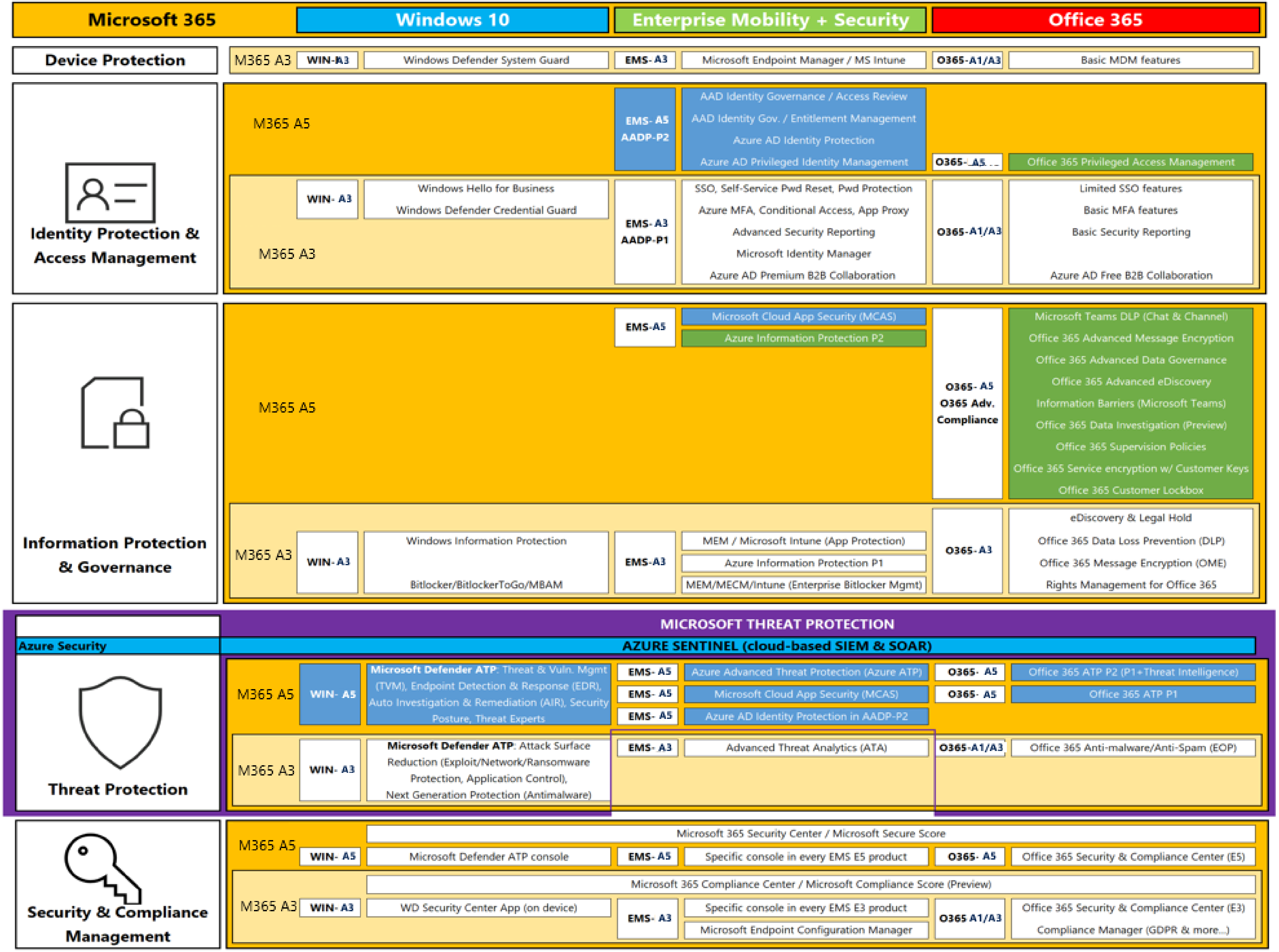
Microsoft

Microsoft 365 Security & Compliance platform

Microsoft 365 A5 Security

Microsoft 365 A5 Compliance



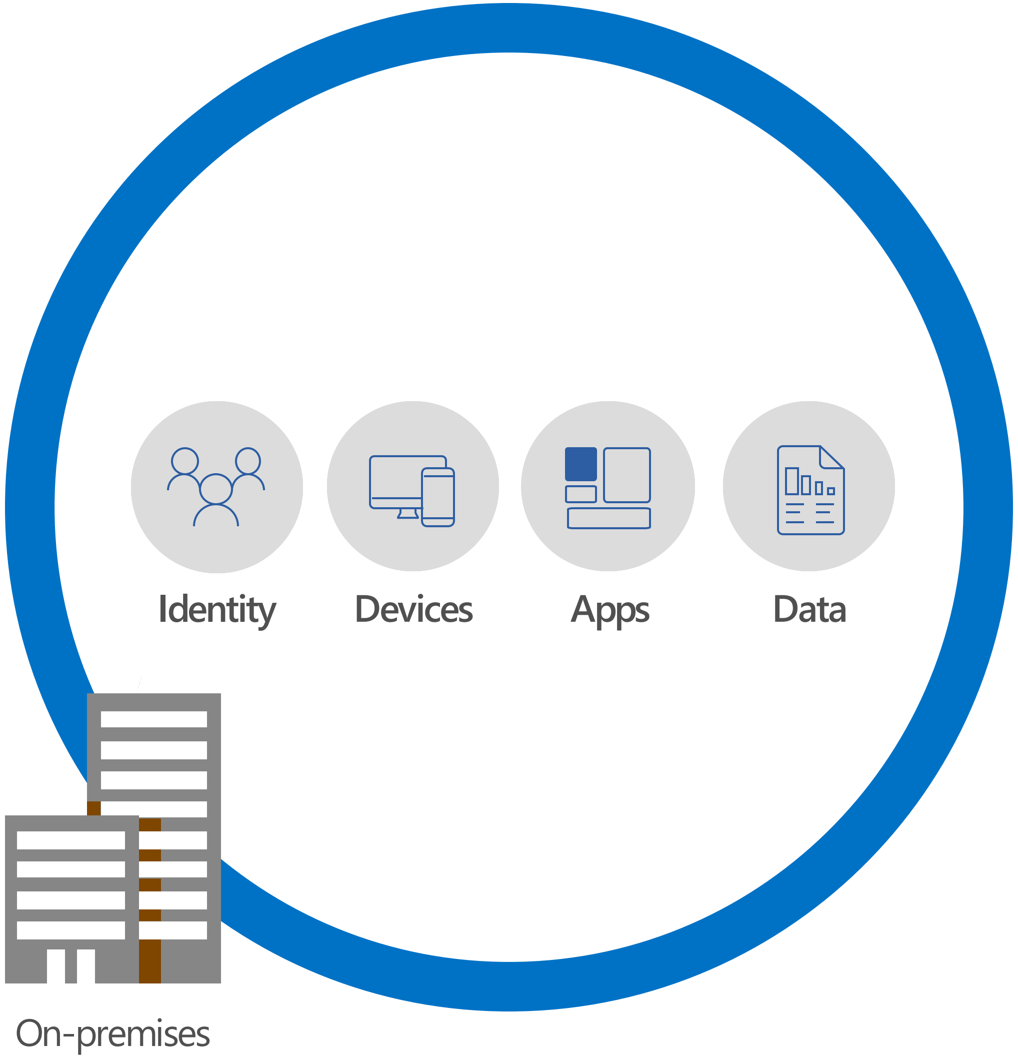
Microsoft 365		Windows 10		Enterprise Mobility + Security		Office 365	
Device Protection	M365 A3	WIN-A3	Windows Defender System Guard	EMS- A3	Microsoft Endpoint Manager / MS Intune	O365-A1/A3	Basic MDM features
Identity Protection & Access Management	M365 A5			EMS- A5 AADP-P2	AAD Identity Governance / Access Review AAD Identity Gov. / Entitlement Management Azure AD Identity Protection Azure AD Privileged Identity Management	O365- A5	Office 365 Privileged Access Management
	M365 A3	WIN- A3	Windows Hello for Business Windows Defender Credential Guard	EMS- A3 AADP-P1	SSO, Self-Service Pwd Reset, Pwd Protection Azure MFA, Conditional Access, App Proxy Advanced Security Reporting Microsoft Identity Manager Azure AD Premium B2B Collaboration	O365-A1/A3	Limited SSO features Basic MFA features Basic Security Reporting Azure AD Free B2B Collaboration
Information Protection & Governance	M365 A5			EMS-A5	Microsoft Cloud App Security (MCAS) Azure Information Protection P2	O365- A5 O365 Adv. Compliance	Microsoft Teams DLP (Chat & Channel) Office 365 Advanced Message Encryption Office 365 Advanced Data Governance Office 365 Advanced eDiscovery Information Barriers (Microsoft Teams) Office 365 Data Investigation (Preview) Office 365 Supervision Policies Office 365 Service encryption w/ Customer Keys Office 365 Customer Lockbox
	M365 A3	WIN-A3	Windows Information Protection Bitlocker/BitlockerToGo/MBAM	EMS-A3	MEM / Microsoft Intune (App Protection) Azure Information Protection P1 MEM/MECM/Intune (Enterprise Bitlocker Mgmt)	O365-A3	eDiscovery & Legal Hold Office 365 Data Loss Prevention (DLP) Office 365 Message Encryption (OME) Rights Management for Office 365
		MICROSOFT THREAT PROTECTION					
Azure Security		AZURE SENTINEL (cloud-based SIEM & SOAR)					
Threat Protection	M365 A5	WIN- A5	**Microsoft Defender ATP**: Threat & Vuln. Mgmt (TVM), Endpoint Detection & Response (EDR), Auto Investigation & Remediation (AIR), Security Posture, Threat Experts	EMS- A5 EMS- A5 EMS- A5	Azure Advanced Threat Protection (Azure ATP) Microsoft Cloud App Security (MCAS) Azure AD Identity Protection in AADP-P2	O365- A5 O365- A5	Office 365 ATP P2 (P1+Threat Intelligence) Office 365 ATP P1
	M365 A3	WIN- A3	**Microsoft Defender ATP**: Attack Surface Reduction (Exploit/Network/Ransomware Protection, Application Control), Next Generation Protection (Antimalware)	EMS- A3	Advanced Threat Analytics (ATA)	O365-A1/A3	Office 365 Anti-malware/Anti-Spam (EOP)
Security & Compliance Management	M365 A5		Microsoft 365 Security Center / Microsoft Secure Score				
		WIN- A5	Microsoft Defender ATP console	EMS- A5	Specific console in every EMS E5 product	O365- A5	Office 365 Security & Compliance Center (E5)
	M365 A3		Microsoft 365 Compliance Center / Microsoft Compliance Score (Preview)				
		WIN- A3	WD Security Center App (on device)	EMS- A3	Specific console in every EMS E3 product Microsoft Endpoint Configuration Manager	O365 A1/A3	Office 365 Security & Compliance Center (E3) Compliance Manager (GDPR & more...)

Microsoft

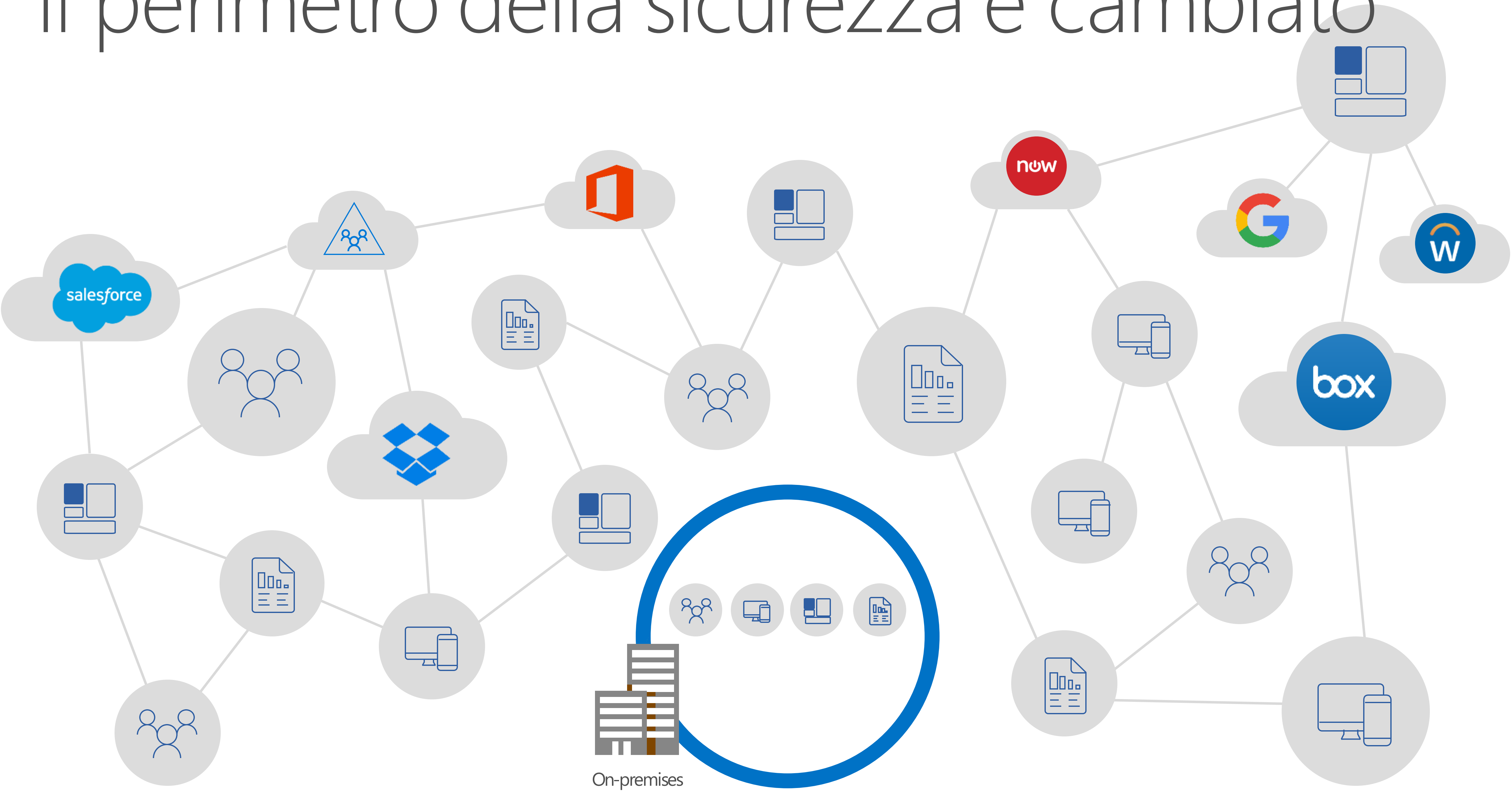
Security with Microsoft

Patrizio Rinaldi
SR Technical Specialist, Microsoft Italia - Security and Compliance
prinaldi@microsoft.com

Il perimetro della sicurezza è cambiato

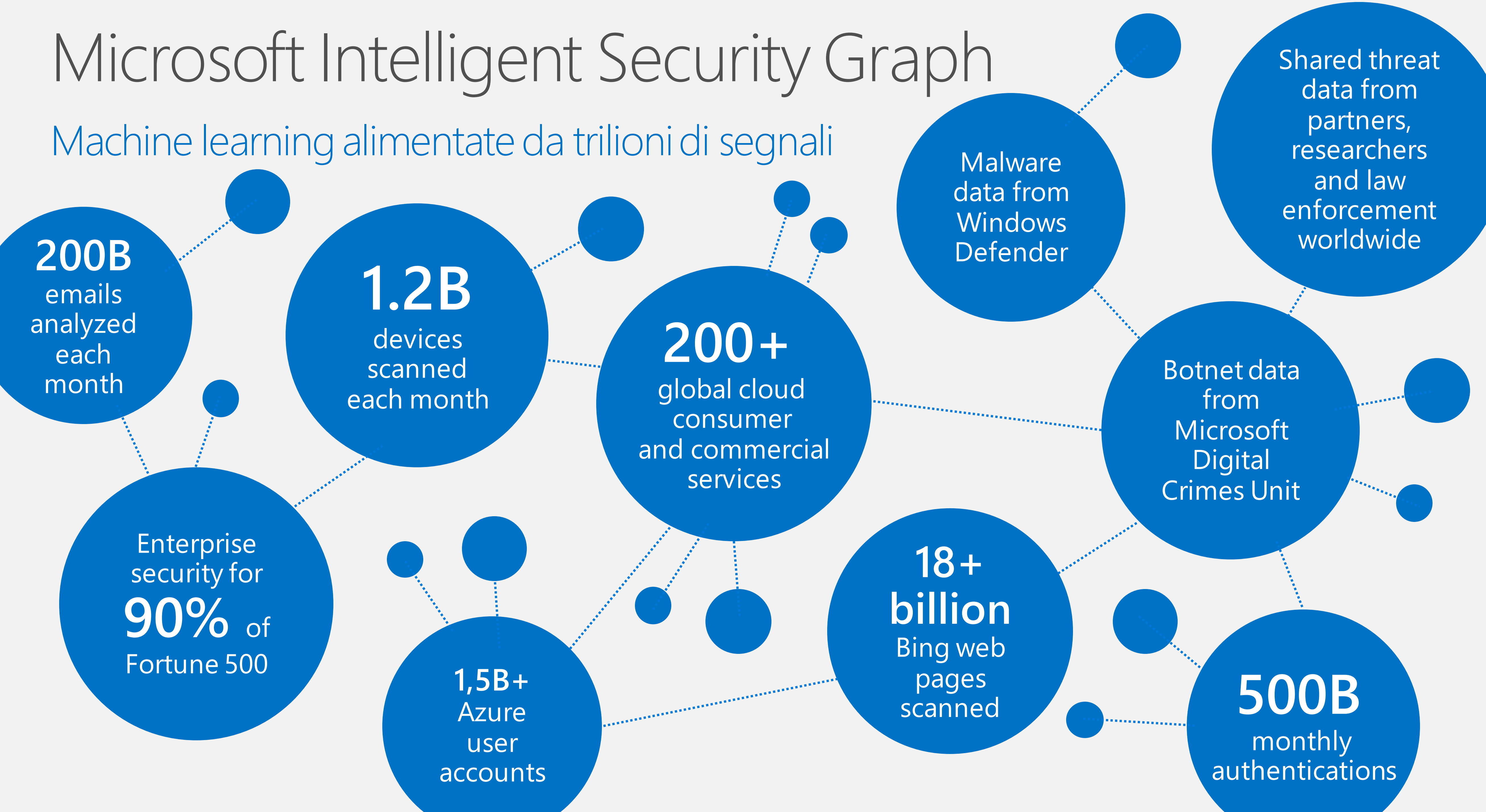


Il perimetro della sicurezza è cambiato



Microsoft Intelligent Security Graph

Machine learning alimentate da trilioni di segnali



200B
emails analyzed each month

1.2B
devices scanned each month

Enterprise security for **90%** of Fortune 500

200+
global cloud consumer and commercial services

1,5B+
Azure user accounts

Malware data from Windows Defender

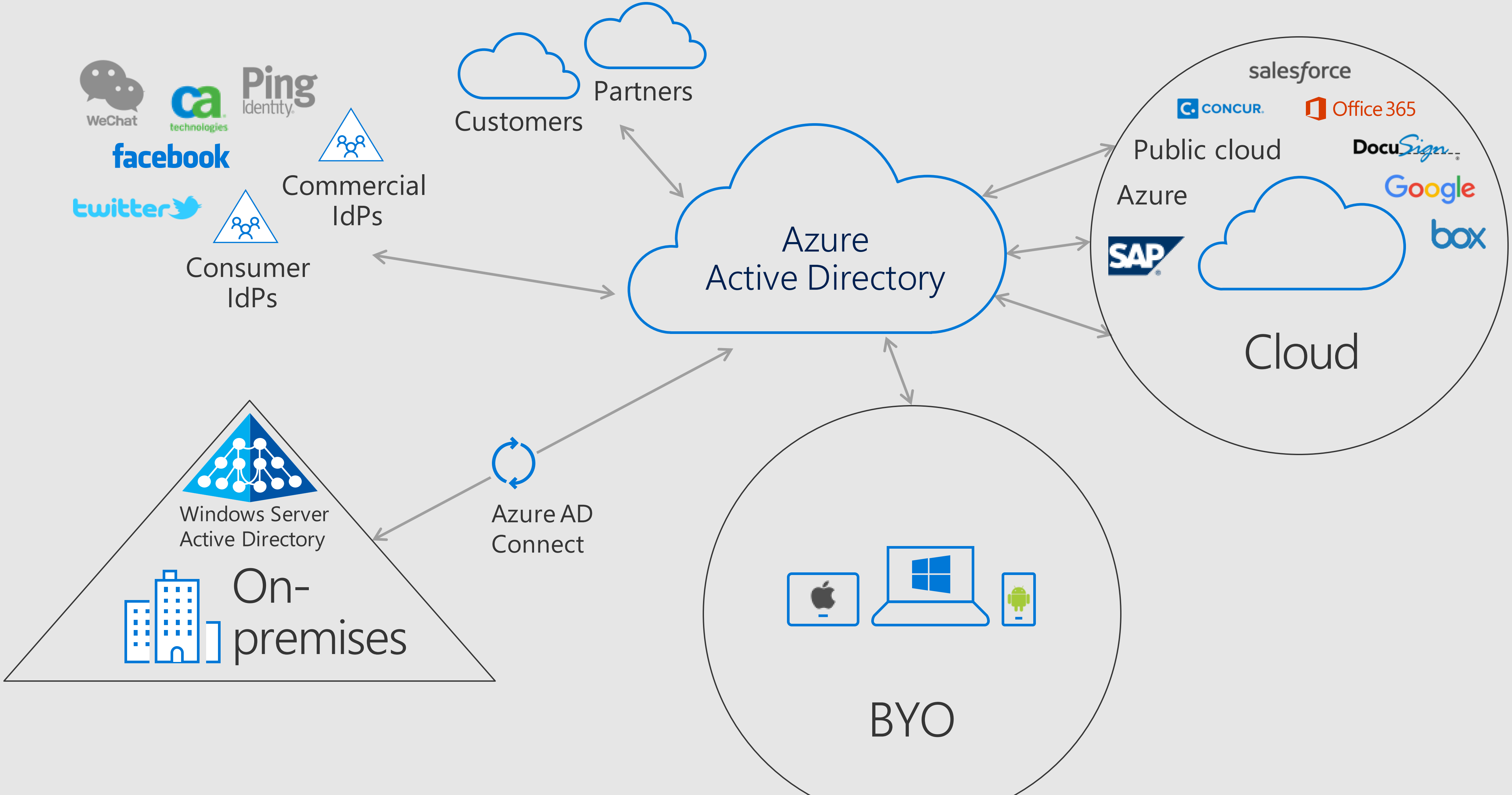
Shared threat data from partners, researchers and law enforcement worldwide

Botnet data from Microsoft Digital Crimes Unit

18+ billion
Bing web pages scanned

500B
monthly authentications

L'identità è il nuovo pannello di controllo



Protezione avanzata degli accessi

Utenze specifiche

Identità

Appartenenza a gruppi

Dispositivo usato

Gestito o non gestito

Compliant o non compliant

Tipologia (Windows, iOS, Android)

Perso o rubato

Applicazione

Applicabile a livello di singola applicazione

Tipo di applicazione usata (Web, mobile rich app)

Altro

Provenienza (paese, IP)

Profilo di rischio della sessione

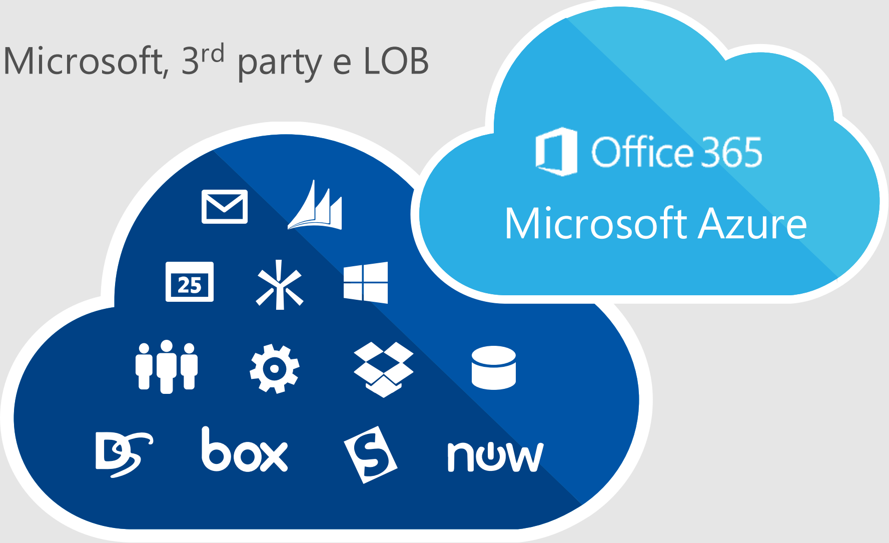
ALLOW

BLOCK

ENFORCE MFA

Applicazione Cloud o
Applicazioni aziendali locali

Microsoft, 3rd party e LOB



Mobile Apps

Push One-Time Passcode (OTP) Token

Phone Calls

Out-of-Band Call

Text Messages

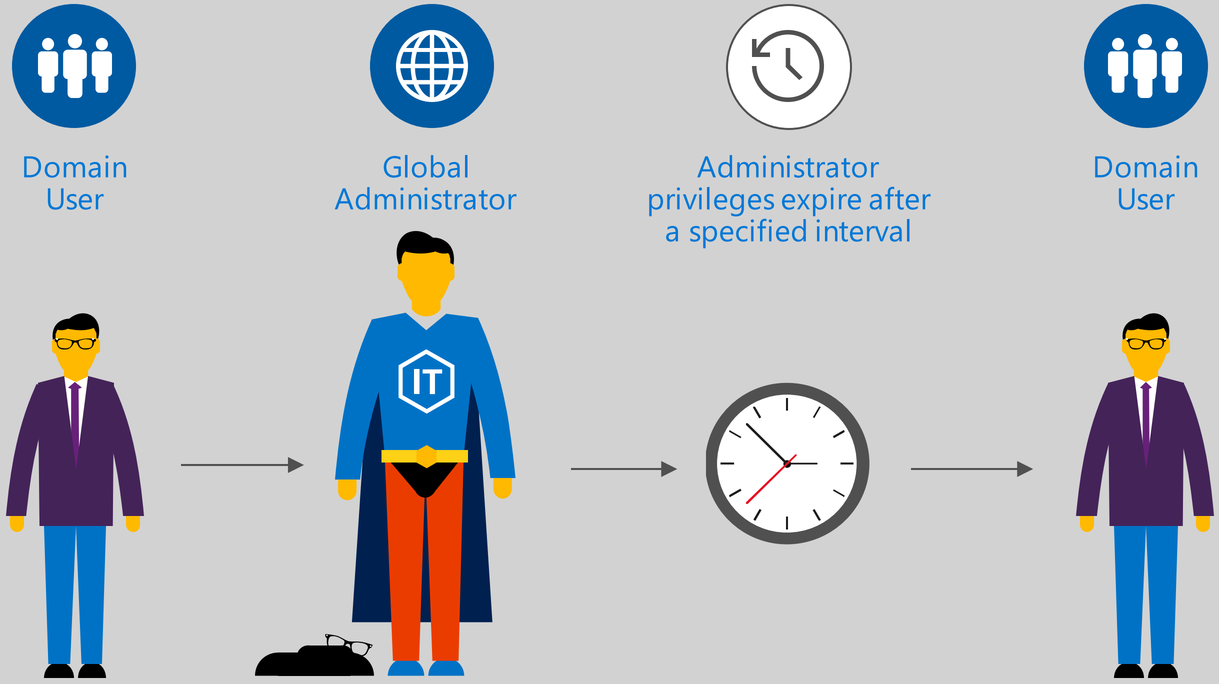
Text One-Time Passcode (OTP) by Text

Gestione delle identità privilegiate

Individuare, limitare e monitorare le identità privilegiate

Abilita l'accesso amministrativo on-demand e just-in-time solo quando necessario

Abilita avvisi e reportistica per la gestione e revisione degli accessi

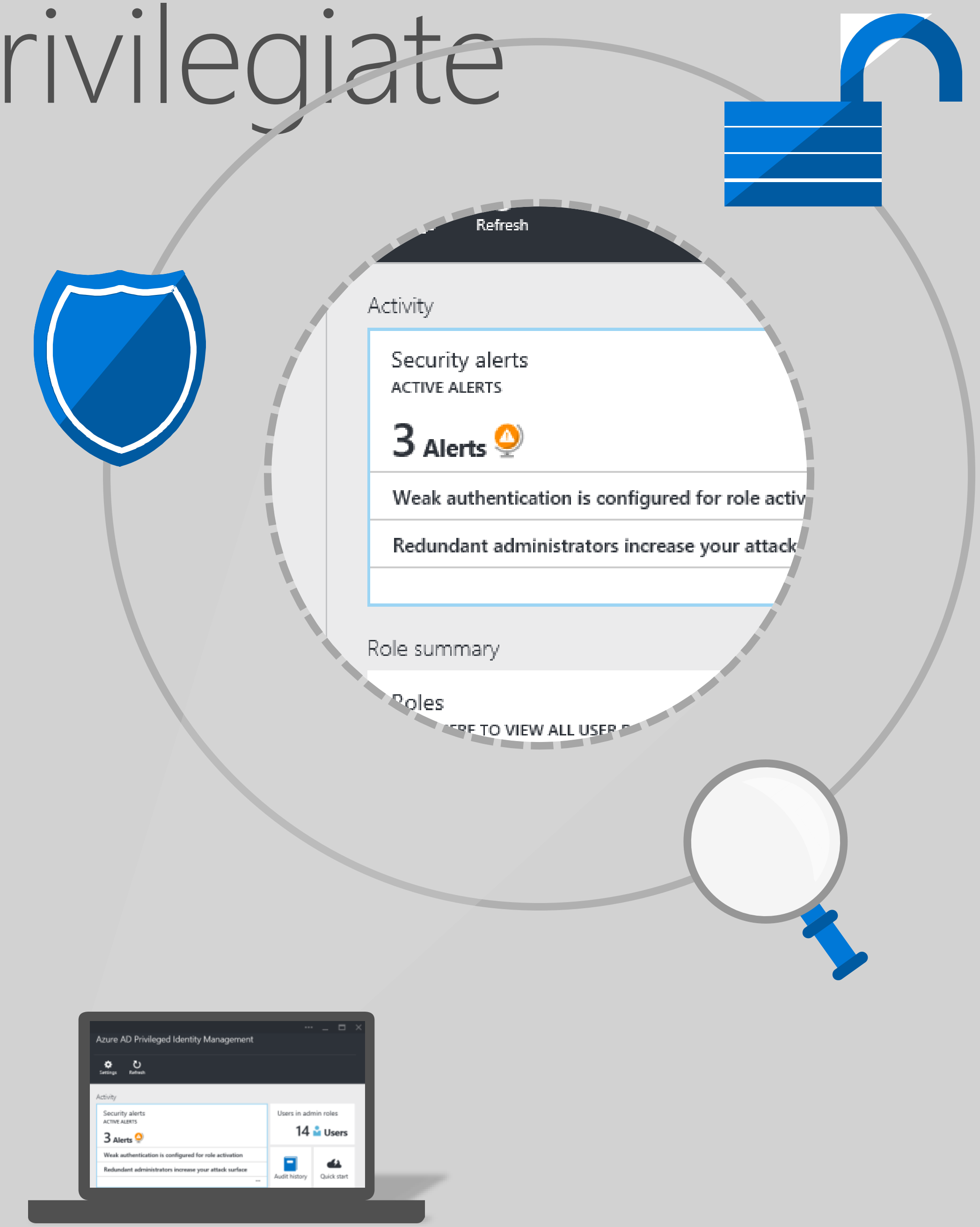


Domain User

Global Administrator

Administrator privileges expire after a specified interval

Domain User



Security alerts
ACTIVE ALERTS
3 Alerts
Weak authentication is configured for role activ
Redundant administrators increase your attack

Security alerts
ACTIVE ALERTS
3 Alerts
Weak authentication is configured for role activation
Redundant administrators increase your attack surface

Users in admin roles
14 Users

PROTECT & GOVERN

Azure AD Identity Governance

Identity lifecycle
facilities collaboration

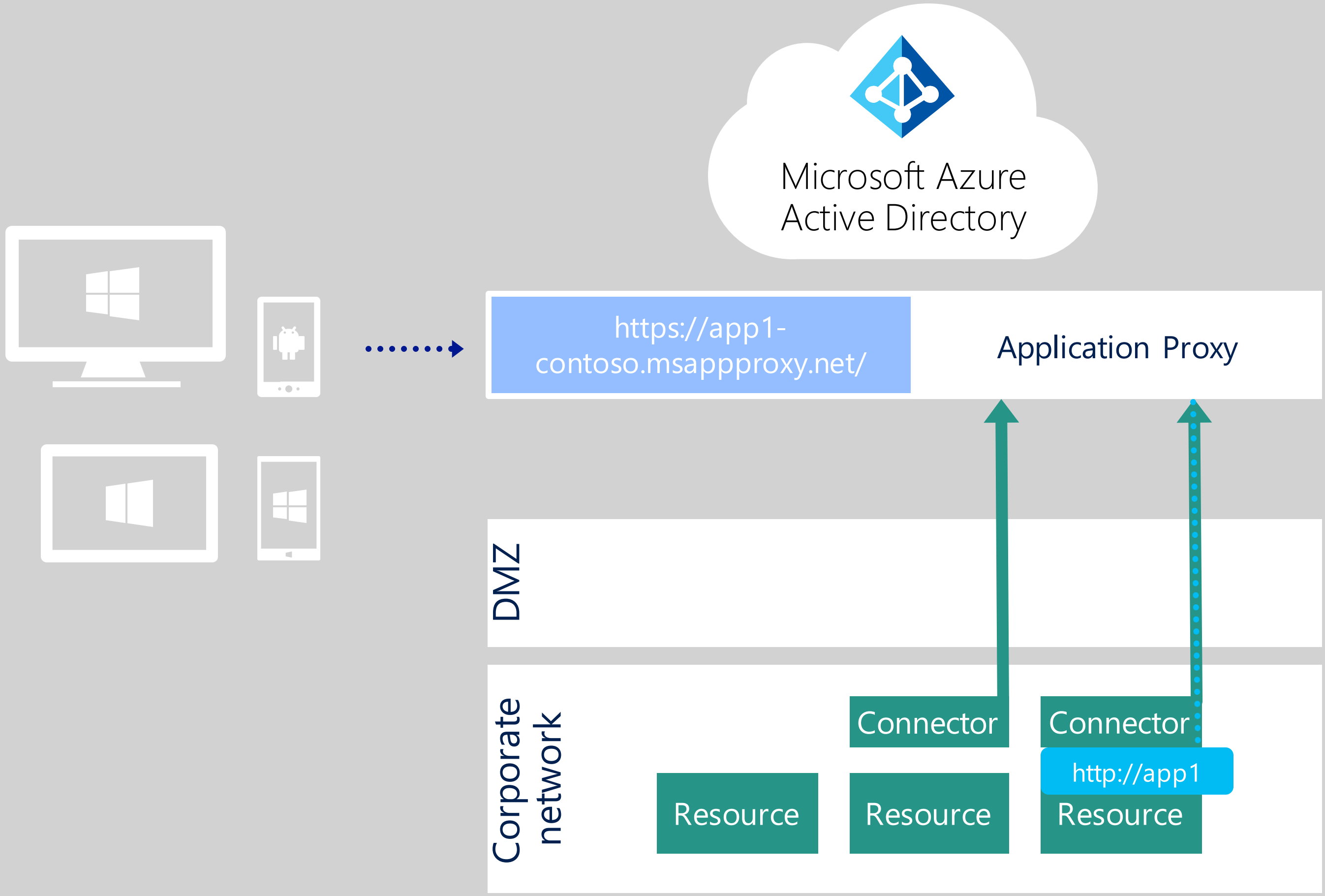
Access lifecycle
provides seamless and efficient access

Privileged access lifecycle
addresses risks inherent in administration

Assicurati che gli utenti giusti abbiano il diritto di accedere alle risorse giuste

Azure Active Directory Application Proxy

Abilita l'accesso sicuro alle applicazioni locali senza VPN



- Abilita sistemi di autenticazione moderni su applicazioni Legacy
- Abilita il SSO in diversi scenari di autenticazione
- Si connette automaticamente al servizio cloud
- Gestibile in logica di alta affidabilità e secondo la scalabilità necessaria
- Non richiede aperture sui firewall
- Gli utenti si connettono al servizio cloud che indirizza il traffico alle risorse tramite i connettori

Azure Active Directory

— Gestione completa dell'identità e degli accessi per dipendenti, partner e clienti —

B2B collaboration	Provisioning-Deprovisioning	Addition of custom cloud apps	Access Panel/MyApps	Dynamic Groups	Identity Protection
Self-Service capabilities	Connect Health	Remote Access to on-premises apps	Azure AD B2C	Group-Based Licensing	Privileged Identity Management
Azure AD Connect	Conditional Access	Microsoft Authenticator - Password-less Access	Azure AD Join	MDM-auto enrollment / Enterprise State Roaming	Security Reporting
SSO to SaaS	Multi-Factor Authentication	Azure AD DS	Office 365 App Launcher	HR App Integration	Access Reviews

Enterprise Mobility + Security

Proteggi i tuoi dati ovunque

58%

dei lavoratori hanno accidentalmente condiviso dati sensibili con persona sbagliata

Stroz Friedberg

Azure Information Protection

Data and e-mail protection on-premises and in the cloud

Classification and labeling

Classify data based on sensitivity and add labels—manually or automatically.

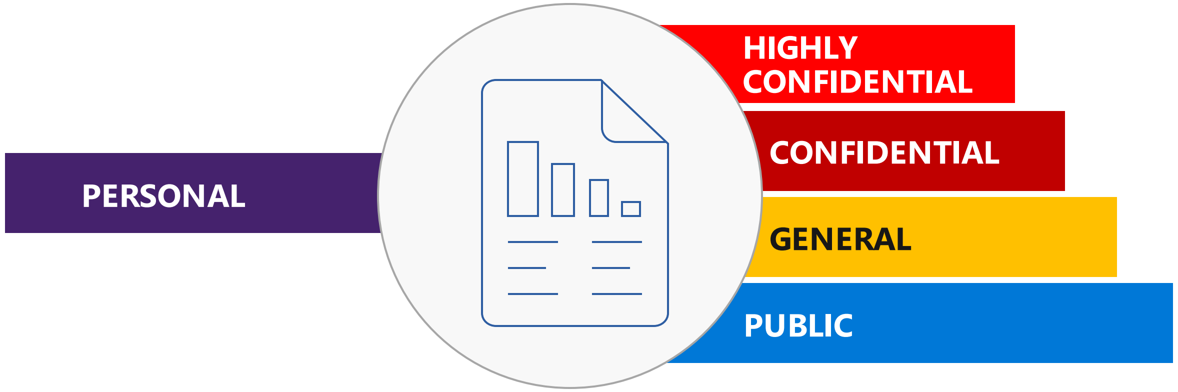
Protection

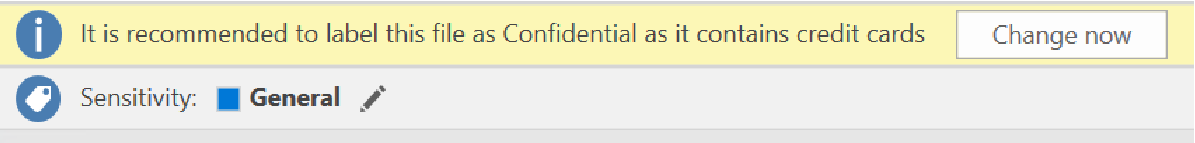
Encrypt your sensitive data and define usage rights or add visual markings when needed.

Monitoring

Use detailed tracking and reporting to see what's happening with your shared data and maintain control over it.

Classification and labeling




It is recommended to label this file as Confidential as it contains credit cards

Sensitivity: 🟦 **General**

Automatic classification

Policies can be set by IT Admins for automatically applying classification and protection to data.

Recommended classification

Based on the content you're working on, you can be prompted with suggested classification.

Manual reclassification

You can override a classification and optionally be required to provide a justification.

User-specified classification

Users can choose to apply a sensitivity label to the email or file they are working on with a single click.

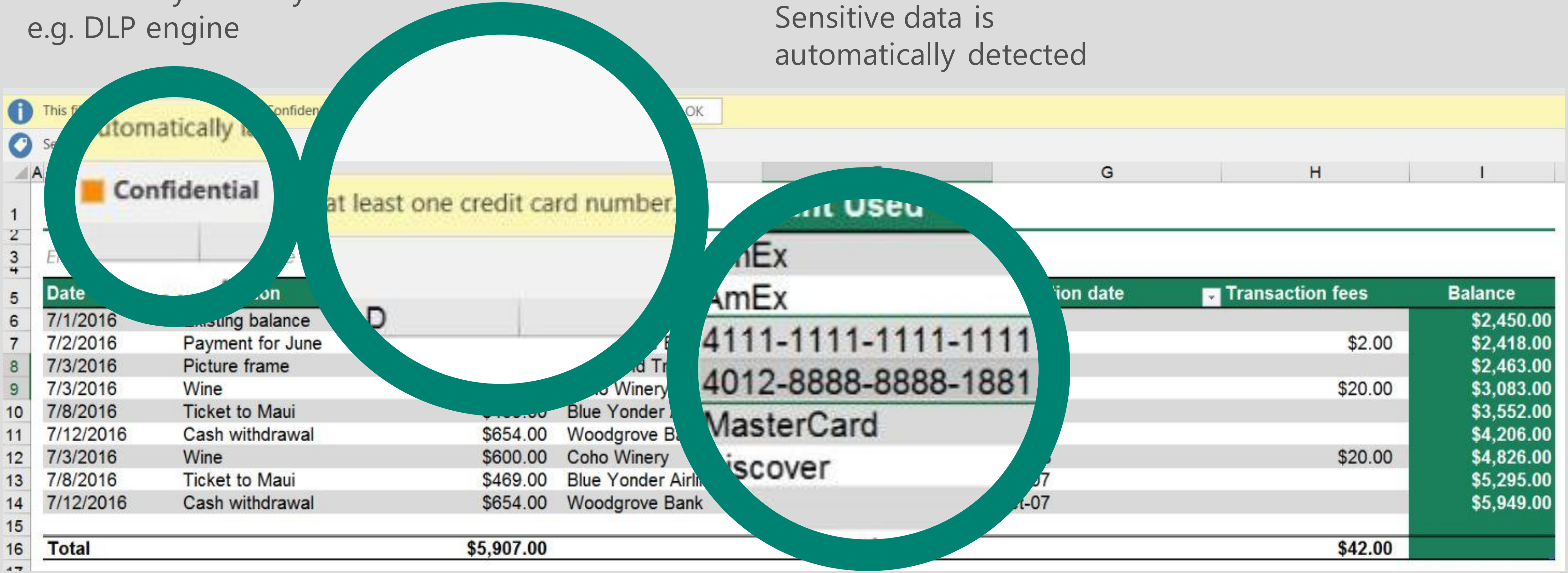
Classification and labeling

Discover personal data and apply persistent labels

Labels are persistent and readable by other systems e.g. DLP engine

Labels are metadata written to data

Sensitive data is automatically detected



This f... Confiden... OK

utomatically la...

Confidential

at least one credit card number.

nt Used

	Date	on			ion date	Transaction fees	Balance
6	7/1/2016	isting balance					$2,450.00
7	7/2/2016	Payment for June				$2.00	$2,418.00
8	7/3/2016	Picture frame		d Tr			$2,463.00
9	7/3/2016	Wine		o Winery		$20.00	$3,083.00
10	7/8/2016	Ticket to Maui		Blue Yonder			$3,552.00
11	7/12/2016	Cash withdrawal	$654.00	Woodgrove B			$4,206.00
12	7/3/2016	Wine	$600.00	Coho Winery		$20.00	$4,826.00
13	7/8/2016	Ticket to Maui	$469.00	Blue Yonder Airli	07		$5,295.00
14	7/12/2016	Cash withdrawal	$654.00	Woodgrove Bank	t-07		$5,949.00
15							
16	Total		$5,907.00			$42.00	

nEx

AmEx

4111-1111-1111-1111

4012-8888-8888-1881

MasterCard

iscover

Monitoring

Distribution visibility

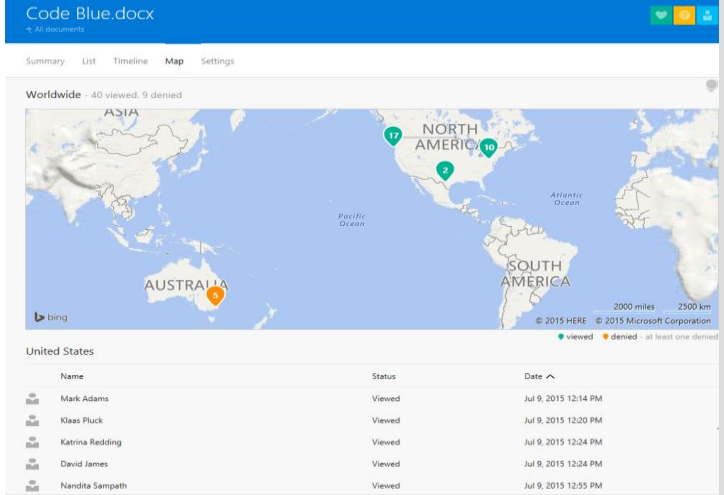
Analyze the flow of personal and sensitive data and detect risky behaviors.

Access logging

Track who is accessing documents and from where.

Access revocation

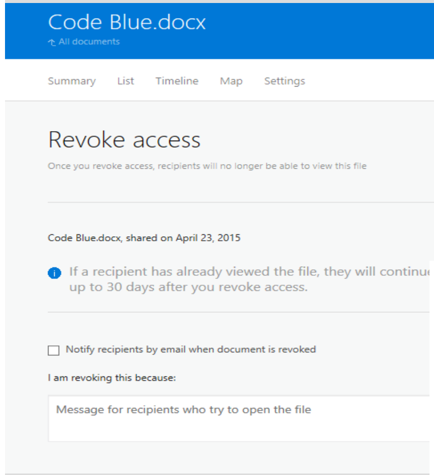
Prevent data leakage or misuse by changing or revoking document access remotely.



Worldwide - 40 viewed, 9 denied

United States

Name	Status	Date
Mark Adams	Viewed	Jul 9, 2015 12:14 PM
Klaas Pluck	Viewed	Jul 9, 2015 12:20 PM
Katrina Redding	Viewed	Jul 9, 2015 12:24 PM
David James	Viewed	Jul 9, 2015 12:24 PM
Nandita Sampath	Viewed	Jul 9, 2015 12:55 PM



Revoke access

Once you revoke access, recipients will no longer be able to view this file

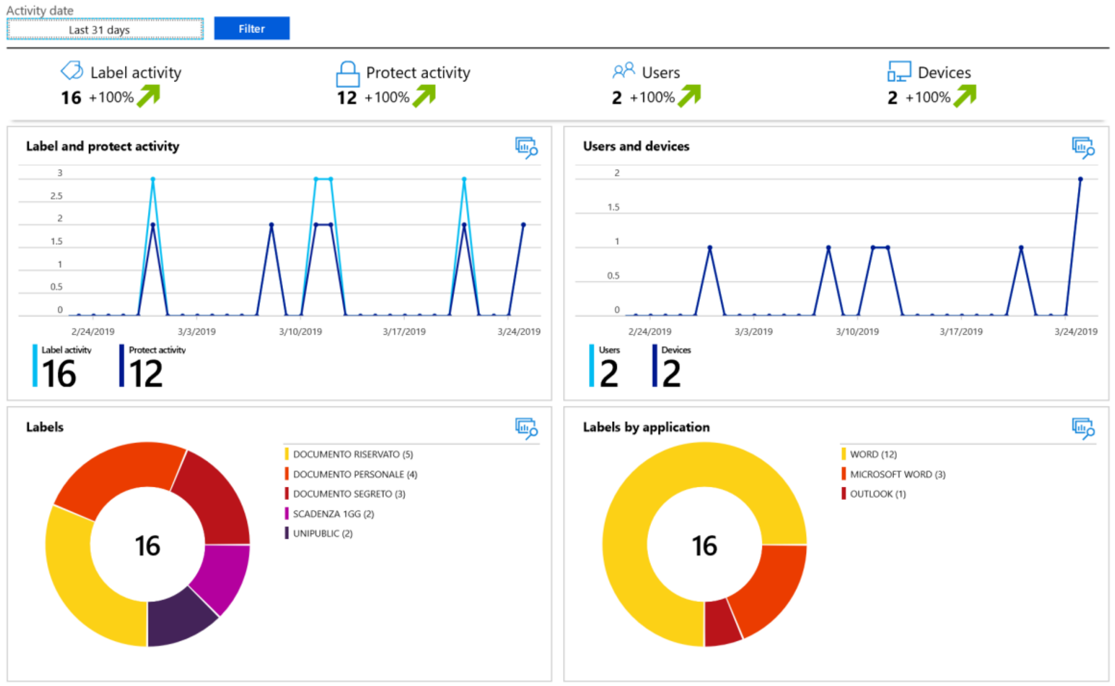
Code Blue.docx, shared on April 23, 2015

If a recipient has already viewed the file, they will continue up to 30 days after you revoke access.

□ Notify recipients by email when document is revoked

I am revoking this because:

Message for recipients who try to open the file



Activity date: Last 31 days

Label activity 16 +100%

Protect activity 12 +100%

Users 2 +100%

Devices 2 +100%

Label activity 16

Protect activity 12

Users 2

Devices 2

Labels:

- DOCUMENTO RISERVATO (5)
- DOCUMENTO PERSONALE (4)
- DOCUMENTO SEGRETO (3)
- SCADENZA 1GG (2)
- UNIPUBLIC (2)

Labels by application:

- WORD (12)
- MICROSOFT WORD (3)
- OUTLOOK (1)

Stay in control with MCAS
Microsoft Cloud App Security

Cloud App Security

Deep visibility and granular controls into cloud app usage

Cloud discovery

Discover cloud apps used in your organization, get a risk assessment and alerts on risky usage.

Data visibility

Gain deep visibility into where data travels by investigating all activities, files and accounts for managed apps.

Data control

Monitor and protect personal and sensitive data stored in cloud apps using granular policies.

Cloud discovery

Discovery of cloud apps and data

Discover 13K+ cloud apps in use across your networks and sensitive data they store.

Cloud app risk assessment

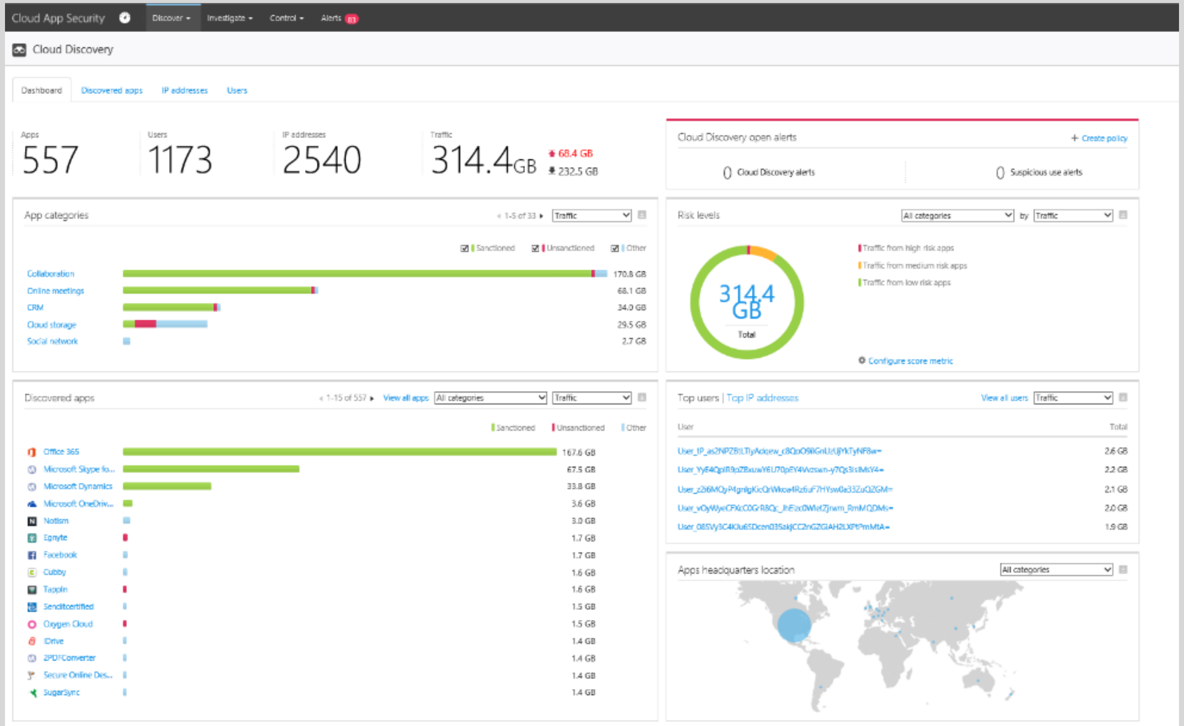
Assess risk cloud apps based on ~60 security and compliance risk factors.

On-going analytics

Get anomalous usage alerts, new app and trending apps alerts.

Log anonymization

Protect your employees' privacy while discovering cloud apps in your environment.



Apps	Users	IP addresses	Traffic
557	1173	2540	314.4GB (68.4 GB up, 232.5 GB down)

Cloud Discovery open alerts: 0 Cloud Discovery alerts; 0 Suspicious use alerts

App categories (1-5 of 33) — ☑ Sanctioned ☑ Unsanctioned ☑ Other

Collaboration	170.8 GB
Online meetings	68.1 GB
CRM	34.0 GB
Cloud storage	29.5 GB
Social network	2.7 GB

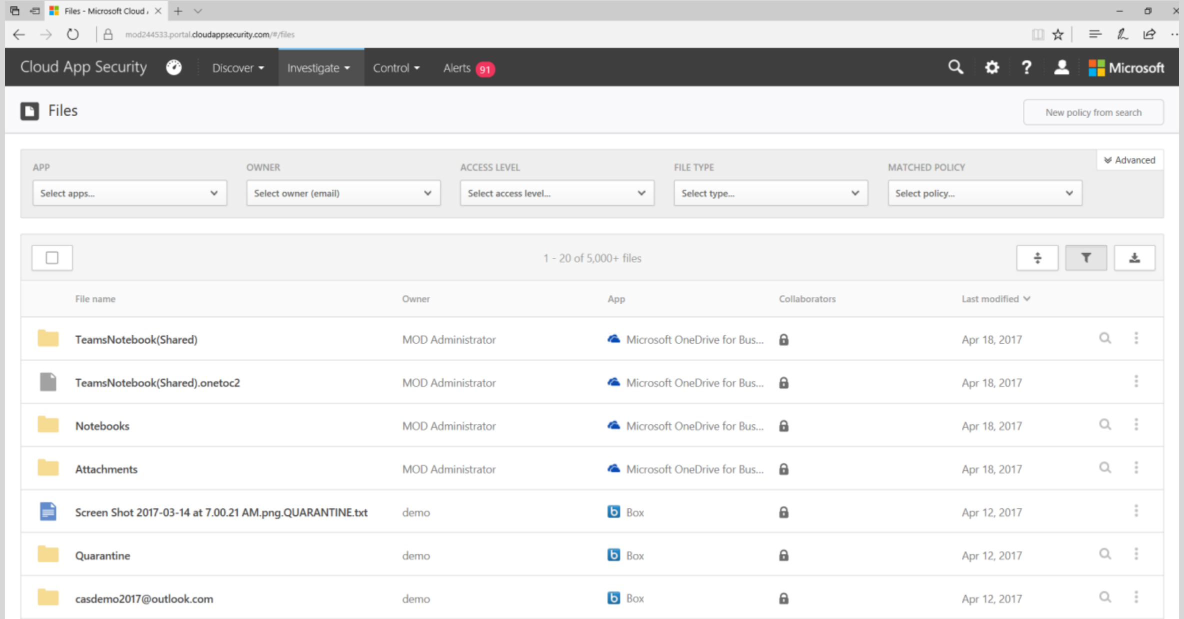
Risk levels: 314.4 GB Total — Traffic from high risk apps; Traffic from medium risk apps; Traffic from low risk apps

Discovered apps (1-15 of 557) — Sanctioned, Unsanctioned, Other

Office 365	167.6 GB
Microsoft Skype fo...	67.5 GB
Microsoft Dynamics	33.8 GB
Microsoft OneDriv...	3.6 GB
Notism	3.0 GB
Egnyte	1.7 GB
Facebook	1.7 GB
Cubby	1.6 GB
TappIn	1.6 GB
Senditcertified	1.5 GB
Oxygen Cloud	1.5 GB
IDrive	1.4 GB
2PDFConverter	1.4 GB
Secure Online Des...	1.4 GB
SugarSync	1.4 GB

Top users

User	Total
User_IP_as2NPZB1LTlyAclqew_c8QoO9iiGnUzUjYkTyNF8w=	2.6 GB
User_YyE4QpIR9pZBauwY6U70pEY4Wzswn-y7Qs3IsIMsY4=	2.2 GB
User_z2i6MQyP4gnlgKicQrWkoa4Rz6uF7HYsw0e33ZuQZGM=	2.1 GB
User_vOyWyeCFXcC0GrR8Qc_lhEizd0WletZjnwm_RmMQDMs=	2.0 GB
User_08SVy3C4KIu65Dcen035akjCC2nGZGIAH2LXPtPmMtA=	1.9 GB



Files

APP: Select apps... | OWNER: Select owner (email) | ACCESS LEVEL: Select access level... | FILE TYPE: Select type... | MATCHED POLICY: Select policy...

1 - 20 of 5,000+ files

File name	Owner	App	Collaborators	Last modified
TeamsNotebook(Shared)	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
TeamsNotebook(Shared).onetoc2	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
Notebooks	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
Attachments	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
Screen Shot 2017-03-14 at 7.00.21 AM.png.QUARANTINE.txt	demo	Box	🔒	Apr 12, 2017
Quarantine	demo	Box	🔒	Apr 12, 2017
casdemo2017@outlook.com	demo	Box	🔒	Apr 12, 2017

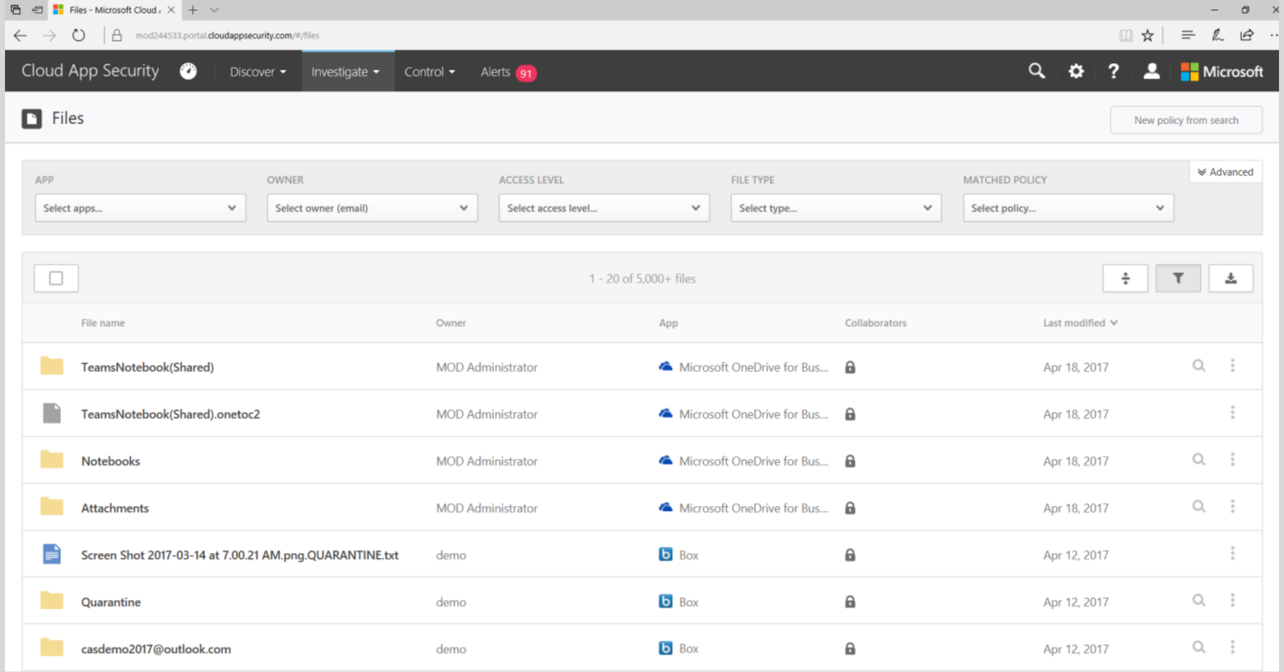
Data visibility

Advanced incident investigation tools

Investigate on users, file, activities, locations and managed apps, quantify exposure and risk.

Cloud data visibility

Compare classification labels against how that data is being shared to identify risk.



Files

APP: Select apps...

OWNER: Select owner (email)

ACCESS LEVEL: Select access level...

FILE TYPE: Select type...

MATCHED POLICY: Select policy...

1 - 20 of 5,000+ files

File name	Owner	App	Collaborators	Last modified
TeamsNotebook(Shared)	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
TeamsNotebook(Shared).onetoc2	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
Notebooks	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
Attachments	MOD Administrator	Microsoft OneDrive for Bus...	🔒	Apr 18, 2017
Screen Shot 2017-03-14 at 7.00.21 AM.png.QUARANTINE.txt	demo	Box	🔒	Apr 12, 2017
Quarantine	demo	Box	🔒	Apr 12, 2017
casdemo2017@outlook.com	demo	Box	🔒	Apr 12, 2017

Data control

Granular Data loss prevention (DLP) policies

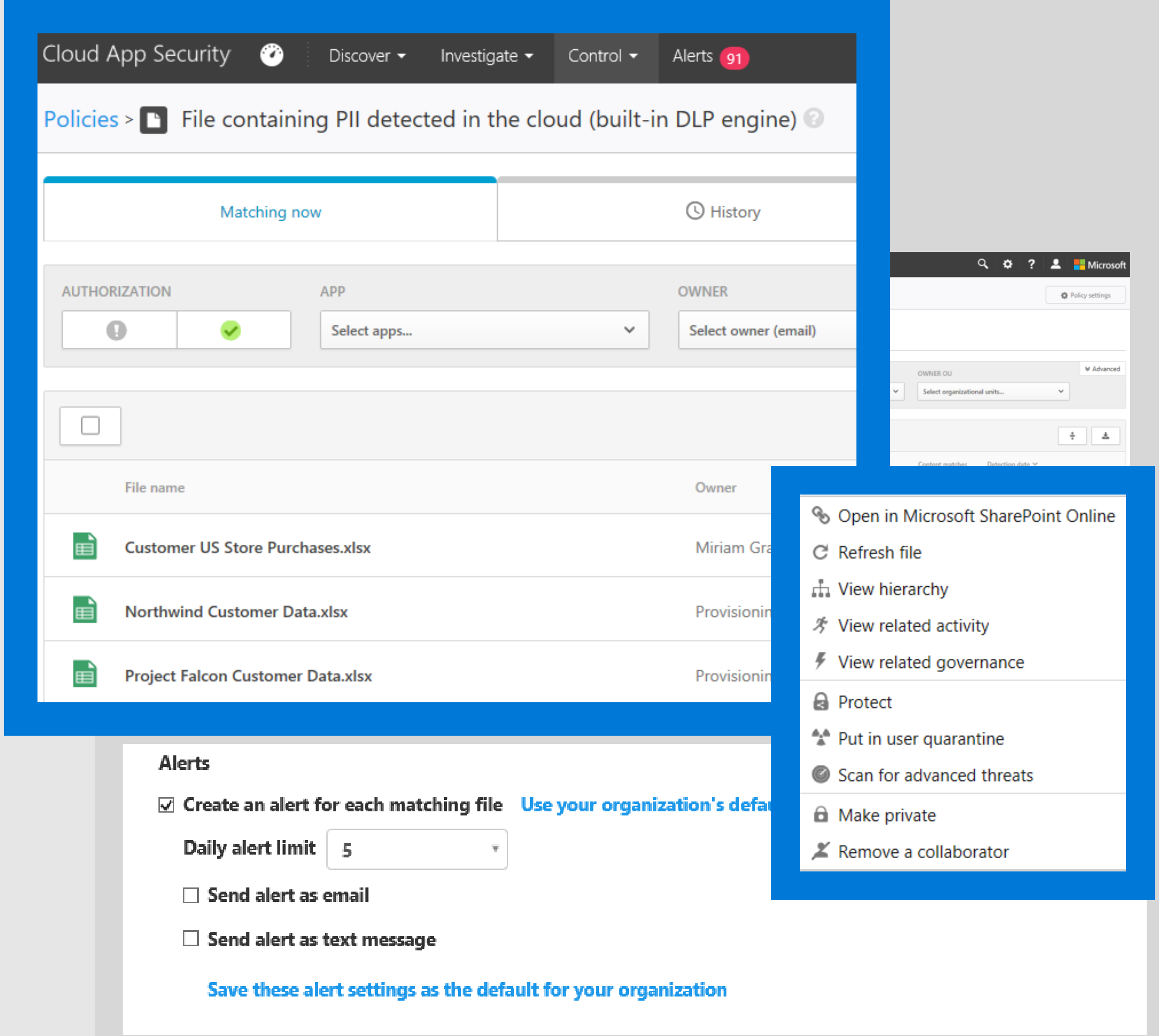
Set granular policies to control data in the cloud—either automated or based on file label—using out-of-the-box policies or you can customize your own.

Policy enforcement

Identify policy violations, enforce actions such as quarantine and permissions removal.

Revoke access for 3rd party apps

Detect and manage 3rd party app access.



Policies > File containing PII detected in the cloud (built-in DLP engine)

Select apps...

Select owner (email)

Select organizational units...

File name	Owner
Customer US Store Purchases.xlsx	Miriam Gra
Northwind Customer Data.xlsx	Provisionin
Project Falcon Customer Data.xlsx	Provisionin

Alerts

☑ Create an alert for each matching file Use your organization's defau

Daily alert limit 5

□ Send alert as email

□ Send alert as text message

Save these alert settings as the default for your organization

Threat detection

Insight into potential breaches

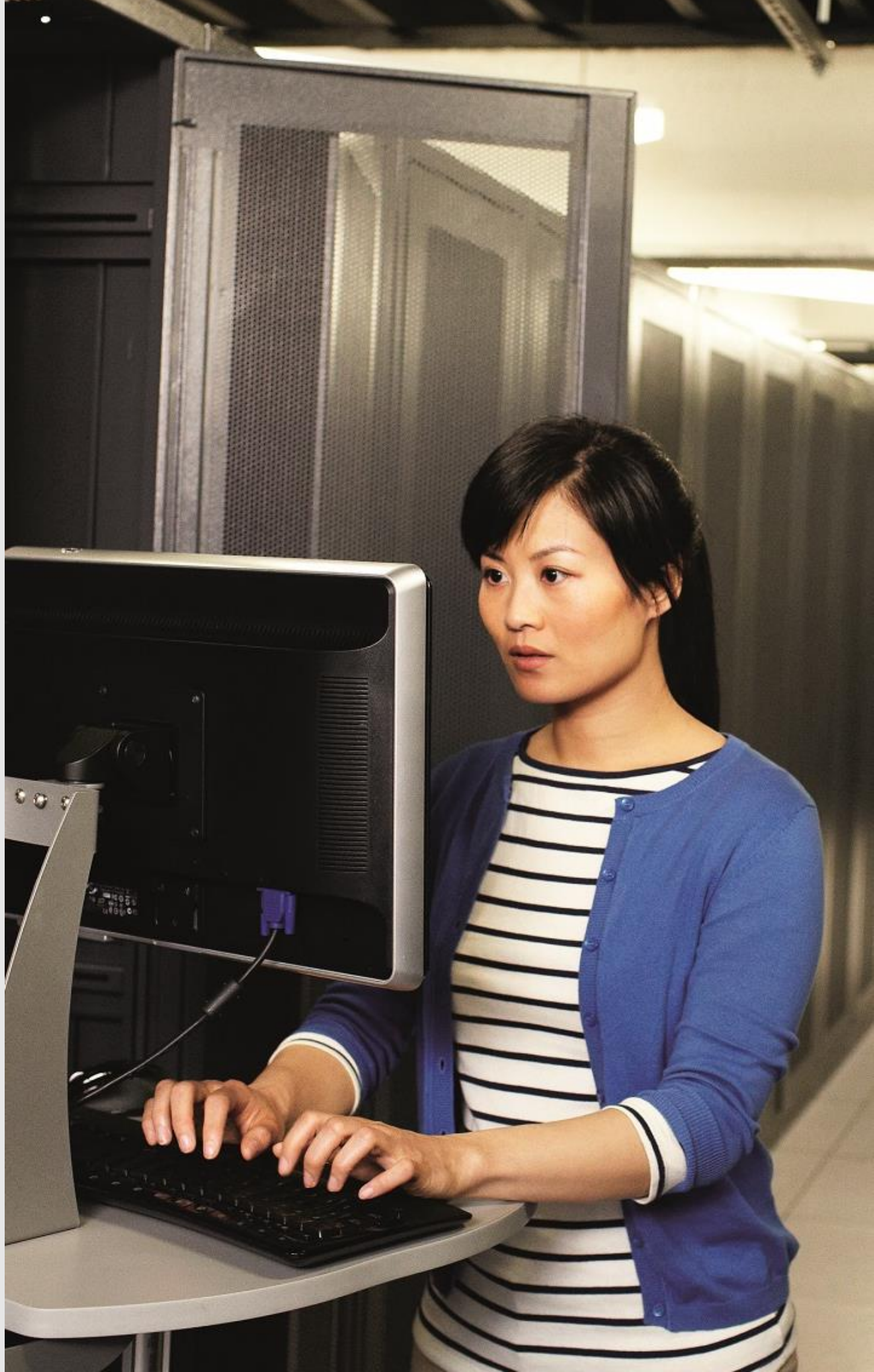
Identify anomalies in your Office 365 environment which may be indicative of a breach.

Assess your risk

Leverage behavioral analytics to assess risk.

Leverage Microsoft's threat intelligence

Identify known attack pattern activities originating from risky sources leveraging Microsoft's threat intelligence.



Threat detection

Anomaly alert

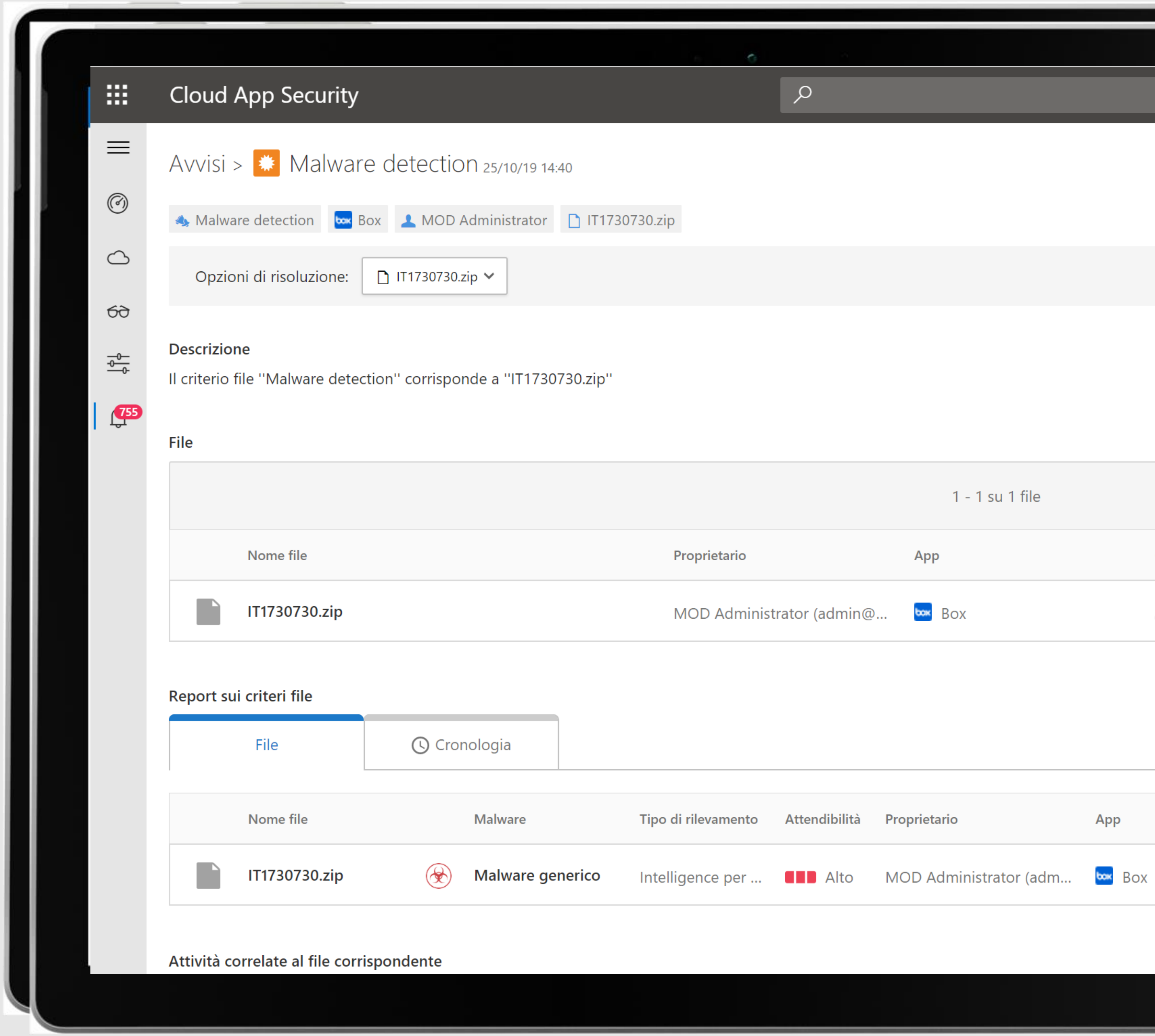
UEBA capabilities cross platform and application

Sandbox

0 day attack protection

WDATP Integration

Every endpoint collaborate to enhance security



Avvisi > Malware detection 25/10/19 14:40

Malware detection | Box | MOD Administrator | IT1730730.zip

Opzioni di risoluzione: IT1730730.zip

Descrizione

Il criterio file "Malware detection" corrisponde a "IT1730730.zip"

File

1 - 1 su 1 file

Nome file	Proprietario	App
IT1730730.zip	MOD Administrator (admin@...	Box

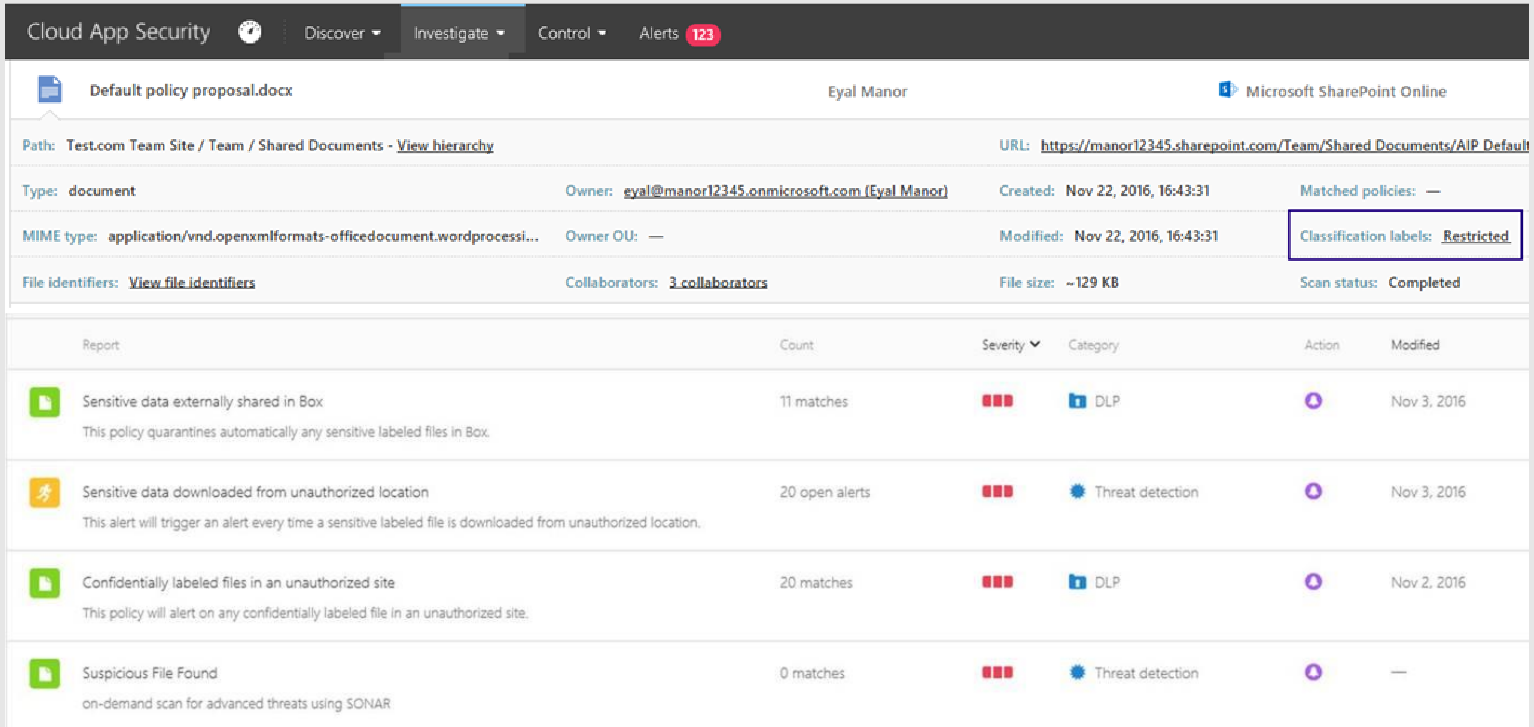
Report sui criteri file

File | Cronologia

Nome file	Malware	Tipo di rilevamento	Attendibilità	Proprietario	App
IT1730730.zip	Malware generico	Intelligence per ...	Alto	MOD Administrator (adm...	Box

Attività correlate al file corrispondente

Cloud App Security and Azure Information Protection integration



Default policy proposal.docx | Eyal Manor | Microsoft SharePoint Online

Path: Test.com Team Site / Team / Shared Documents - View hierarchy

URL: https://manor12345.sharepoint.com/Team/Shared Documents/AIP Default

Type: document

Owner: eyal@manor12345.onmicrosoft.com (Eyal Manor)

Created: Nov 22, 2016, 16:43:31

Matched policies: —

MIME type: application/vnd.openxmlformats-officedocument.wordprocessi...

Owner OU: —

Modified: Nov 22, 2016, 16:43:31

Classification labels: Restricted

File identifiers: View file identifiers

Collaborators: 3 collaborators

File size: ~129 KB

Scan status: Completed

Report	Count	Severity	Category	Action	Modified
Sensitive data externally shared in Box This policy quarantines automatically any sensitive labeled files in Box.	11 matches	■■■	DLP	○	Nov 3, 2016
Sensitive data downloaded from unauthorized location This alert will trigger an alert every time a sensitive labeled file is downloaded from unauthorized location.	20 open alerts	■■■	Threat detection	○	Nov 3, 2016
Confidentially labeled files in an unauthorized site This policy will alert on any confidentially labeled file in an unauthorized site.	20 matches	■■■	DLP	○	Nov 2, 2016
Suspicious File Found on-demand scan for advanced threats using SONAR	0 matches	■■■	Threat detection	○	—

Increased visibility

Cloud App Security reads labels set by AIP to give admins visibility into sharing of sensitive files.

Improved control

Admins can set policies for controlling sharing of sensitive files and also get alerted if the policies are violated.

IaaS, PaaS and SaaS security posture

Insight into potential breaches

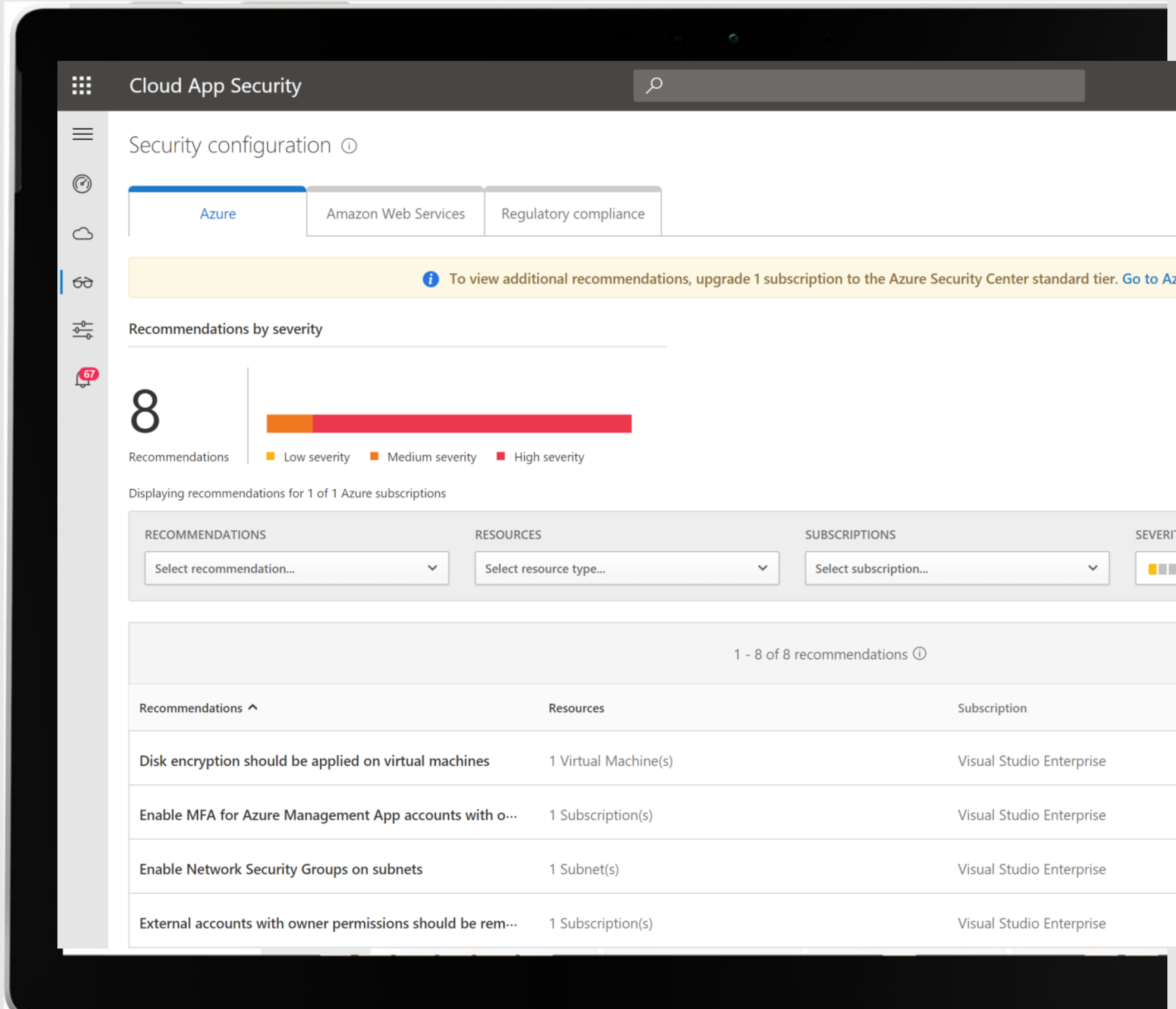
Identify anomalies in your Office 365 environment which may be indicative of a breach.

Assess your risk

Leverage behavioral analytics to assess risk.

Leverage Microsoft’s threat intelligence

Identify known attack pattern activities originating from risky sources leveraging Microsoft’s threat intelligence.



Security configuration ⓘ

ⓘ To view additional recommendations, upgrade 1 subscription to the Azure Security Center standard tier. Go to Az

Recommendations by severity

8
Recommendations

🟨 Low severity 🟧 Medium severity 🟥 High severity

Displaying recommendations for 1 of 1 Azure subscriptions

RECOMMENDATIONS | RESOURCES | SUBSCRIPTIONS | SEVERI

1 - 8 of 8 recommendations ⓘ

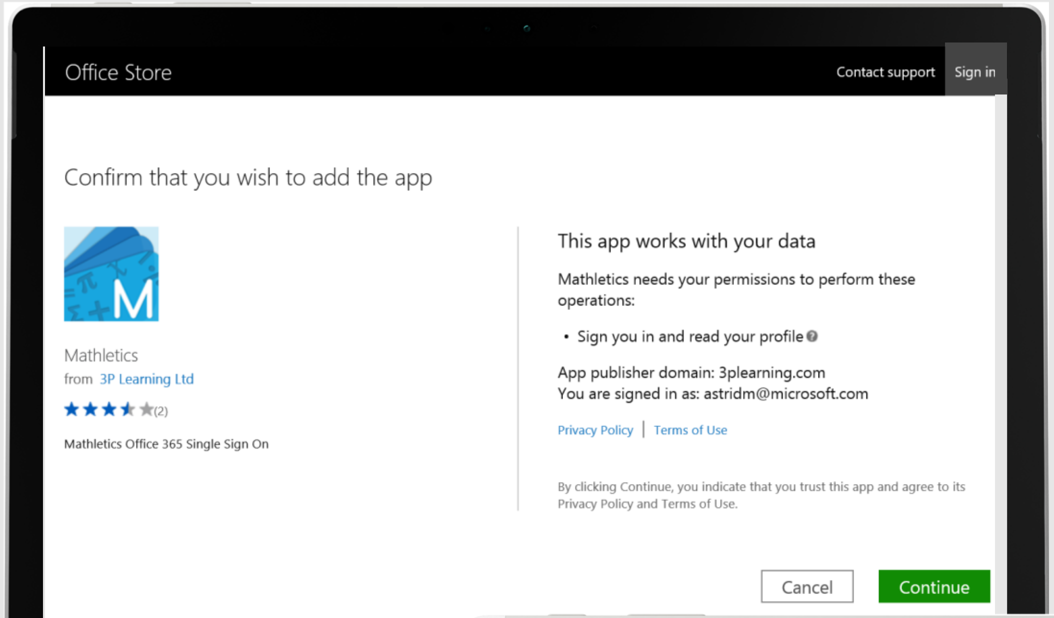
Recommendations ^	Resources	Subscription
Disk encryption should be applied on virtual machines	1 Virtual Machine(s)	Visual Studio Enterprise
Enable MFA for Azure Management App accounts with o...	1 Subscription(s)	Visual Studio Enterprise
Enable Network Security Groups on subnets	1 Subnet(s)	Visual Studio Enterprise
External accounts with owner permissions should be rem...	1 Subscription(s)	Visual Studio Enterprise

App permissions

Users grant apps permission to SaaS platform.

IT has limited visibility.

Revoke app permissions across organization.



Confirm that you wish to add the app

Mathletics
from 3P Learning Ltd
★★★★☆(2)

Mathletics Office 365 Single Sign On

This app works with your data

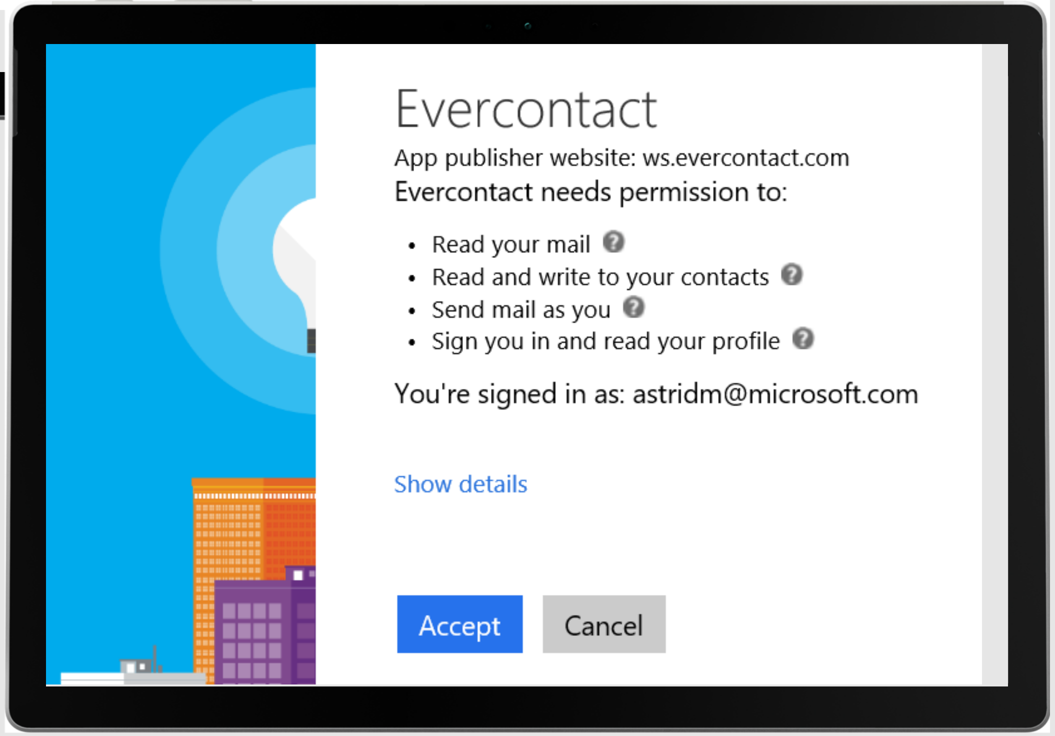
Mathletics needs your permissions to perform these operations:

- Sign you in and read your profile

App publisher domain: 3plearning.com
You are signed in as: astridm@microsoft.com

Privacy Policy | Terms of Use

By clicking Continue, you indicate that you trust this app and agree to its Privacy Policy and Terms of Use.



Evercontact

App publisher website: ws.evercontact.com
Evercontact needs permission to:

- Read your mail
- Read and write to your contacts
- Send mail as you
- Sign you in and read your profile

You're signed in as: astridm@microsoft.com

Protecting an endpoint ~~is~~ was hard.

Malware

Phishing

Ransomware

0-day

World-wide outbreaks

Advanced attacks

Supply chain

Fileless attacks

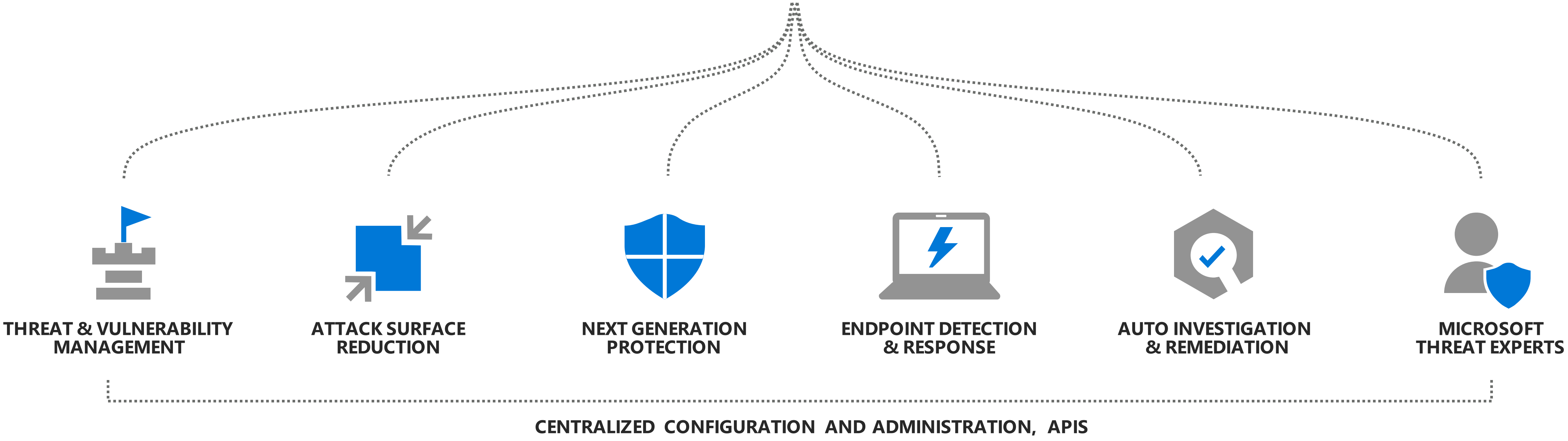
Vulnerabilities

Microsoft Defender ATP

Built-in. Cloud-powered.

Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

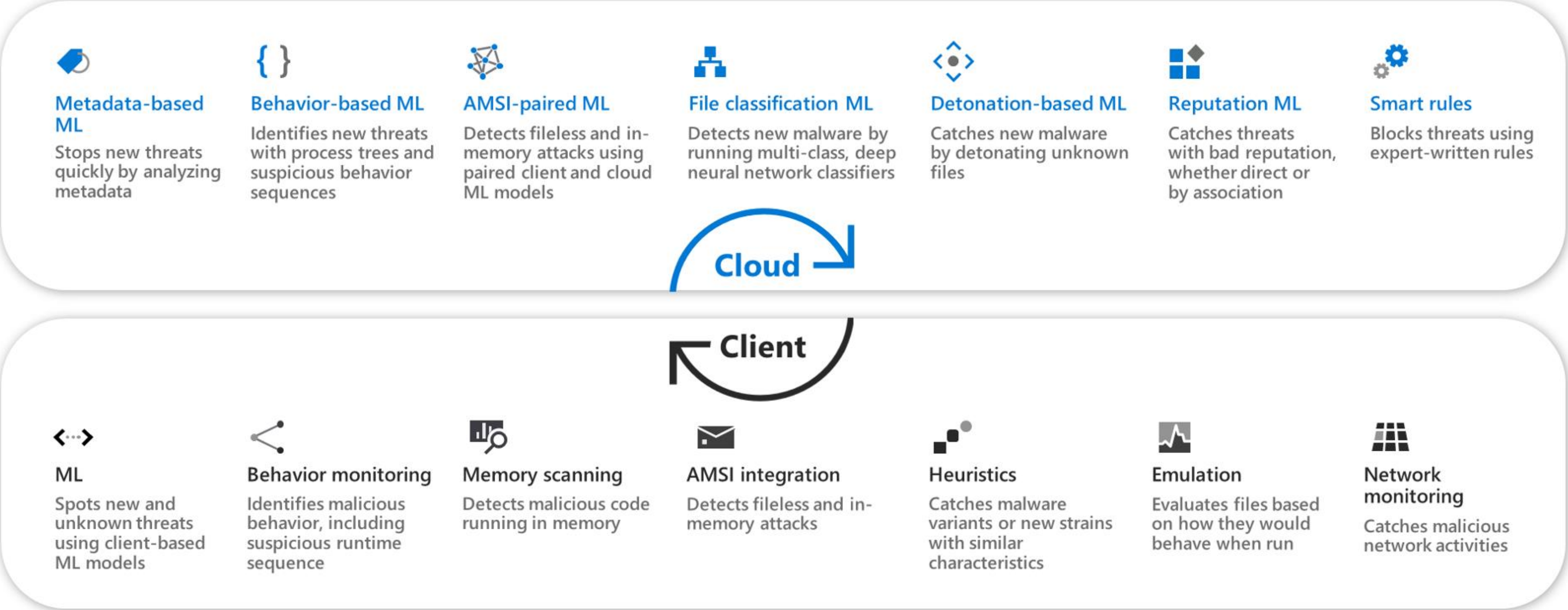
ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIS

Microsoft Defender ATP next generation protection engines



Metadata-based ML
Stops new threats quickly by analyzing metadata

Behavior-based ML
Identifies new threats with process trees and suspicious behavior sequences

AMSI-paired ML
Detects fileless and in-memory attacks using paired client and cloud ML models

File classification ML
Detects new malware by running multi-class, deep neural network classifiers

Detonation-based ML
Catches new malware by detonating unknown files

Reputation ML
Catches threats with bad reputation, whether direct or by association

Smart rules
Blocks threats using expert-written rules

ML
Spots new and unknown threats using client-based ML models

Behavior monitoring
Identifies malicious behavior, including suspicious runtime sequence

Memory scanning
Detects malicious code running in memory

AMSI integration
Detects fileless and in-memory attacks

Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

Network monitoring
Catches malicious network activities

Microsoft is a strong security Company

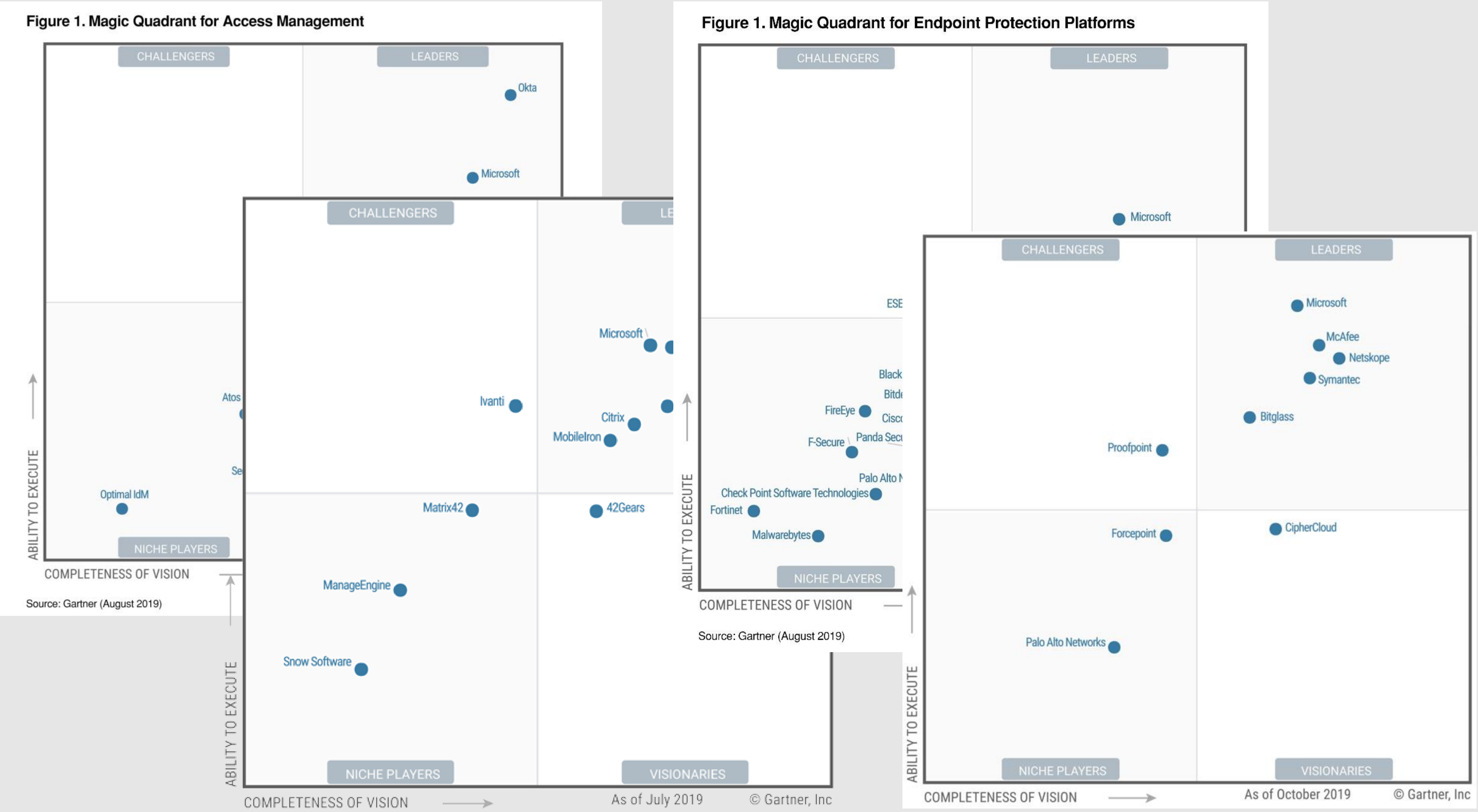


Figure 1. Magic Quadrant for Access Management

Source: Gartner (August 2019)

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

As of July 2019 © Gartner, Inc

As of October 2019 © Gartner, Inc

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

Microsoft