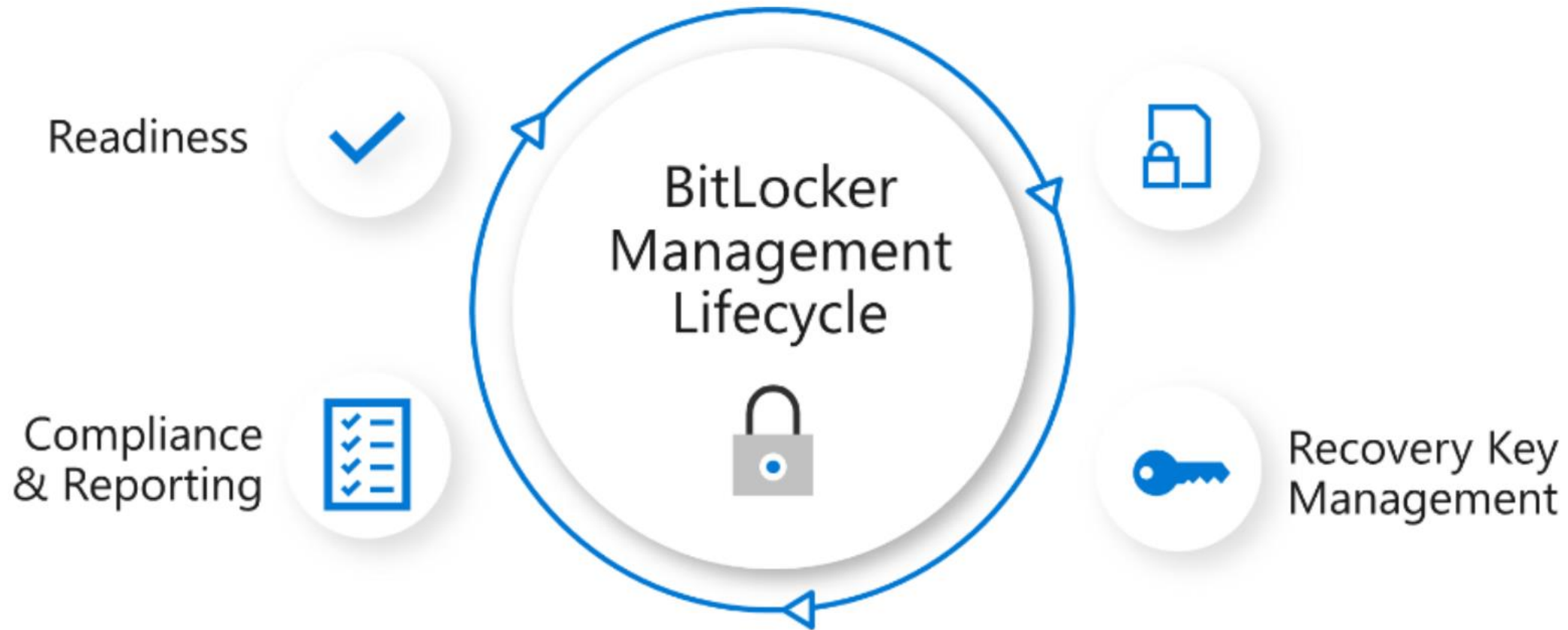
Windows Information Protection (MAM)

LEAK PROTECTION

Azure Information Protection (Office 365 Labeling)
Office 365 ATP

SHARING PROTECTION

BitLocker Management



WINDOWS INFORMATION PROTECTION

Integrated protection against accidental data leaks



Protects data at rest locally and on removable storage.



Common experience across all Windows 10 devices with copy and paste protection.



Since Windows 10 Version 1607

Corporate vs personal data identifiable wherever it rests on the device and can be wiped.



Seamless integration into the platform, No mode switching and use any app.



Prevents unauthorized apps from accessing business data and users from leaking data via copy and paste protection.



Azure Information Protection

Comprehensive protection of sensitive data throughout the lifecycle—across devices, apps, cloud services, and on-premises



Discover & classify
sensitive information



Apply protection
based on policy

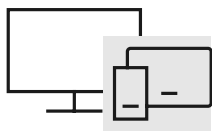


Monitor &
remediate

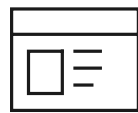


Accelerate
Compliance

Across



Devices



Apps



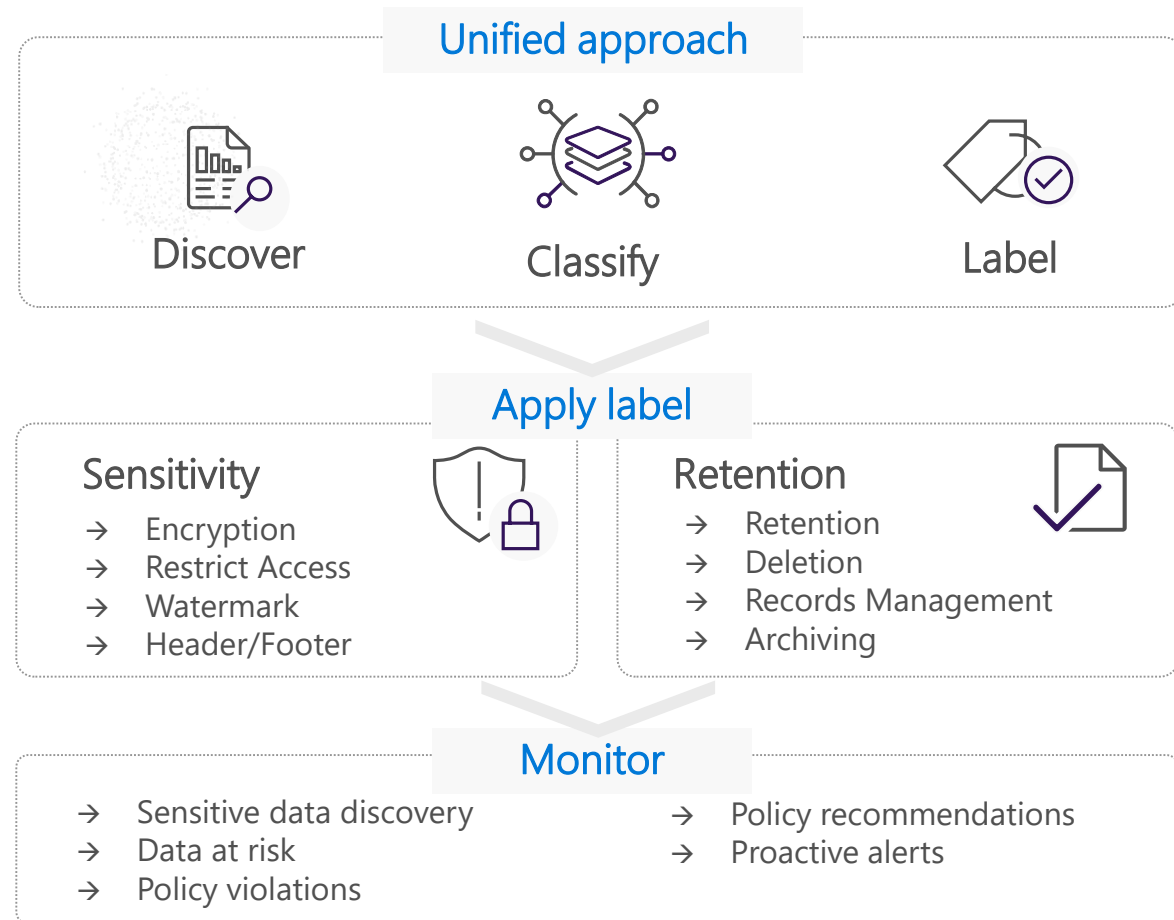
Cloud services



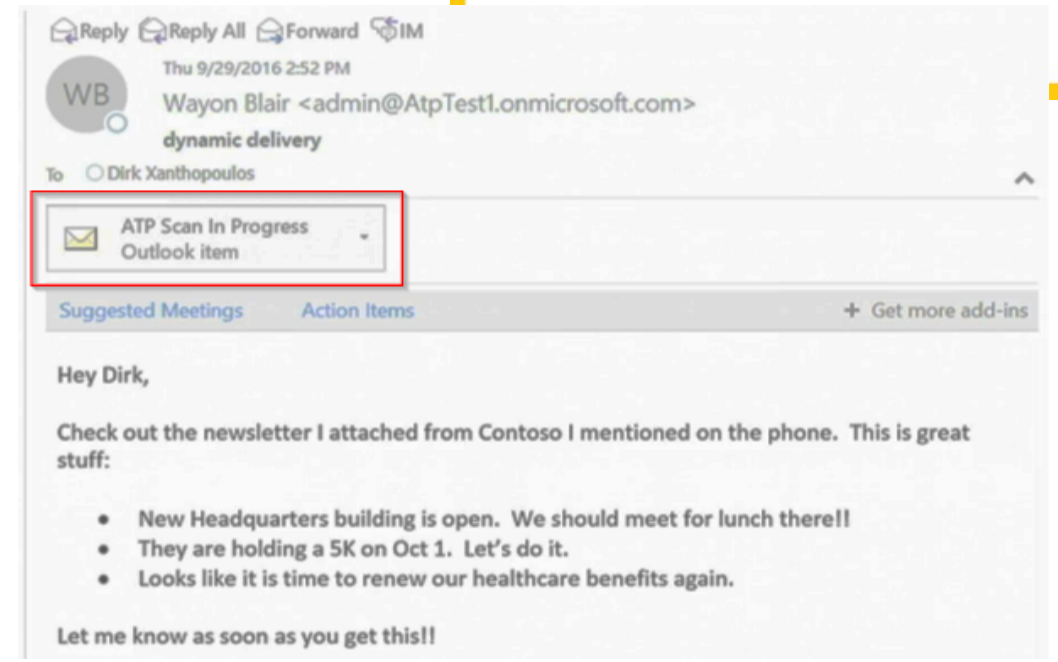
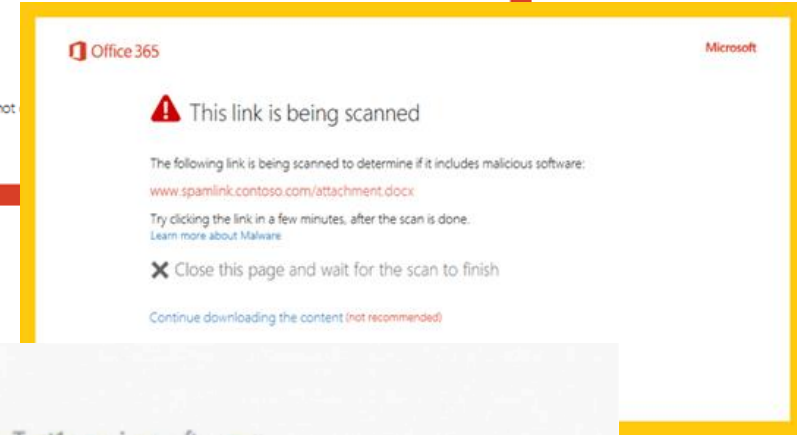
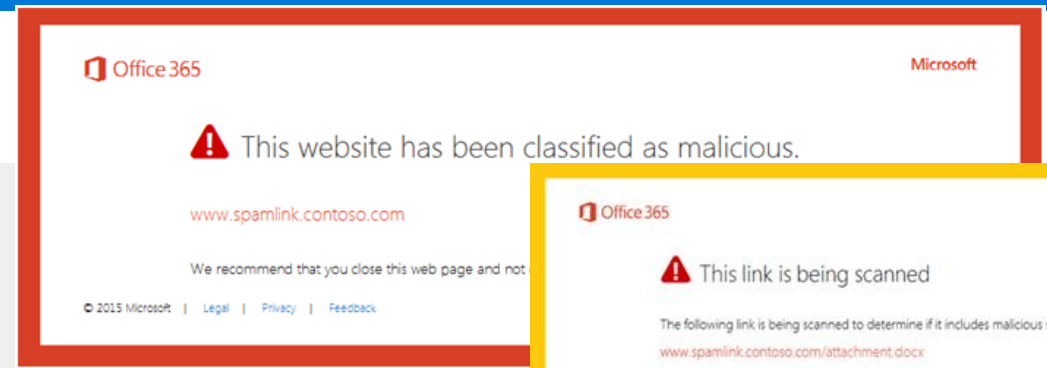
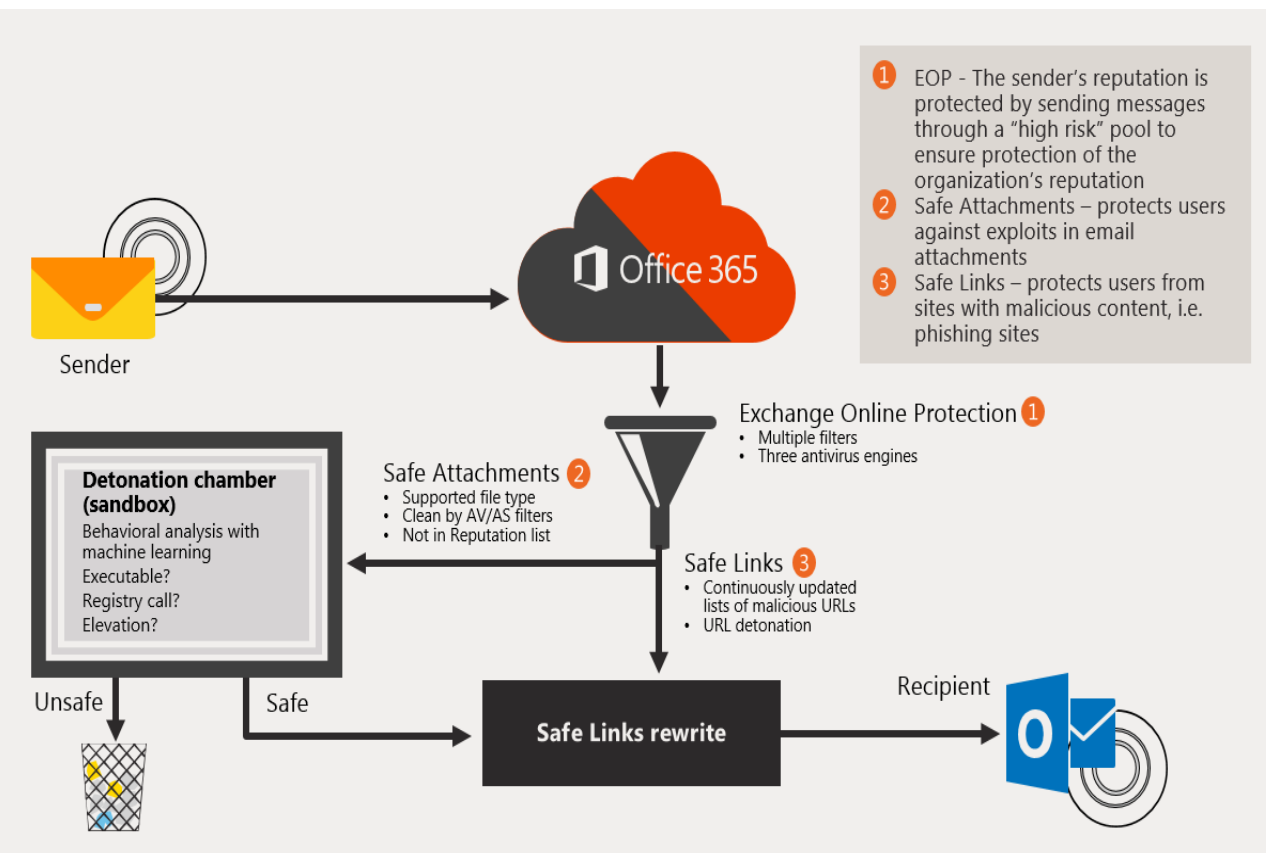
On-premises

Data protection & data governance go hand-in-hand

- ✓ Unified approach to discover, classify & label
- ✓ Automatically apply policy-based actions
- ✓ Proactive monitoring to identify risks
- ✓ Broad coverage across locations

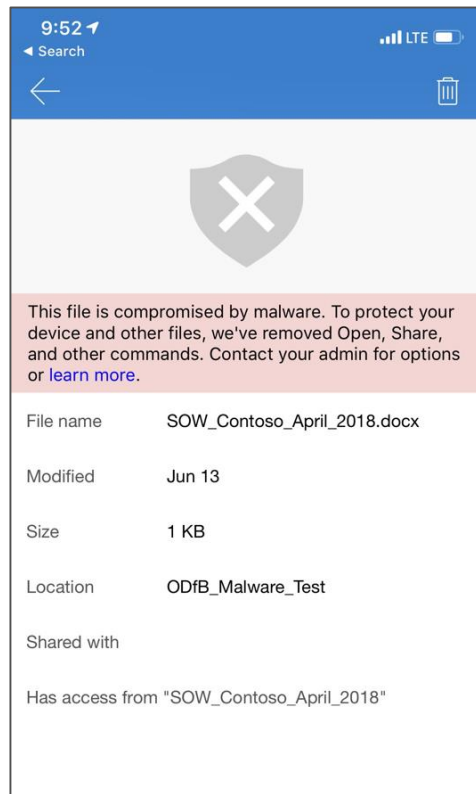


Office 365 Advanced Threat Protection

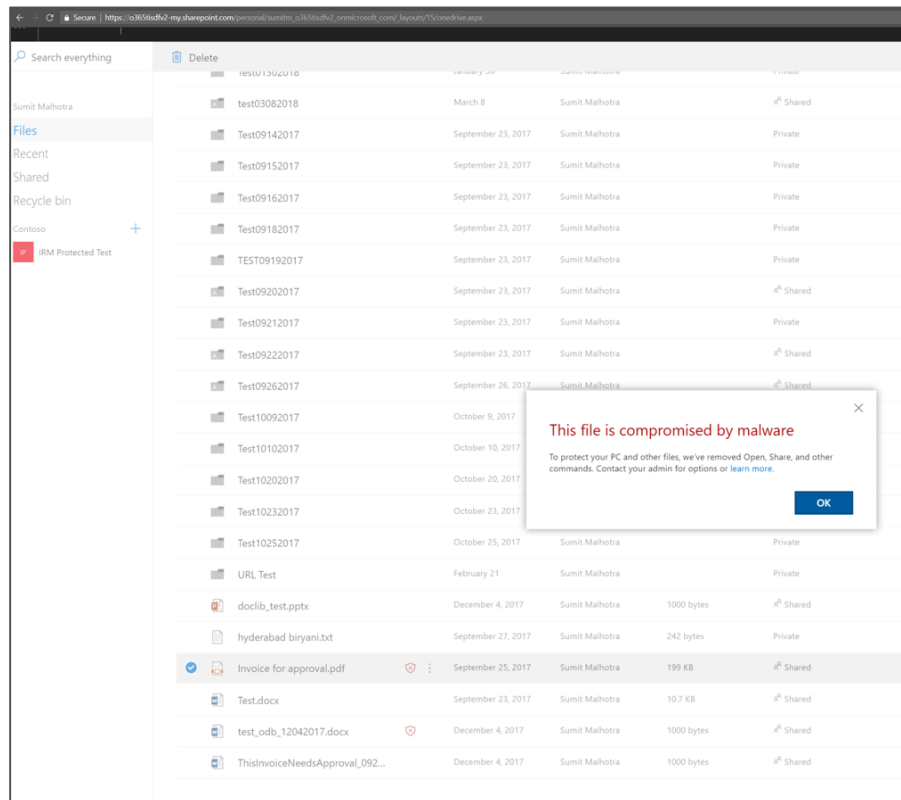


O365 ATP: Securing your collaboration scenarios

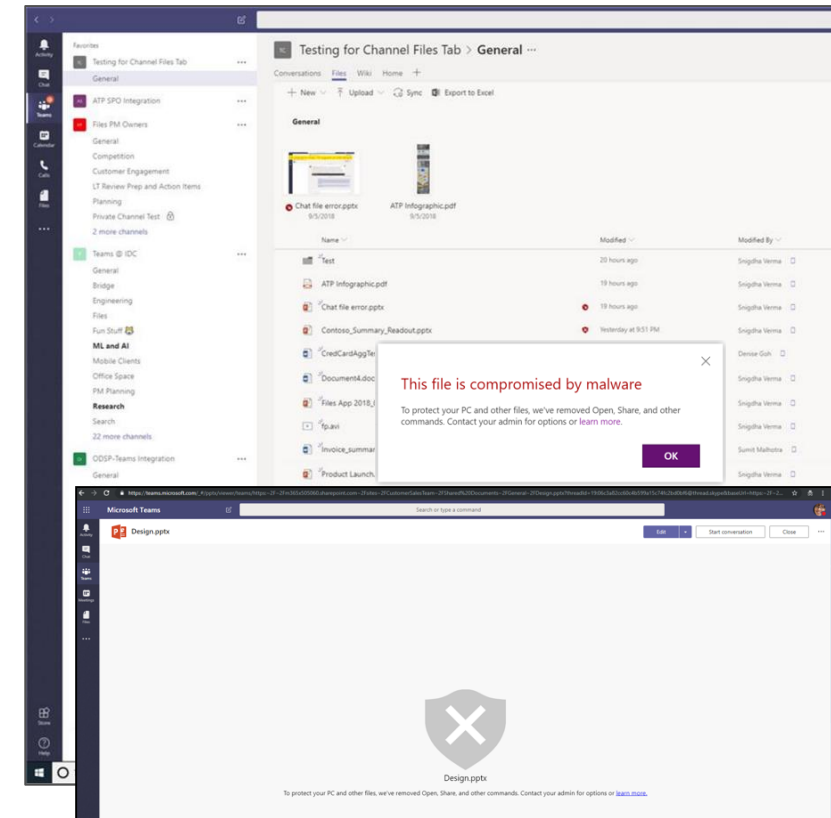
SharePoint Online, OneDrive for Business and Microsoft Teams



OneDrive iOS app showing files detected and blocked by [Office 365 ATP](#)

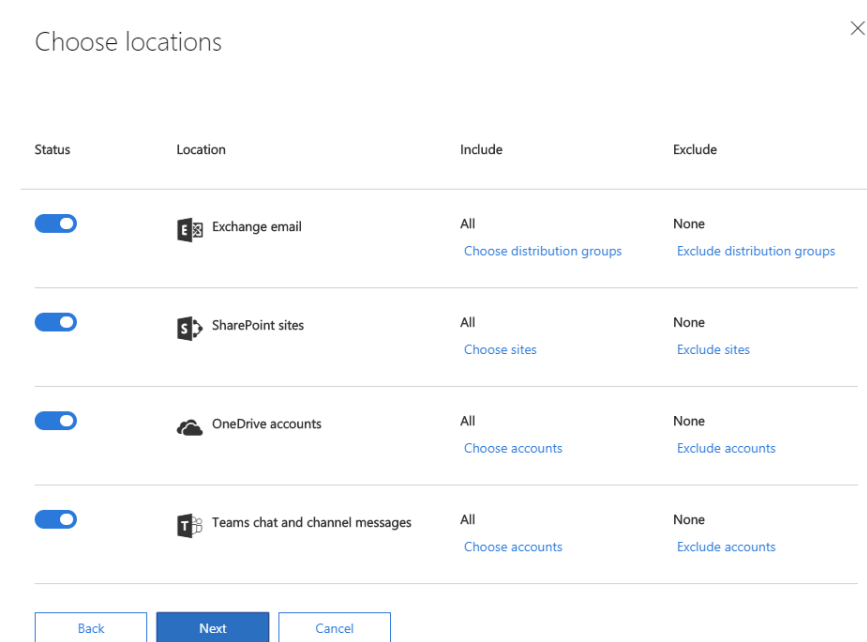
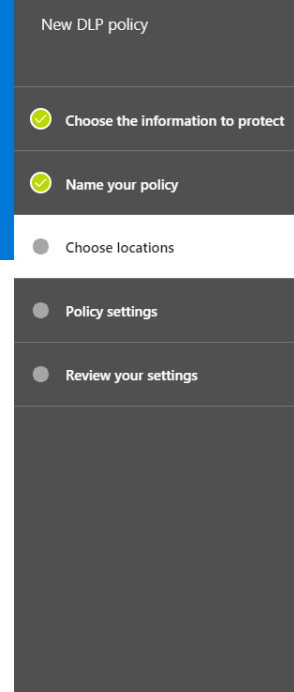


SharePoint Online WebUX showing files detected and blocked by [Office 365 ATP](#)



Microsoft Teams desktop client showing files detected and blocked by [Office 365 ATP](#)

Office 365 Data Loss Prevention



Built-in Policies & Templates

Over 40 policy templates for common industry regulations and compliance needs – included out of the box

Proactive default protection policy for most common sensitivity content

System-generated insights with step-by-step enablement for additional protection controls

Rich customization

Conditions & Exceptions describe what the content looks like (or doesn't look like), and what events to look for.

Actions define what type of automatic remediation you want to take when the conditions match

User notifications & overrides define what the user sees, and if they have the ability to override with a business justification

Incident reports trigger email notifications or Alerts based upon severity of event

Protection Across Office 365

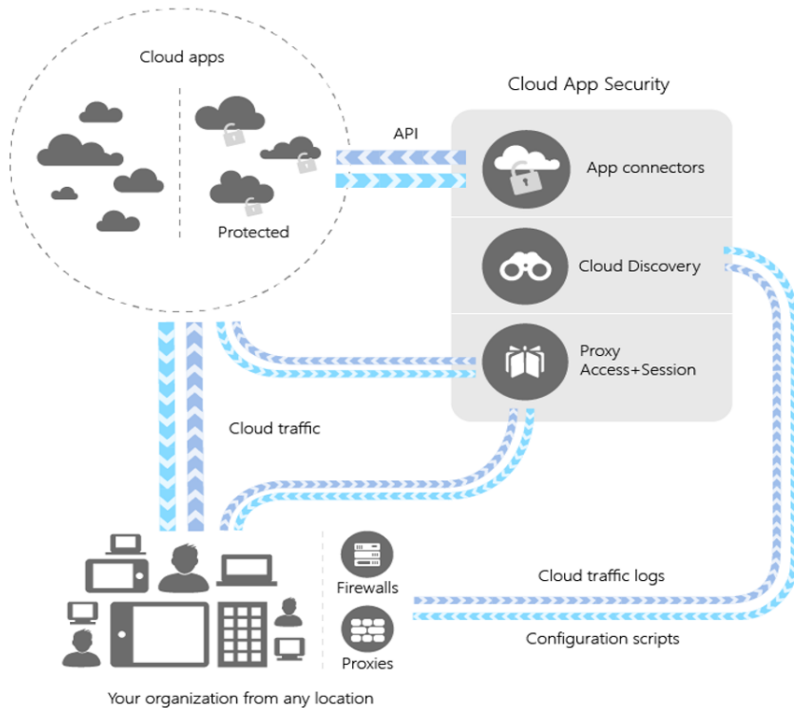
Centralized portal to manage policies, protection insights, and investigate matches

Policies configured once and **applied across Office 365 services** and client end-points

DLP for Teams chat and channel messages

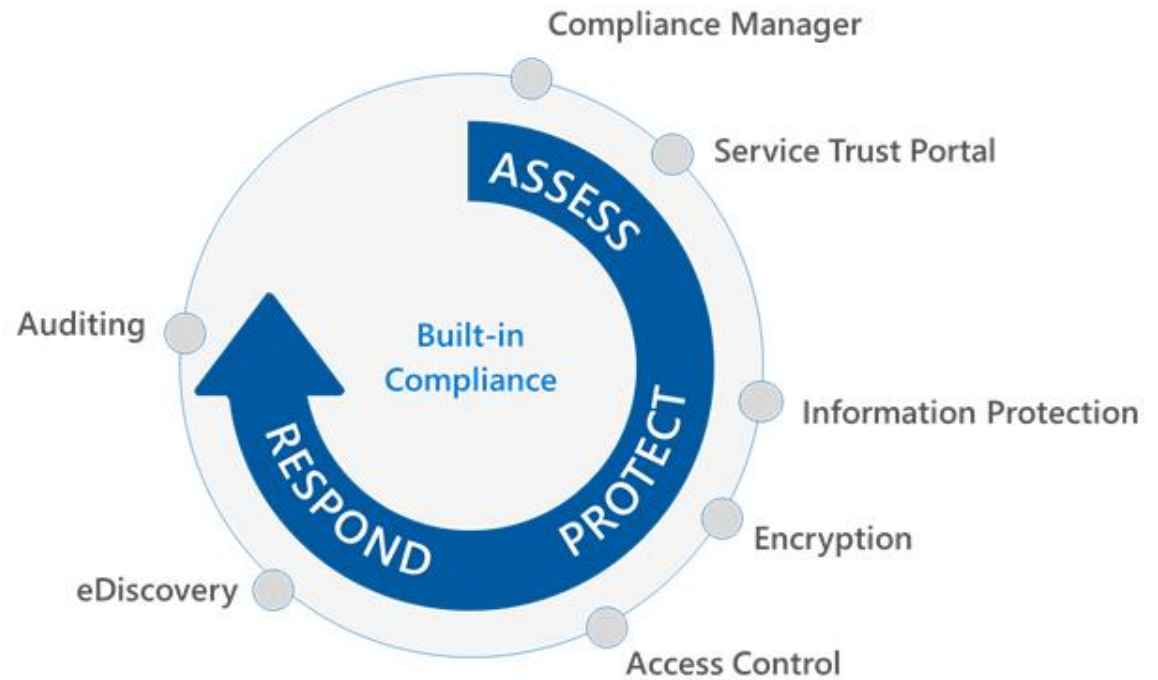
Cloud App Security

- ✓ Discover and control the use of Shadow IT
- ✓ Protect your sensitive information anywhere in the cloud
- ✓ Protect against cyberthreats and anomalies
- ✓ Assess the compliance of your cloud apps



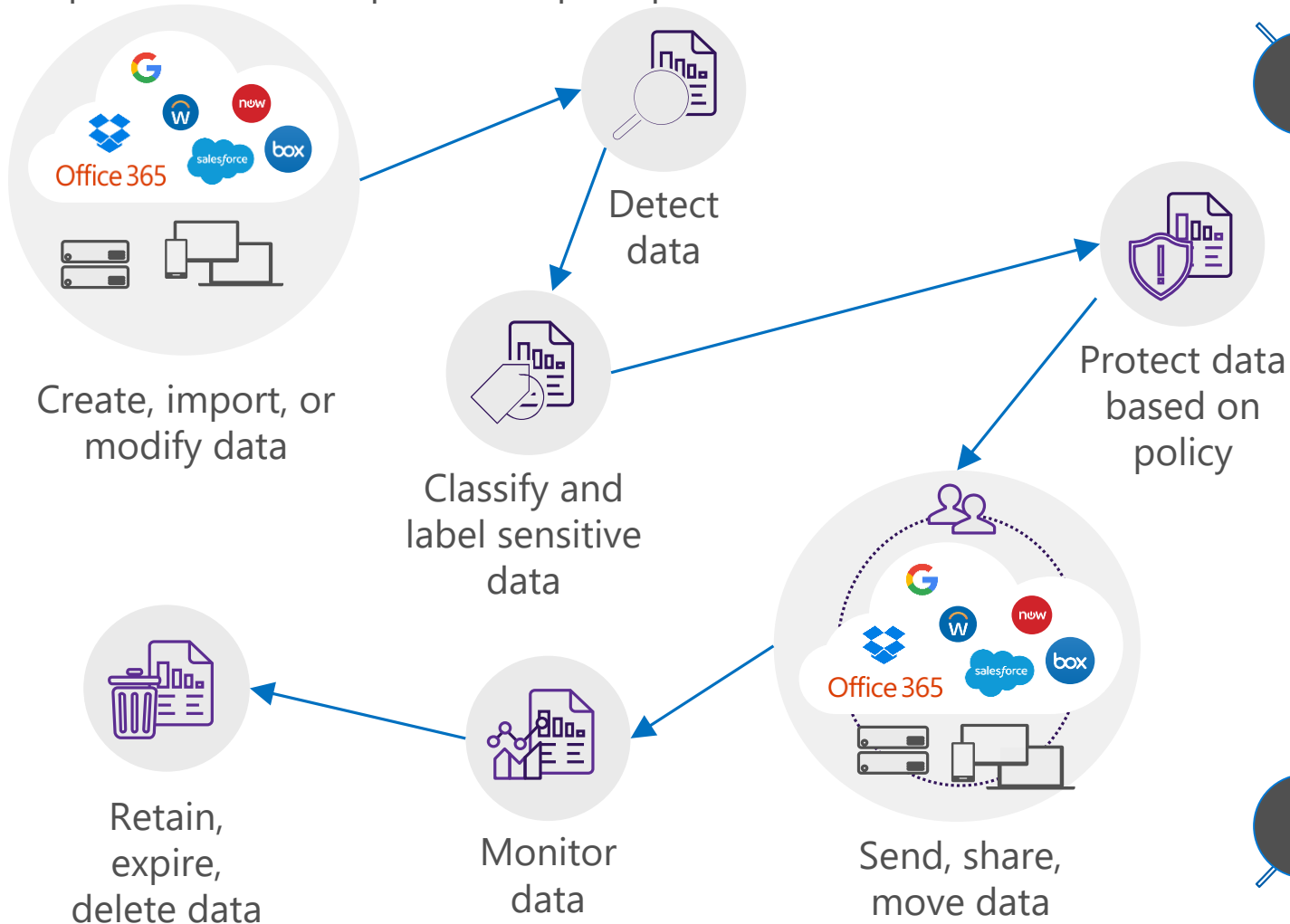
10 GENERAL			
Category: E-commerce	Headquarters: United States	Data center: Ireland	Hosting company: Amazon Web Servi...
Founded: 1994	Holding: Public	Domain: *amazon.co.uk	Terms of service: amazon.co.uk/gp/he...
Domain registration: Jan 1, 1996	Consumer popularity: 10	Privacy policy: amazon.co.uk/gp/help...	Logon URL: www.amazon.co.uk/ap/si...
Vendor: Amazon.com	Data types: Documents, Media file...	<input checked="" type="checkbox"/> Disaster Recovery Plan	
9 SECURITY			
Latest breach: —	<input type="checkbox"/> Data-at-rest encryption method	<input type="checkbox"/> Multi-factor authentication	<input type="checkbox"/> IP address restriction
<input checked="" type="checkbox"/> User audit trail	<input type="checkbox"/> Admin audit trail	<input checked="" type="checkbox"/> Data audit trail	<input type="checkbox"/> User can upload data
<input type="checkbox"/> Data classification	<input checked="" type="checkbox"/> Remember password	<input type="checkbox"/> User-roles support	<input type="checkbox"/> File sharing
<input checked="" type="checkbox"/> Valid certificate name	<input checked="" type="checkbox"/> Trusted certificate	Encryption protocol: TLS 1.2	<input checked="" type="checkbox"/> Heartbleed patched
HTTP security headers: Partial	<input checked="" type="checkbox"/> Supports SAML	<input checked="" type="checkbox"/> Protected against DROWN	<input type="checkbox"/> Penetration Testing
<input type="checkbox"/> Requires user authentication	<input type="checkbox"/> Password policy		
9 COMPLIANCE			
<input checked="" type="checkbox"/> ISO 27001	<input checked="" type="checkbox"/> ISO 27018	<input checked="" type="checkbox"/> ISO 27017	<input type="checkbox"/> IS Suggest an improvement
<input type="checkbox"/> FINRA	<input type="checkbox"/> FISMA	<input type="checkbox"/> GAAP	<input type="checkbox"/> HIPAA i o
<input type="checkbox"/> ISAE 3402	<input type="checkbox"/> ITAR	<input checked="" type="checkbox"/> SOC 1	<input checked="" type="checkbox"/> SOC 2
<input checked="" type="checkbox"/> SOC 3	<input checked="" type="checkbox"/> SOX	<input type="checkbox"/> SP 800-53	<input type="checkbox"/> SSAE 16
<input checked="" type="checkbox"/> Safe Harbor	PCI DSS version: 1	<input type="checkbox"/> GLBA	FedRAMP level: Not supported
<input type="checkbox"/> CSA STAR level	<input type="checkbox"/> Privacy Shield	<input type="checkbox"/> FFIEC	<input type="checkbox"/> GAPP
<input type="checkbox"/> COBIT	<input type="checkbox"/> COPPA	<input type="checkbox"/> FERPA	<input type="checkbox"/> HITRUST CSF
<input type="checkbox"/> Jericho Forum Commandments			
10 LEGAL			
<input type="checkbox"/> Data ownership	<input checked="" type="checkbox"/> DMCA	<input type="checkbox"/> Data retention policy	GDPR readiness statement: aws.amaz...
<input checked="" type="checkbox"/> GDPR - Right to erasure	<input checked="" type="checkbox"/> GDPR - Report data breaches	<input checked="" type="checkbox"/> GDPR - Data protection	<input checked="" type="checkbox"/> GDPR - User ownership

GDPR in M365



GDPR - Protect data all over its lifecycle

Dictates to put in place appropriate technical and organizational measures to implement the data protection principles



GDPR compliance use cases

- Discover personal data (PII) in unstructured data
- Ensure data is protected on-premises, in the cloud and on mobile devices
- Grant and restrict access to data
- Gain visibility and control of data stored in cloud apps
- Detect data breaches before they cause damage
- Prove the right things are in place for good faith effort to be compliant
- Manage Data Subject Requests

Adopted on 14 April 2016, enforced on 25 May 2018

Accelerate GDPR compliance with Microsoft 365

The GDPR requires Data Controllers to only use third-party data processors that meet the GDPR requirements for personal data processing. In March 2017, Microsoft made available contractual guarantees that provide these assurances across our cloud services. Customers should evaluate their GDPR responsibilities and learn about the advanced compliance and security capabilities available as add-ons or in suites. Visit Microsoft.com/GDPR for details.

Security & Compliance Controls

- The most secure and up-to-date version of Office & Windows
- Conditional Access (User, Device, app, location)
- Self-service Password reset for on-prem identities
- Advanced Threat Protection: Safe Links, Safe Attachments
- Data Loss Prevention*
- Classification and Labeling
- Multi-Factor Authentication
- Message Encryption and Rights Management
- Mobile device and application Management
- Benchmark your controls with Secure Score
- Gain visibility with the Compliance Manager

Microsoft 365 Business

Unlock: Advanced Compliance & Protection

- Tracking, Reporting, and Revoking Privileges
- Advanced Threat Analytics
- Windows Enterprise: Device Guard, Credential Guard, App Locker, Enterprise Data Protection
- Automatically classify, protect & preserve sensitive data
- Shadow IT Detection with Cloud App Security
- Real Time Risk based access to corporate network
- Anomalous Attack Detection and Reporting
- Additional customer access controls

Microsoft 365 Enterprise E5

Solutions that help customers demonstrate their [GDPR compliance](#)

Compliance Manager: Manage your compliance from one place



Ongoing risk assessment

An intelligent score reflects your compliance posture against regulations or standards



Actionable insights

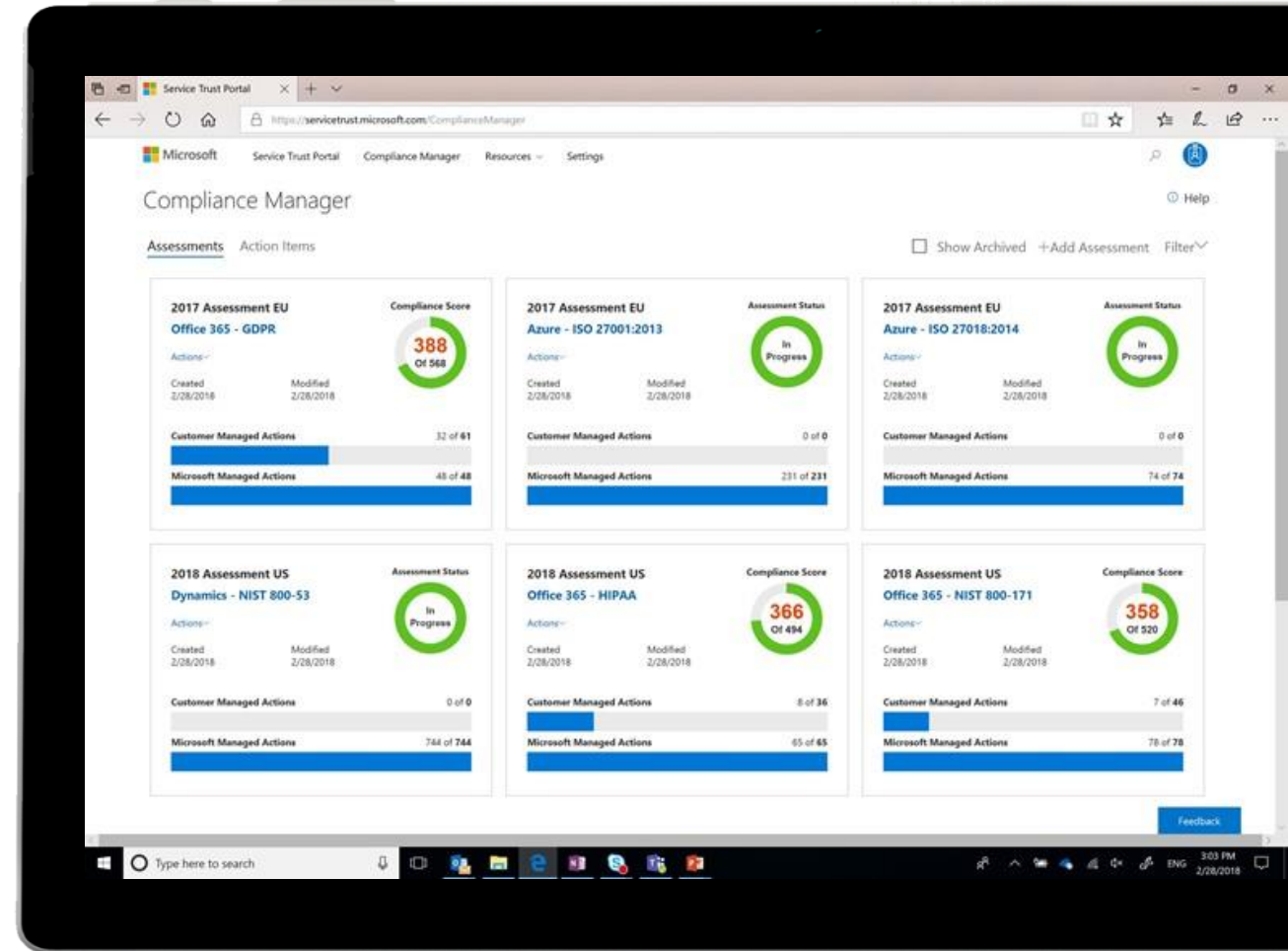
Recommended actions to improve your data protection capabilities



Simplified compliance

Streamlined workflow across teams and richly detailed reports for auditing preparation

Compliance Manager is a dashboard that provides the Compliance Score and a summary of your data protection and compliance stature as well as recommendations to improve data protection and compliance. This is a recommendation, it is up to you to evaluate and validate the effectiveness of customer controls as per your regulatory environment. Recommendations from Compliance Manager and Compliance Score should not be interpreted as a guarantee of compliance.



Let's bring it all together: Microsoft solution

MICROSOFT SECURE

End-to-end approach - safeguard data and prevent leakage – no interfering with user experience
Protect, detect & automatically respond to threats across endpoints, mails, files and IDs
Security capabilities are built in (not bolted on), comprehensive, and integrated



Identity & access management

Protect users' identities & control access to valuable resources based on user risk level

Azure Active Directory
Conditional Access
Windows Hello
Windows Credential Guard
Azure Advanced Threat Protection



Device Protection

Protect against advanced threats and recover quickly when attacked

Microsoft Defender
Advanced Threat Protection
Intune MDM
Windows 10 Application Guard
Windows 10 Application Control
Windows 10 Exploit Guard
Windows 10 Firewall and Defender



Information protection

Ensure documents and emails are seen only by authorized people

Azure Information Protection
Office 365 Advanced Threat Protection
Office 365 Data Loss Prevention
Windows Information Protection
Microsoft Cloud App Security
Intune MAM

Microsoft 365 Security & Compliance platform

March 2019 update v.6.3

New Security & Compliance suites started on Feb. 2019 (*):

Microsoft 365 E5 Security

Microsoft 365 E5 Compliance

(*) for eligible customers with M365 E3 or equivalent Win Ent E3 + EMS E3 + O365 E3 combination of licenses

Latest news: [Announcing Microsoft Defender ATP, TVM, MDATP x Mac !!!](#)

Courtesy of <https://NonSoloSecurity.cloud> by Feliciano Intini (MS #emp)

	Microsoft 365	Windows 10	Enterprise Mobility + Security	Office 365			
Device Protection	M365-E3	WIN-E3	Windows Defender System Guard	EMS-E3	Microsoft Intune	O365-E3/E1	Basic MDM features
Identity Protection & Access Management	M365-E5			EMS-E5 AADP-P2	AAD Identity Governance / Access Review Azure AD Identity Protection Azure AD Privileged Identity Management	O365-E5	Office 365 Privileged Access Management
	M365-E3	WIN-E3	Windows Hello for Business Windows Defender Credential Guard	EMS-E3 AADP-P1	SSO, Self-Service Pwd Reset, App Proxy Azure MFA, Conditional Access Advanced Security Reporting Microsoft Identity Manager Azure AD Premium B2B Collaboration	O365-E3/E1	Limited SSO features Basic MFA features Basic Security Reporting Azure AD Free B2B Collaboration
Information Protection	M365-E5			EMS-E5	Microsoft Cloud App Security (MCAS) Azure Information Protection P2	O365-E5	Office 365 Advanced Data Governance Office 365 Advanced eDiscovery Office 365 Service encryption w/ Customer Keys Office 365 Customer Lockbox
	M365-E3	WIN-E3	Windows Information Protection Bitlocker/BitlockerToGo/MBAM	EMS-E3	Microsoft Intune App Protection Azure Information Protection P1	O365-E3	eDiscovery & Legal Hold Office 365 Data Loss Prevention Office 365 Message Encryption Rights Management for Office 365
MICROSOFT THREAT PROTECTION							
Azure Security (coming soon) → AZURE SENTINEL (*Preview)							
Threat Protection	M365-E5	WIN-E5	Microsoft Defender ATP: Threat & Vuln. Mgmt (TVM), Endpoint Detection & Response (EDR), Auto Investigation & Remediation (AIR), Security Posture, Threat Experts (*Preview)	EMS-E5	Azure Advanced Threat Protection (Azure ATP)	O365-E5	Office 365 ATP P2 (P1+Threat Intelligence)
	M365-E3	WIN-E3	Microsoft Defender ATP: Attack Surface Reduction (Exploit/Network/Ransomware Protection, Application Control), Next Generation Protection (Antimalware)	EMS-E3	Advanced Threat Analytics (ATA)	O365-E3/E1	Office 365 Anti-malware/Anti-Spam (EOP)
Security & Compliance Management	M365-E5				Microsoft 365 Security Center / Microsoft Secure Score / Microsoft 365 Compliance Center		
	M365-E3	WIN-E3	WD Security Center App (on device)	EMS-E3	ATA Portal Microsoft Intune System Center Configuration Manager	O365-E3/E1	Office 365 Security & Compliance Portal Office 365 Secure Score Compliance Manager (GDPR)