



# Leveraging your investment

Microsoft security capabilities you probably already own

**Michael Richards**

Security and Compliance Specialist  
[michael.richards@microsoft.com](mailto:michael.richards@microsoft.com)



Source: Boston Meridian Partners





# Complexity is the enemy of intelligent security

**70** from **35**

Security products

Security vendors

Is the average for companies  
with over 1,000 employees

[Nick McQuire, VP Enterprise Research CCS Insight.](#)

**\$1.37M**

On average that an  
organization spends annually  
in time wasted responding to  
erroneous malware alerts

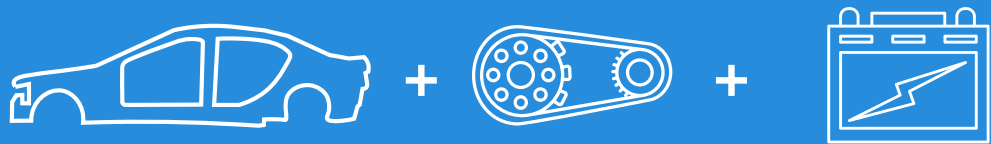
["The Cost of Insecure Endpoints" Ponemon Institute©  
Research Report, June 2017](#)

**1.87M**

Global cybersecurity  
workforce shortage by 2022

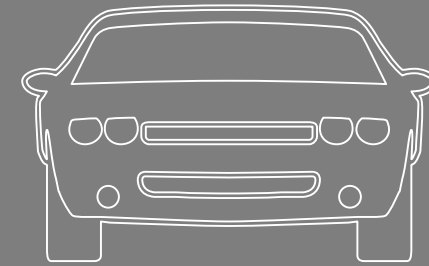
[Global Information Security Workforce Study 2017](#)

# Changing the Conversation

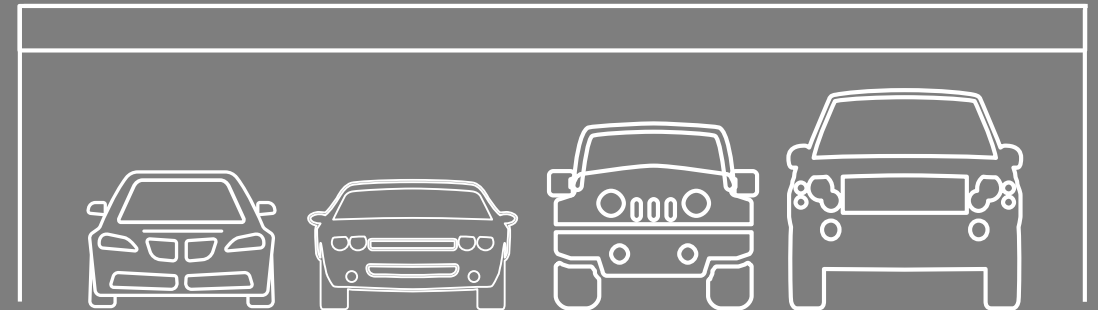


+ ...

Used to assembling “best of breed”  
into a custom solution



Microsoft has already integrated  
security into our products

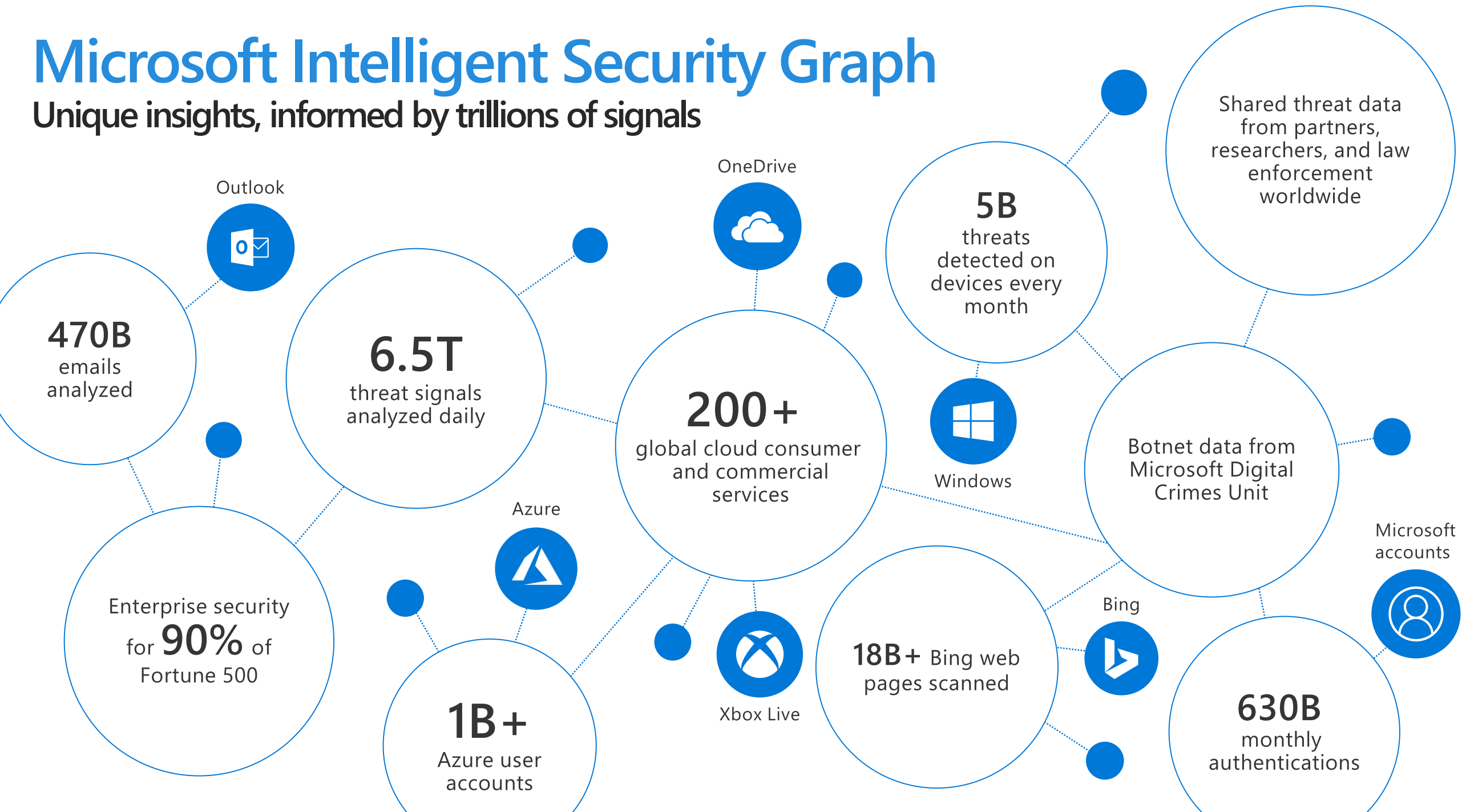


Microsoft integrates with  
existing capabilities



# Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



# Partnerships





## Identity & Access Management

Single Sign-on (SSO)  
Multi-Factor Authentication (MFA)  
Access Control  
Privileged Access Management (PAM)

Secrets Management



## Information Protection

Data Loss Prevention (DLP)  
Data Encryption  
Information Protection  
Data Classification  
Data Governance  
Cloud Access Security Broker (CASB)  
Key Management  
Mobile Application Management

Database Security  
Encrypted Cloud Storage  
Back Up  
Disaster Recovery

Virtual Private Networks (VPN)



## Threat Protection

Secure Email Gateway  
Endpoint Detection and Response (EDR)  
Endpoint Protection (EPP)  
Anti-phishing  
Anti-virus/ Anti-malware  
User and Entity Behavior Analytics (UEBA)  
Anomaly Detection  
Threat Intelligence Feeds  
Remote Browser  
Intrusion Detection System (IDS)  
Intrusion Prevention System (IPS)  
Host intrusion prevention system (HIPS)  
Host Firewall

IoT Protection  
Cloud Workload Protection  
DDoS Protection  
Incident Response Services

Cross-platform endpoint protection

Incident Ticket System  
Network Firewall  
Mobile Threat Detection tools

⊗ Network traffic analysis (NTA)  
⊗ Container Security\*  
⊗ Anti-tamper software\*  
⊗ Deception  
⊗ Web content filtering



## Security Management

Security Scoring  
Reporting

Cloud-based Management  
SIEM (SIM/ SEM/ Log management)

Asset Discovery  
Pen Testing/ Risk Assessment  
Vulnerability Assessment  
Web Application Testing  
Managed detection and response (MDR)  
SOC  
Security training

Security categories M365 Enterprise covers

Security categories other Microsoft solutions cover

What Microsoft Services/ MSSPs/ ISVs cover

What Microsoft integrates with

⊗ What Microsoft doesn't do

# Endpoint Protection (Antivirus)

*Applies to:*

*Windows 10*

*Windows Server 2016*

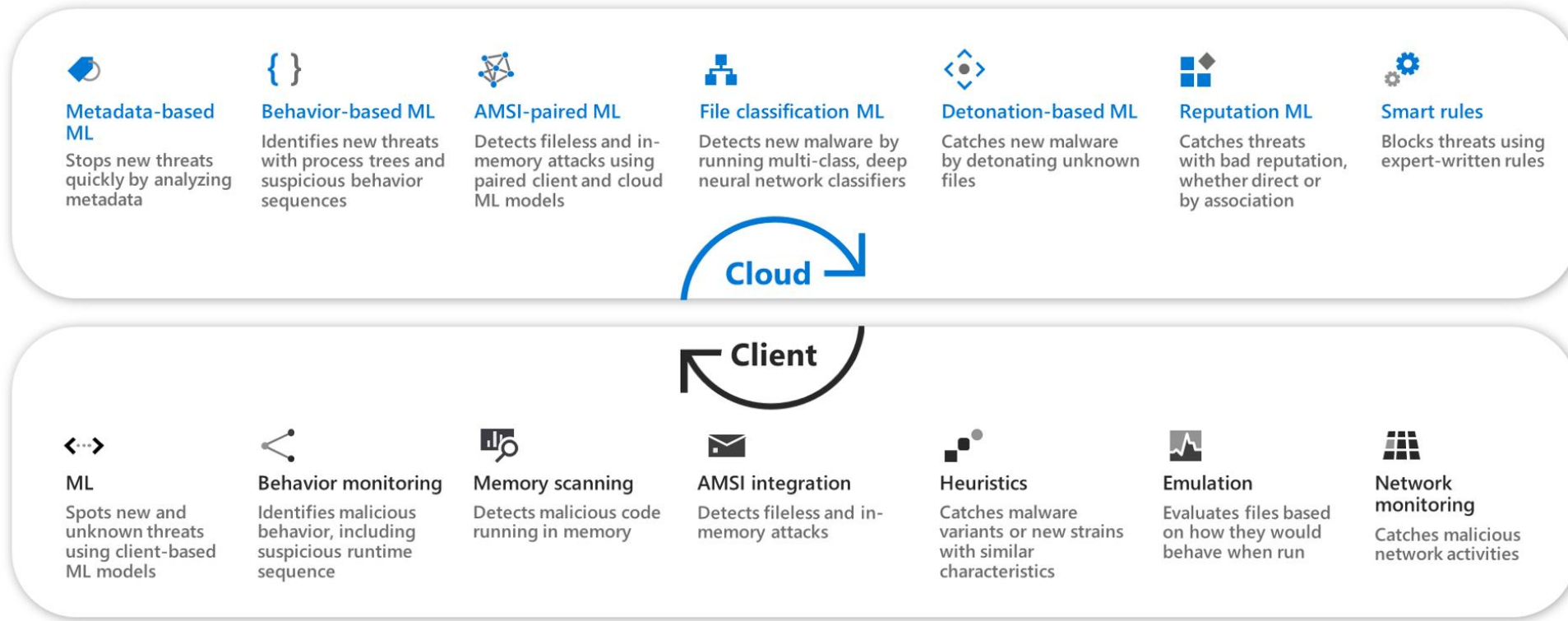
*Windows Server 2019*

*Windows 8.1*

*Windows 7\**

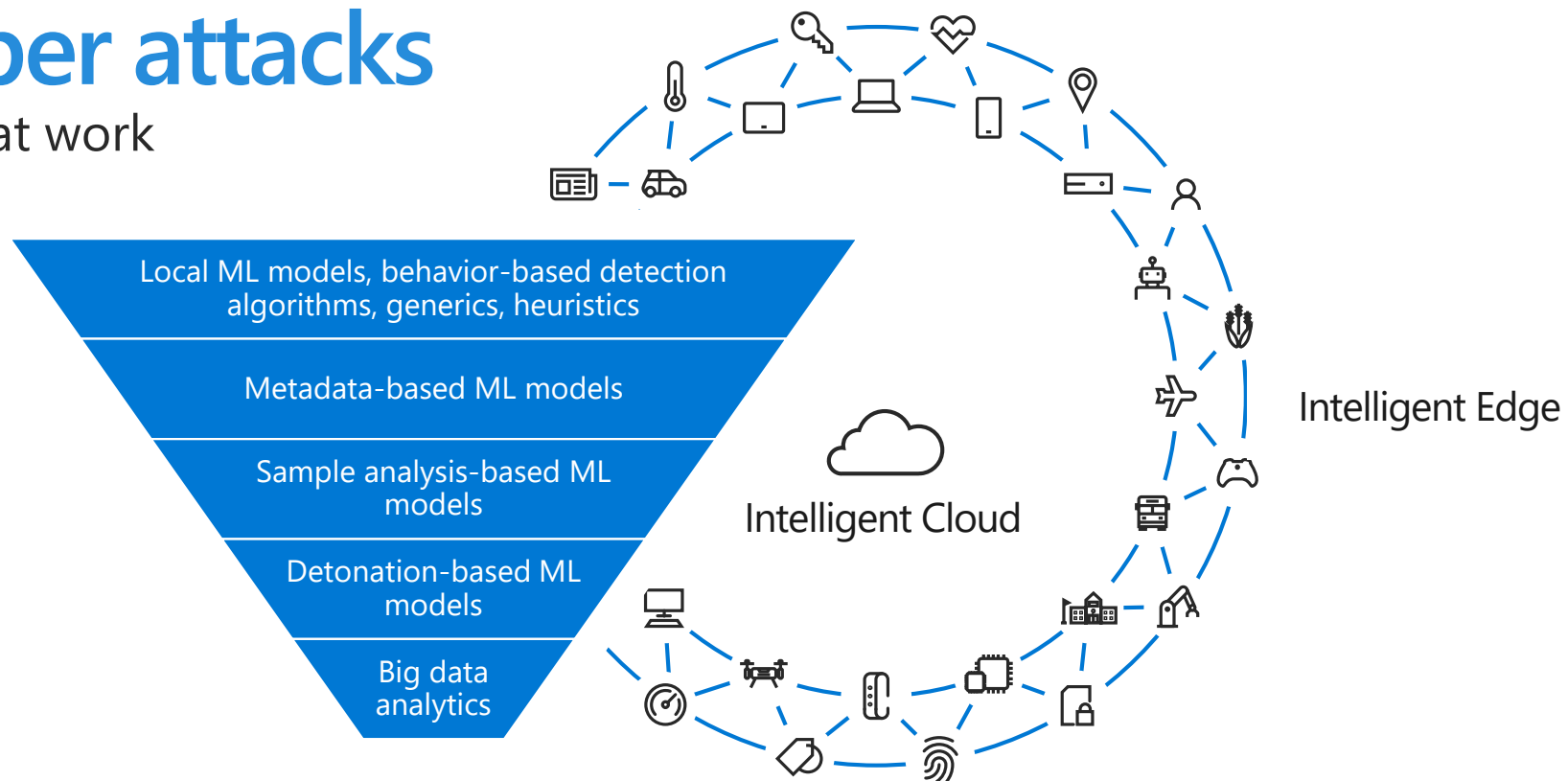


# Microsoft Defender next-gen protection engines



# Stopping cyber attacks

Real-world intelligence at work



**October 2017** – Cloud-based detonation ML models identified [Bad Rabbit](#), protecting users 14 minutes after the first encounter.

**March 6** – Behavior-based detection algorithms blocked more than 400,000 instances of the [Dofoil](#) trojan.

**February 3** – Client machine learning algorithms automatically stopped the malware attack [Emotet](#) in real time.

**August 2018** – Cloud machine learning algorithms blocked a highly targeted campaign to deliver [Ursnif](#) malware to under 200 targets

2017

2018

# Cloud Protection and Block at First Sight

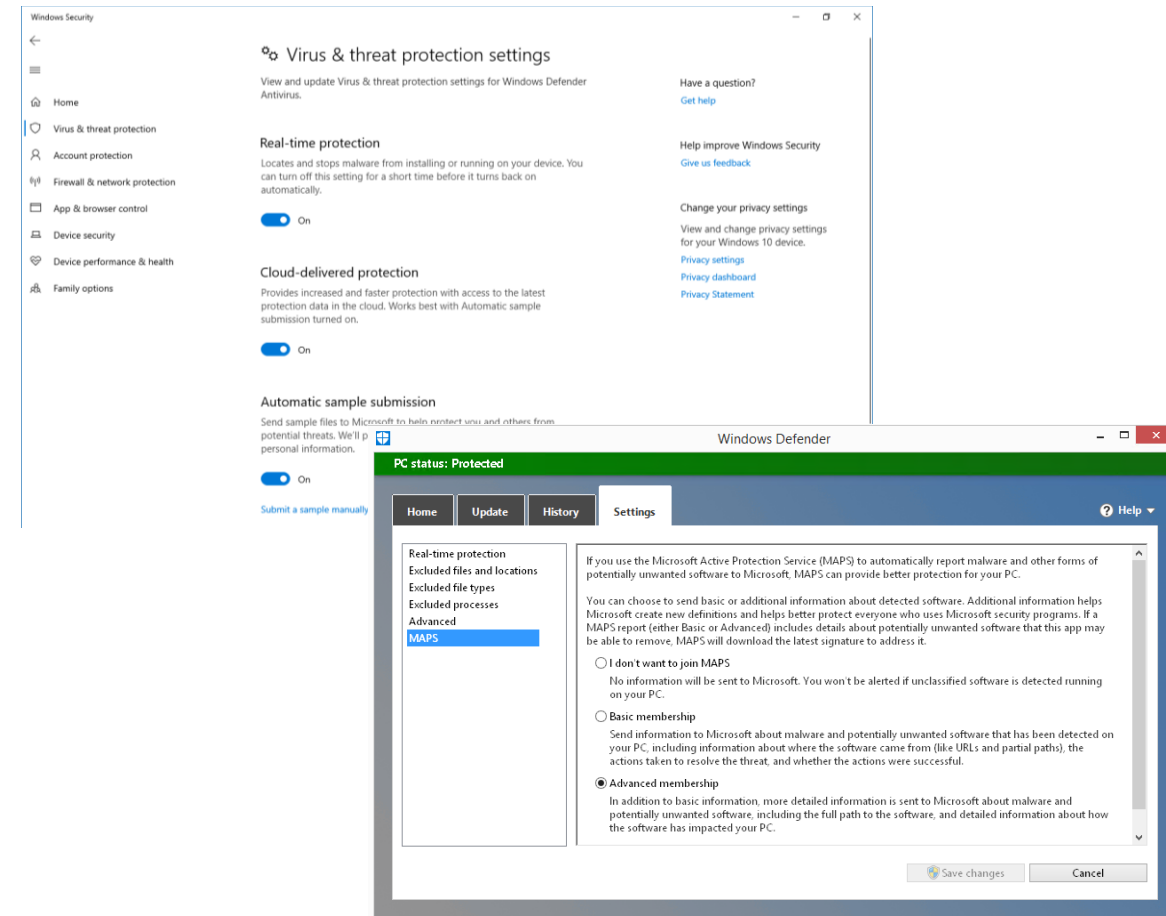
**Cloud-delivered Protection** is enabled by default in Windows 10 (opt-in to MAPS for Windows 7/8.1)

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/utilize-microsoft-cloud-protection-windows-defender-antivirus>

**Block at First Sight** requires Windows 10 1607 or later.

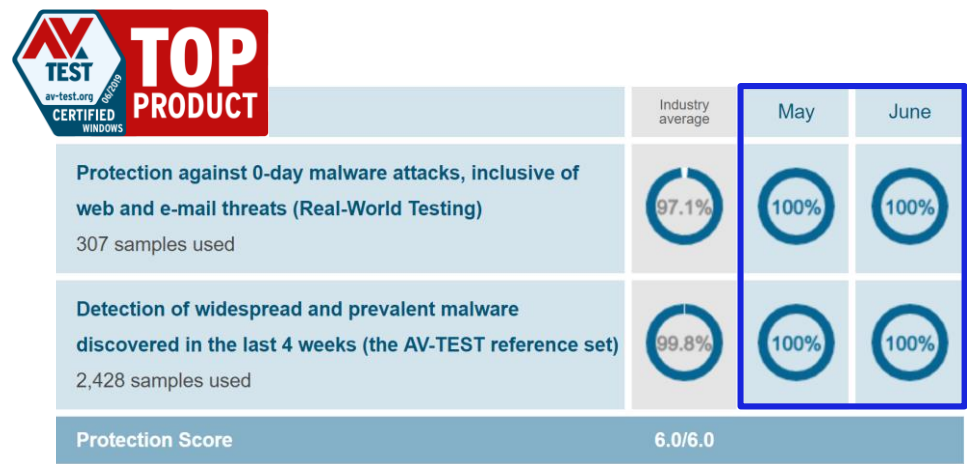
Windows 10 1803 or later blocks non-PE files (JS, VBS, macros)

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-block-at-first-sight-windows-defender-antivirus>





# Don't take our word for it...



Technique	Step	Microsoft	Cybereason	CrowdStrike w/ managed service	Endgame	CarbonBlack	CounterTack	SentinelOne	FireEye w/ managed service	RSA
Credential Dumping (T1003)	5.A.1	Alert	Alert	Alert	Alert	Alert	None	None	None	None
Credential Dumping (T1003)	5.A.2	Telemetry	Telemetry	Alert	Alert	Telemetry	Telemetry	None	None	None
Input Capture (T1055)	15.A.1	Alert	Alert	Alert	None	Telemetry	None	Telemetry	None	None
Input Capture (T1055)	8.C.1	Alert	None	None	None	None	None	Telemetry	None	None
Process Injection (T1056)	3.C.1	Alert	Alert	Alert	Alert	Alert	Alert	Telemetry	Alert	Telemetry
Process Injection (T1056)	5.A.1	Alert	Alert	Telemetry	Telemetry	Telemetry	Alert	None	None	None
Process Injection (T1056)	5.A.2	Alert	Alert	Telemetry	Alert	Alert	Alert	Telemetry	None	None
Process Injection (T1056)	8.D.1	Telemetry	Alert	Telemetry	Alert	Telemetry	Telemetry	Telemetry	None	None

Coverage of critical techniques as evaluated by MITRE



## Security Pros: Embrace The Change

For security pros that have been around awhile, don't let your cynicism cloud (pardon our pun . . .) the potential advantages your organization could experience by making use of these tools **Take off the tinfoil hat, and realize that Microsoft is a security company now.**

What Google and Microsoft have introduced will make the entire industry better, and that's something to applaud.

<https://go.forrester.com/blogs/tech-titans-google-and-microsoft-are-transforming-cybersecurity/>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/top-scoring-industry-antivirus-tests>

## Windows Defender is the best antivirus around, claims testing lab

By Darren Allan · a day ago · Software

Microsoft's antivirus is joint top with three others – but they're paid offerings



<https://www.techradar.com/news/windows-defender-is-the-best-antivirus-around-claims-testing-lab>

PCMag Australia | Windows 10 | News

## Windows Defender Achieves 'Best Antivirus' Status

BY MATTHEW HUMPHRIES 6 AUG 2019, 9:30 P.M.

AV-TEST awarded Microsoft's security solution its top score and 'Top Product' award, which only 3 other (premium) antivirus products achieved.

<https://au.pcmag.com/windows-10/63049/windows-defender-achieves-best-antivirus-status>

# Password Protection

*Applies to:*

*Office 365 E1/E3/E5\**

*Microsoft 365 Business\**

*Microsoft 365 E3/E5*

*Azure Active Directory Premium*

# Eliminate weak passwords

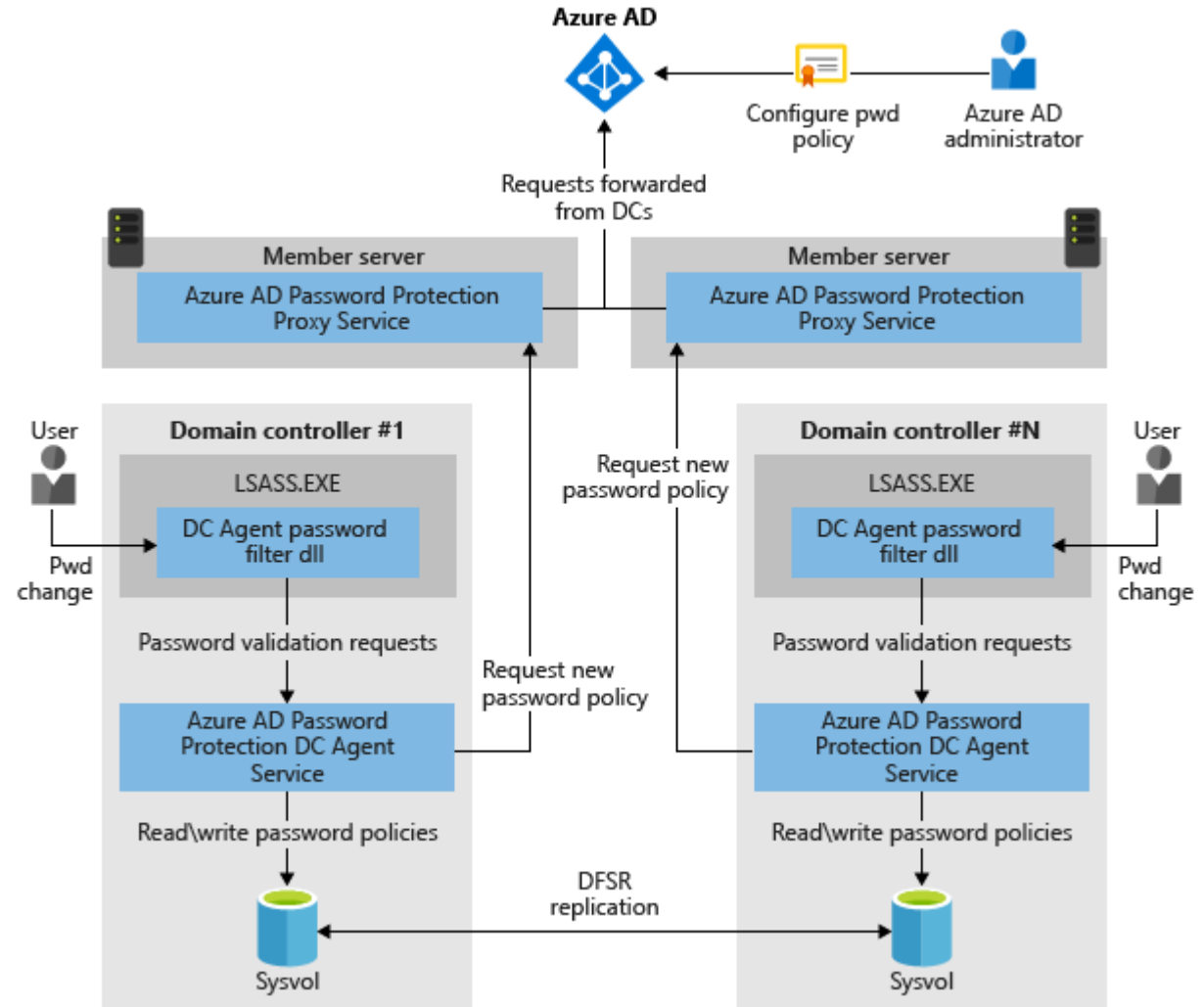
## Cloud-only users:

- global banned list applies to all Azure AD accounts
- custom banned list requires Azure AD Premium

## On-premises (Active Directory):

- requires Azure AD Premium

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>





# Multi-factor Authentication

*Applies to:*

*Office 365 E1/E3/E5*

*Office 365 Business Essentials/Premium*

*Microsoft 365 Business*

*Microsoft 365 E3/E5*

*Azure Active Directory Premium*

# Secure authentication using MFA

Multi-factor authentication prevents 99.9% of identity attacks



Push  
notification



SMS



Voice call

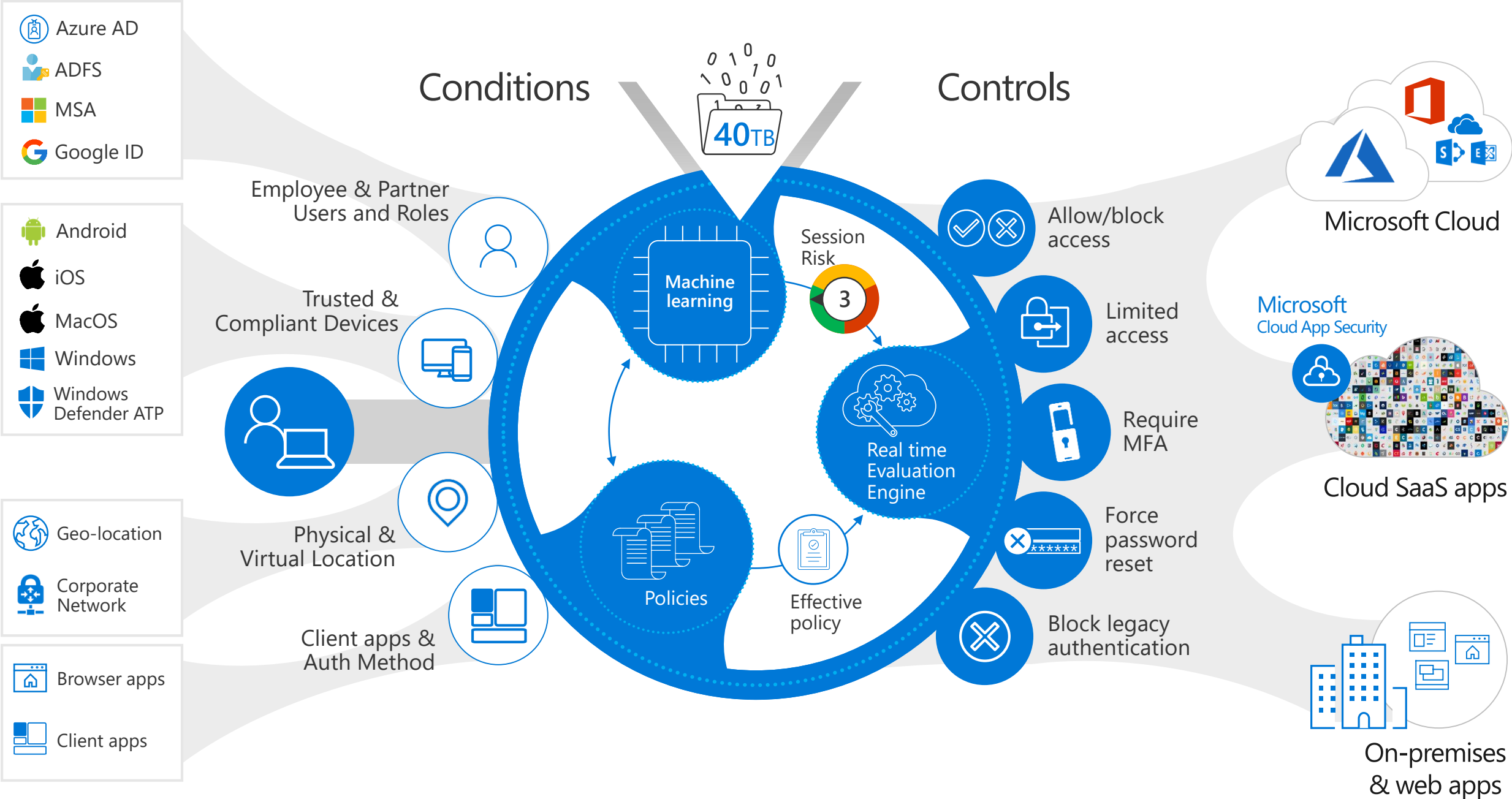


OATH  
Token



OATH  
codes

# Conditional Access



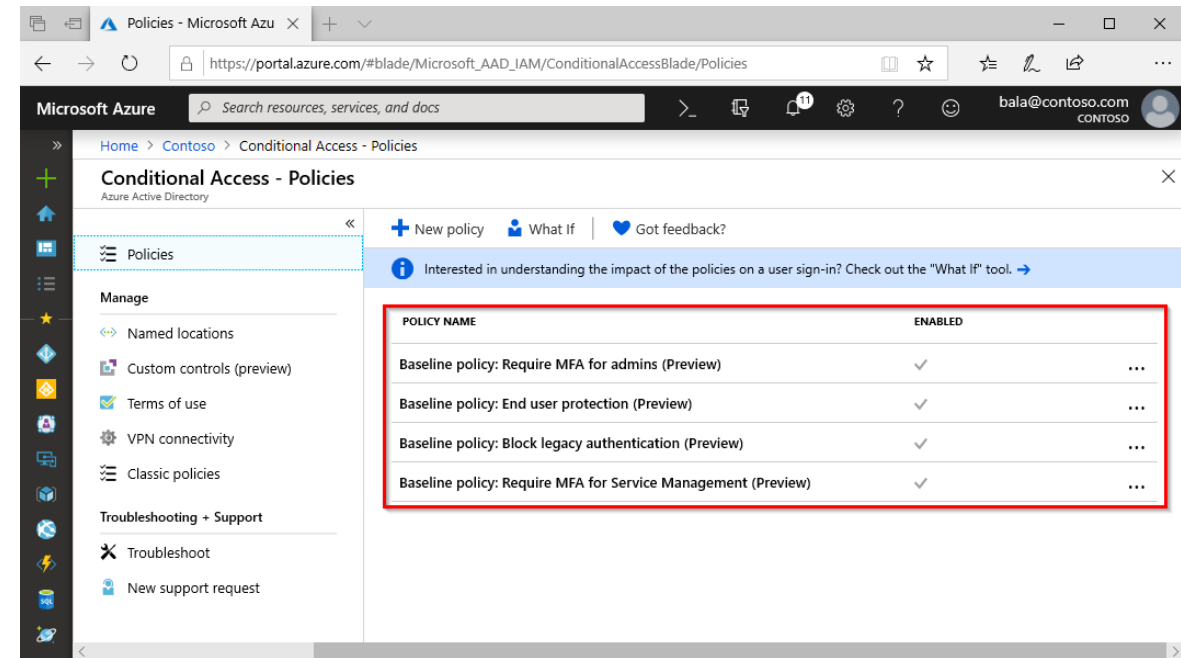


# Azure Multi-Factor Authentication

**Azure Active Directory Premium** or **Microsoft 365 Business** - Full featured MFA

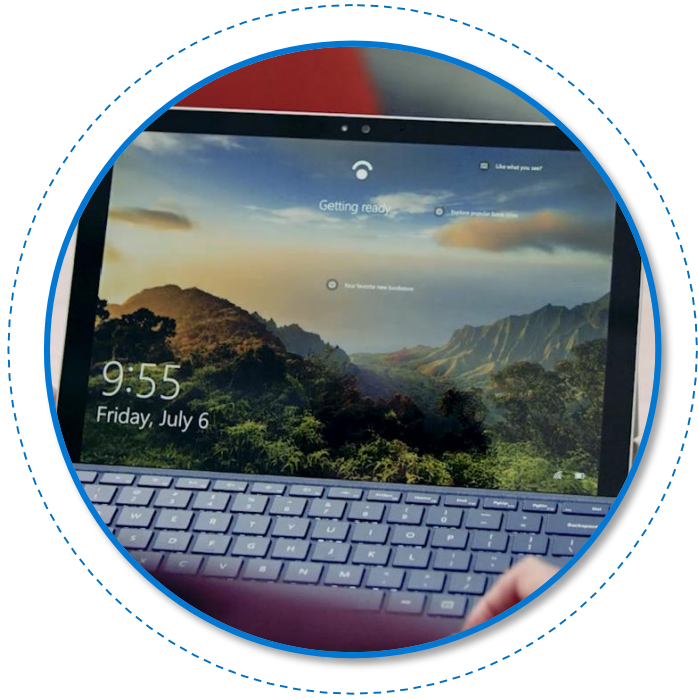
**Azure AD Free** or standalone **Office 365** licenses - use pre-created Conditional Access baseline protection policies

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>



# Getting to a world without passwords

High security, convenient methods of strong authentication



Windows Hello



Microsoft Authenticator



FIDO2 Security Keys

# Application whitelisting

*Applies to:*

*Windows 10*

*Windows Server 2016*

*Windows Server 2019*

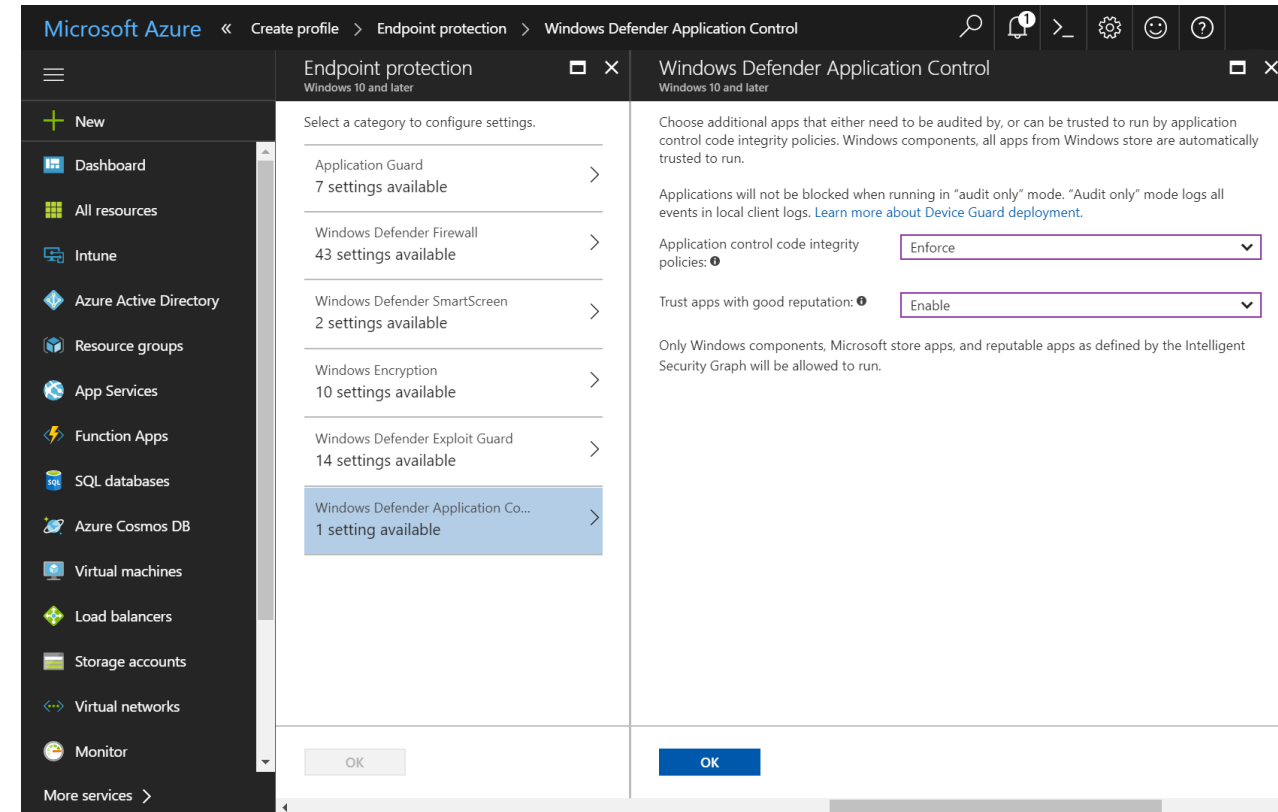
# Windows Defender Application Control

**Restrict applications** that users are allowed to run and the code that runs in the System Core (kernel).

**Block unsigned scripts and MSIs**, and control whether specific plug-ins, add-ins, and modules can run from specific apps.

**Trusted Installer** and **ISG** options to simplify deployment.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control>



# Secure access to on-premises web applications

*Applies to:*

*Office 365 E1/E3/E5*

*Microsoft 365 Business*

*Microsoft 365 E3/E5*

*Azure Active Directory Premium*



# Azure AD Application Proxy

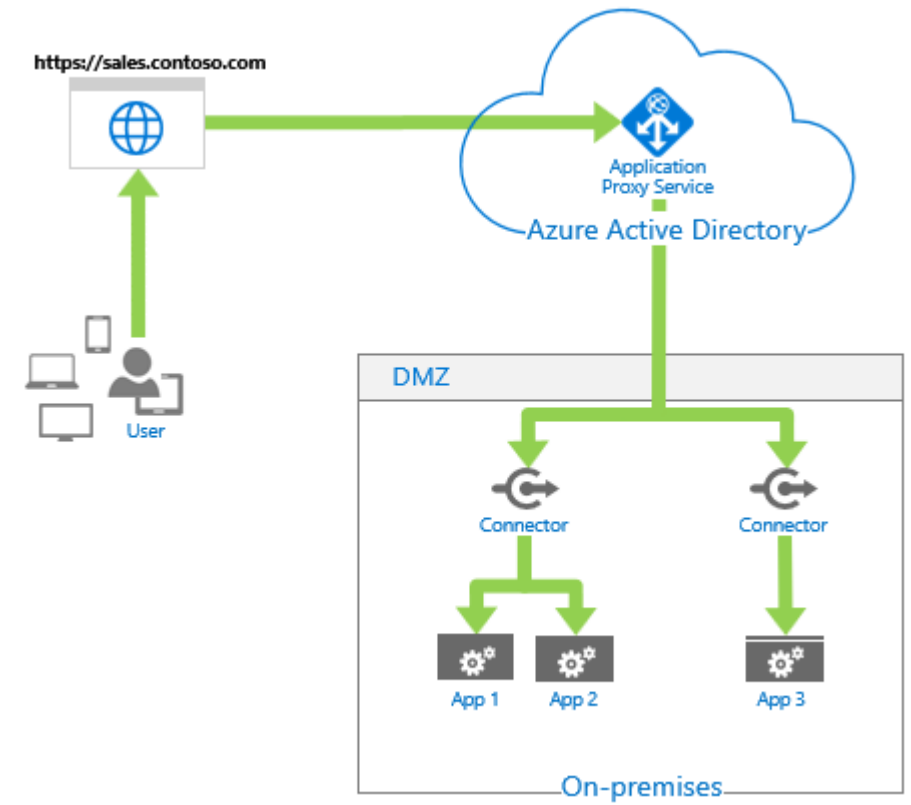
## Publish on-premises web apps

externally without a DMZ

Support **single sign-on** across devices, resources and apps

Support **multi-factor authentication** for apps hosted on-premises

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-proxy>



# Data loss prevention

*Applies to:*

*Office 365 E3/E5*

*Microsoft 365 Business*

*Microsoft 365 E3/E5*

# Office 365 Data Loss Prevention

**Identify sensitive information** across Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams\*

**Prevent accidental sharing** of sensitive information

**Help users learn** to stay compliant

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

The screenshot displays the Office 365 Data Loss Prevention (DLP) interface. On the left, a sidebar lists categories: Financial, Medical and health, Privacy (selected), and Custom. The main area shows the 'Australia Privacy Act' policy, specifically 'Australia Personally Identifiable Information (PII) Data'. A description states: 'Helps detect the presence of information commonly considered to be personally identifiable information (PII) in Australia, like tax file number and driver's license.' It also lists what is protected: 'Australia Tax File Number' and 'Australia Driver's License Number'.

Below this, a 'Policy Tip' is shown for a file named 'Book1' on OneDrive. The tip states: 'This file conflicts with a policy in your organization. If you don't resolve this conflict, access to this file might be blocked.' It lists issues: 'This file contains the U.S. Social Security Number' and provides a 'Resolve' button.

In the foreground, an email composition window is visible. It shows a 'Policy tip' notification at the top: 'Policy tip: Your email message conflicts with a policy in your organization. Learn more'. Below this, the email fields (To, Cc, Subject) are visible. An attachment named 'SSN.txt' (167 bytes) is highlighted with a red box, indicating it is the source of the policy conflict.

# Information protection

*Applies to:*

*Office 365 E3/E5*

*Microsoft 365 Business*

*Microsoft 365 E3/E5*

*Azure Information Protection*

# Office 365 Message Encryption

Share protected email with anyone on any device

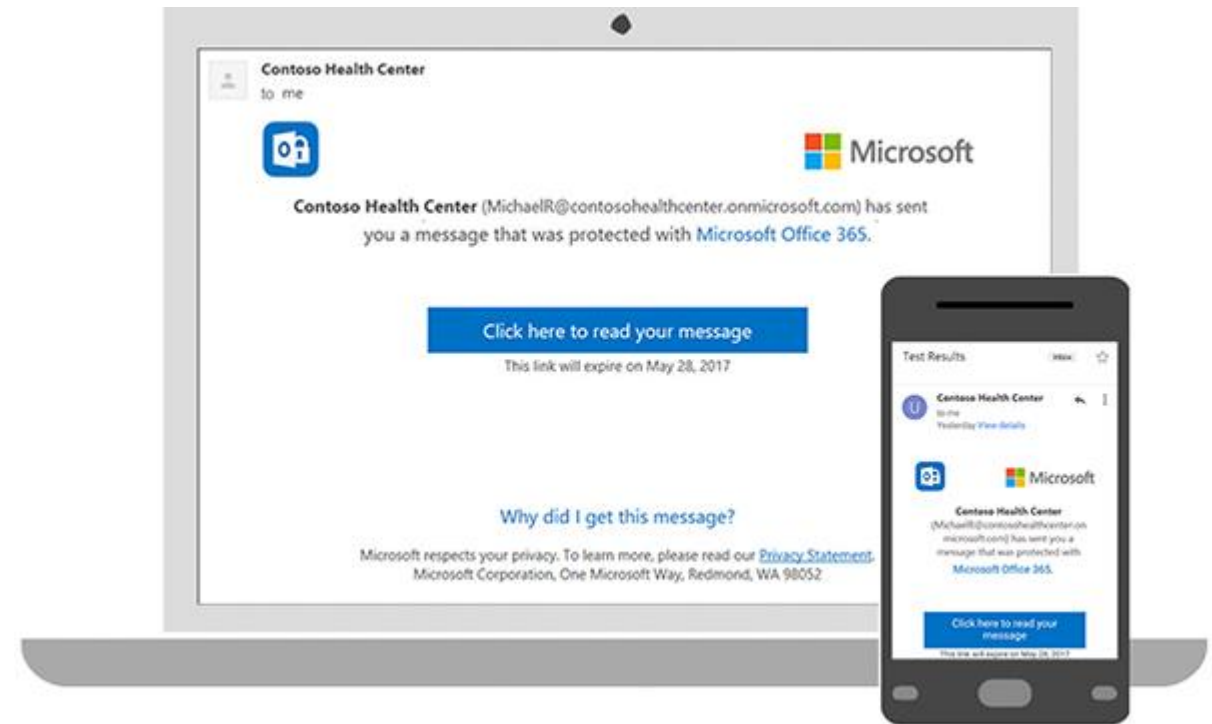
Leverages protection features in **Azure Rights Management Services**

Set specific permissions such as **Do Not Forward** or Do Not Print

**Transparent to Office 365 users** with Outlook 2016 or Outlook on the web

Sign in to **Gmail** or **a single-use code**

<https://docs.microsoft.com/en-us/office365/securitycompliance/ome>





# Azure Information Protection

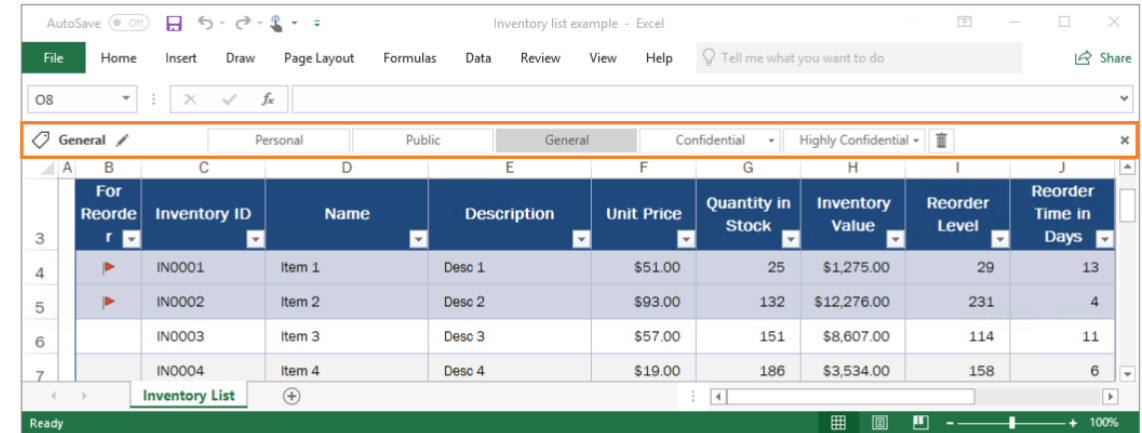
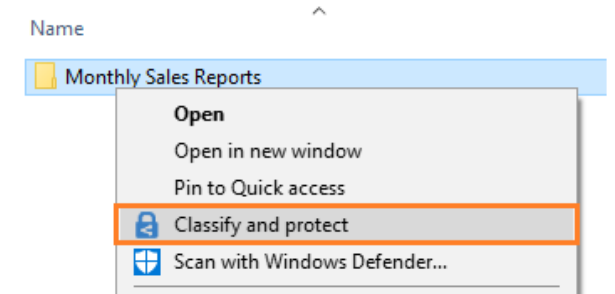
**Classify and optionally protect** documents and emails by applying labels

Flexible **role-based taxonomy**

Mandatory, default and **automatic classification**

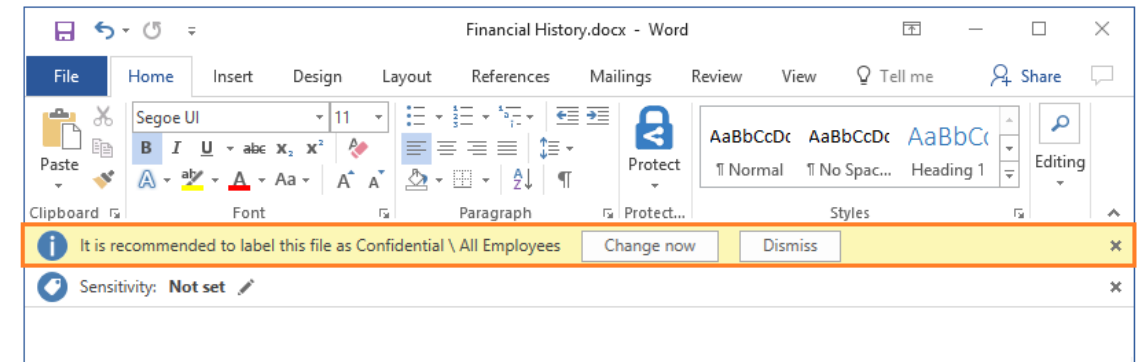
**Visual markings** such as header, footer or watermark. **Metadata** in clear text for use with other services

<https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection>



A screenshot of an Excel spreadsheet titled 'Inventory list example'. The spreadsheet contains a table with the following data:

Inventory ID	Name	Description	Unit Price	Quantity in Stock	Inventory Value	Reorder Level	Reorder Time in Days
IN0001	Item 1	Desc 1	\$51.00	25	\$1,275.00	29	13
IN0002	Item 2	Desc 2	\$93.00	132	\$12,276.00	231	4
IN0003	Item 3	Desc 3	\$57.00	151	\$8,607.00	114	11
IN0004	Item 4	Desc 4	\$19.00	186	\$3,534.00	158	6



# Security baselines

*Applies to:*

*Windows 10*

*Windows Server 2016*

*Windows Server 2019*

*Intune*

# Windows security baselines

Microsoft Baseline Security Analyzer has been deprecated

Evaluate **Patch compliance with WSUS/SCCM** or WUA offline script

Security baselines with Group Policy and the **Security Compliance Toolkit**

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>

Secure the modern desktop using **MDM security baselines**

<https://docs.microsoft.com/en-us/intune/security-baselines>

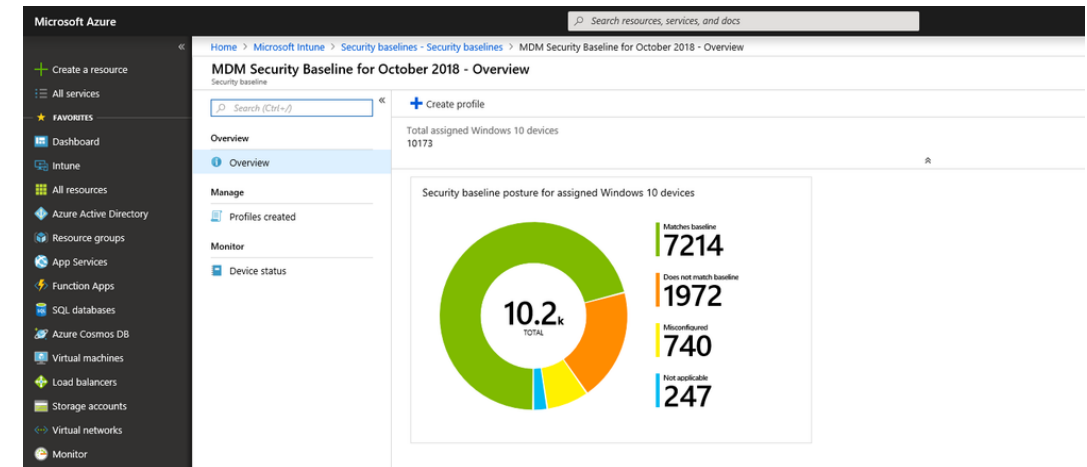
Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	STIG-Win10-2015-	Win10-IE11-Basel...
HKCU	Software\Policies\Microsoft\Window...	NoToastApplicationNotification...		1	1
HKLM	Software\Microsoft\WcmSvc\wifin...	AutoConnectAllowedOEM		0	0
HKLM	Software\Microsoft\Windows NT\Cu...	SecurityLevel	0	0	0
HKLM	Software\Microsoft\Windows NT\Cu...	CachedLogonsCount	10		4
HKLM	Software\Microsoft\Windows NT\Cu...	ScRemoveOption	0	1	1
HKLM	Software\Microsoft\Windows\Curren...	EnumerateAdministrators		0	0
HKLM	Software\Microsoft\Windows\Curren...	NoAutorun		1	1
HKLM	Software\Microsoft\Windows\Curren...	NoDriveTypeAutoRun		255	255
HKLM	Software\Microsoft\Windows\Curren...	NoWebServices		1	1
HKLM	Software\Microsoft\Windows\Curren...	ConsentPromptBehaviorAdmin	5	2	2
HKLM	Software\Microsoft\Windows\Curren...	ConsentPromptBehaviorUser	3	0	0
HKLM	Software\Microsoft\Windows\Curren...	DisableAutomaticRestartSignOn		1	1
HKLM	Software\Microsoft\Windows\Curren...	EnableInstallerDetection	1	1	1
HKLM	Software\Microsoft\Windows\Curren...	EnableLUA	1	1	1

**Policy Path:**  
User Configuration  
Start Menu and Taskbar\Notificat...\br/>Turn off toast notifications on the lock screen

**Local registry:**  
Not specified

**STIG-Win10-2015-10-30:**  
Option: Enabled  
Data: 1  
Type: REG\_DWORD

**Win10-IE11-Baselines-DRAFT:**  
Option: Enabled  
Data: 1  
Type: REG\_DWORD





Date : \_\_\_\_\_

# To Do List

1. Consider a Microsoft-first approach to security

2. Evaluate built-in capabilities

3. Enable Multi-Factor Authentication (MFA)

4. Provide feedback/suggestions on community engagement to

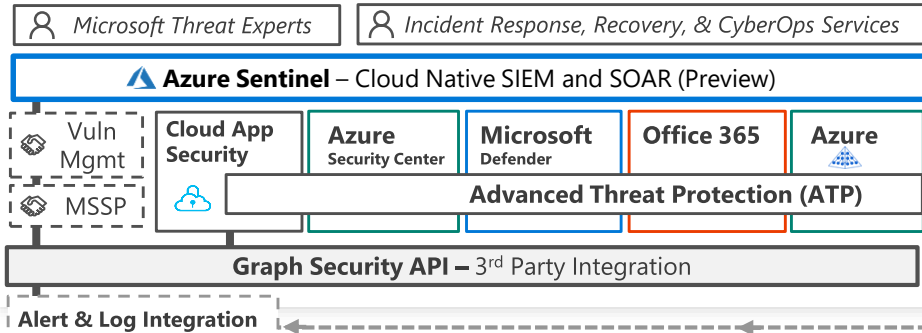
[michael.richards@microsoft.com](mailto:michael.richards@microsoft.com)

[@microsoft.com](mailto:michael.richards@microsoft.com)





## Security Operations Center (SOC)



## Cybersecurity Reference Architecture

April 2019 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

### Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petya\)](#)

## Software as a Service

### Office 365

Secure Score  
Customer Lockbox



### Dynamics 365

### Information Protection

### Identity & Access

Azure Active Directory

### Conditional Access – Identity Perimeter Management

Cloud App Security

### Azure Information Protection (AIP)

Discover  
Classify  
Protect  
Monitor

Hold Your Own Key (HYOK)

### AIP Scanner



### Office 365

- [Data Loss Protection](#)
- [Data Governance](#)
- [eDiscovery](#)

Azure SQL  
Threat Detection

SQL Encryption &  
Data Masking

Azure SQL Info  
Protection

Microsoft Defender ATP

Azure AD Identity Protection  
Leaked cred protection  
Behavioral Analytics

Azure AD PIM

Multi-Factor  
Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

## Clients

### Unmanaged & Mobile Devices



Intune MDM/MAM

### Managed Clients



System Center  
Configuration Manager

Microsoft Defender ATP



Secure Score  
Threat Analytics

## Windows 10 Enterprise Security

Network protection  
Credential protection  
Exploit protection  
Reputation analysis  
Full Disk Encryption  
Attack surface reduction

App control  
Isolation  
Antivirus  
Behavior monitoring

S Mode

## Hybrid Cloud Infrastructure

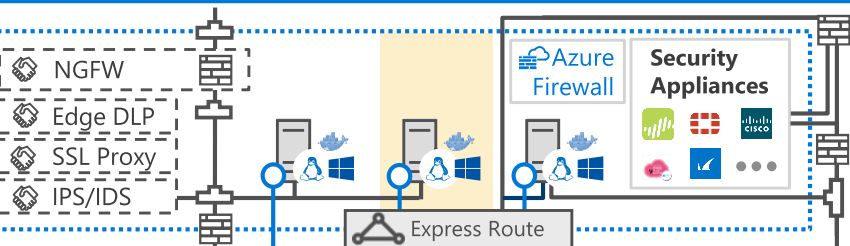
On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Extranet



Windows Server 2019 Security  
Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs  
Azure Stack

Privileged Access Workstations (PAWs)



## IoT and Operational Technology

Windows 10 IoT

Azure IoT Security



Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.)  
Premium Security Feature

Security Development Lifecycle (SDL)

Configuration Hygiene  
Just in Time VM Access  
Adaptive App Control

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network  
Security Groups

Backup & Site  
Recovery

Disk & Storage  
Encryption

Confidential  
Computing

DDoS attack  
Mitigation+Monitor

Compliance Manager

Trust Center

Intelligent Security Graph







Thank you.