- MSFT Elite Partner
- MSFT Security Partner Advisory Council

  (1 of 10 in USA)
- MSFT Priority Managed Partner

  (1 of 25 in USA)
- MSFT FastTrack Ready Partner
- MSFT Account Guard (US 2020 Elections)
- MSFT Cloud Services Provider (CSP)
- 600+ Completed Projects since 2015

PATRIOT
CONSULTING

Microsoft
Partner
Microsoft

Gold Cloud Productivity
Gold Enterprise Mobility Management
Gold Datacenter
Silver Cloud Platform
Silver Collaboration and Content

About Joe

CEO and Principal Architect

Principal Systems Architect with 17 Years of experience

Technical certifications: MCSE, MCITP Office 365, CISSP

B.S. Biola University.

Microsoft "Virtual Technology Sales Professional"

Twitter: @ITGuySoCal

Blog: www.TheCloudTechnologist.com

LinkedIN: https://www.linkedin.com/in/jstocker101

Company: www.PatriotConsultingTech.com

MVP

Microsoft®

Most Valuable Professional

PATRIOT

CONSULTING

Microsoft Security Overview

1. Prevent Unauthorized Access
2. Prevent Spear Phishing
3. Enable Single Sign On
4. Detect and Prevent Shadow IT
5. Detect & Prevent Data Breaches
6. Secure Employee Exits
7. Endpoint Detection & Response (EDR)
8. Office 365 Governance
9. Prevent Sensitive Data Leaks
10. Prevent Ransomware Attacks
11. Ignite 2020 Announcements

Security Issue #1

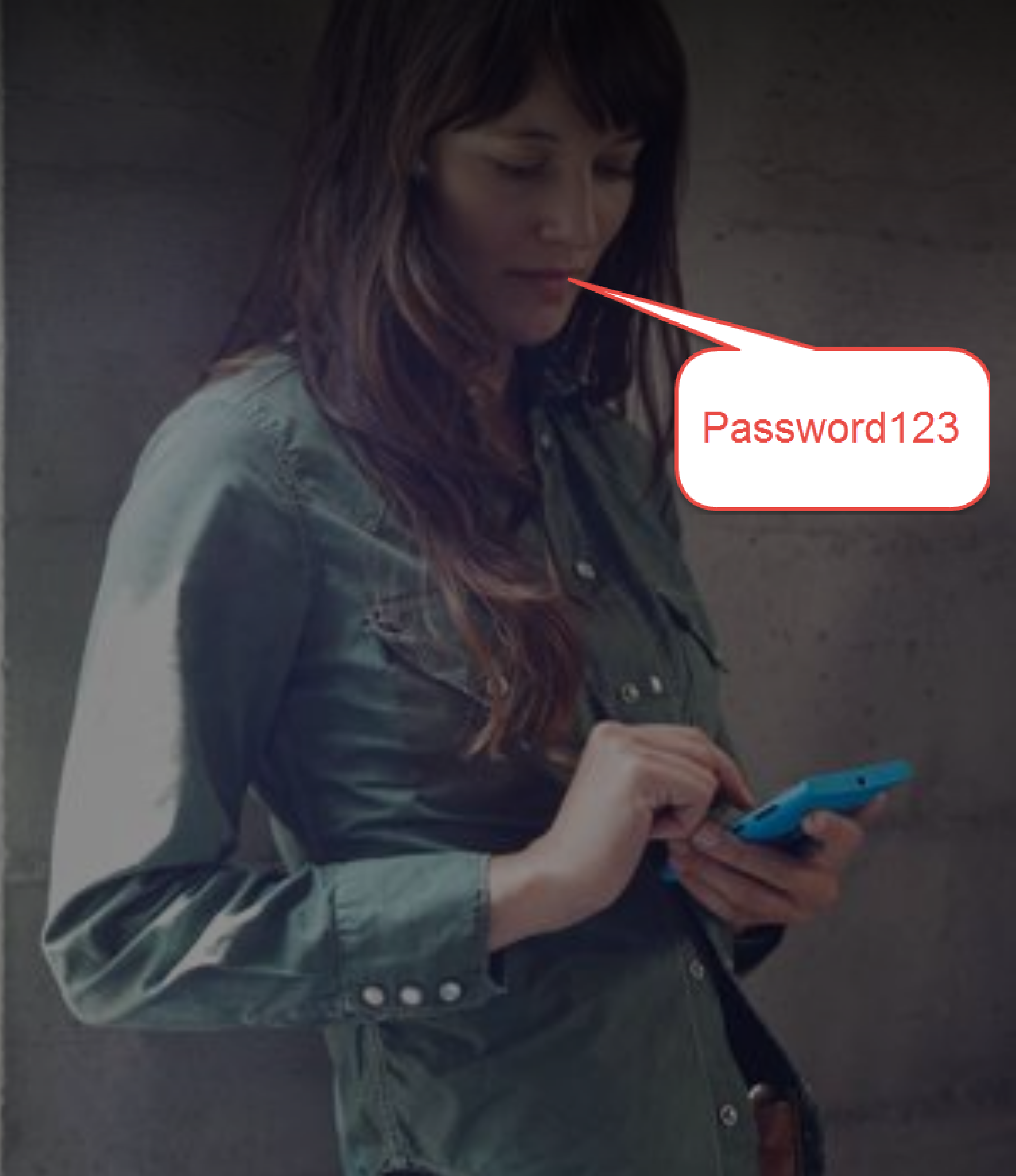
90%

of Data breaches…

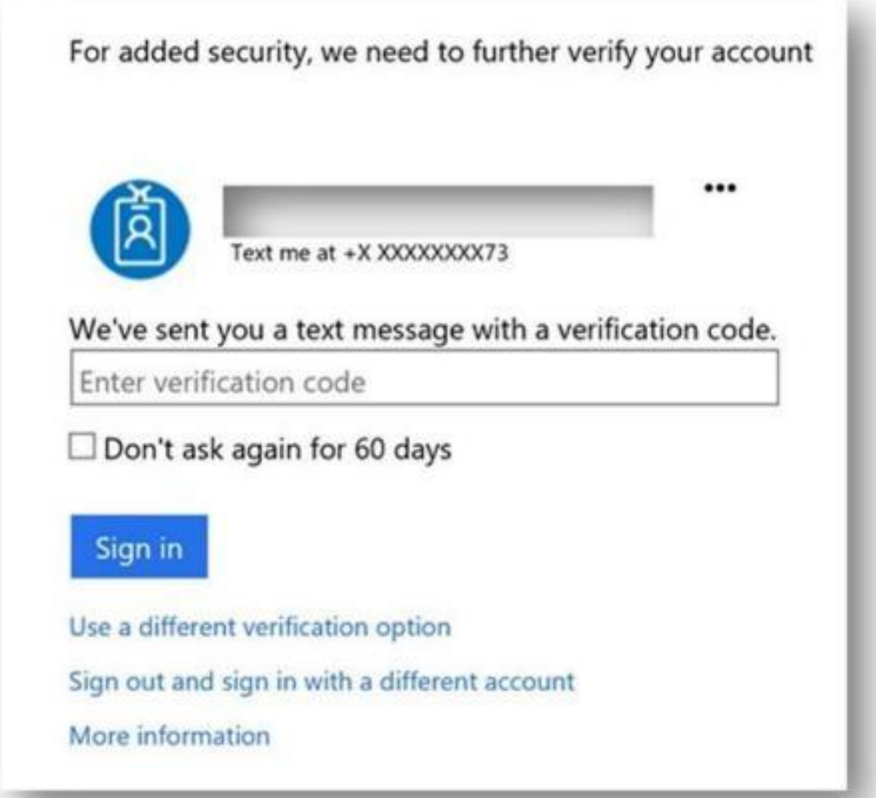
involve weak, default, or stolen passwords.

70% of employees use the same password for all logins

50% of employees will be tricked by clever phishing emails



Solution #1 SMS-based Multi-Factor Authentication (MFA)



For added security, we need to further verify your account

[redacted]

Text me at +X XXXXXXXX73

We've sent you a text message with a verification code.

•••
Enter verification code

□ Don't ask again for 60 days

Sign in
Use a different verification option
Sign out and sign in with a different account
More information

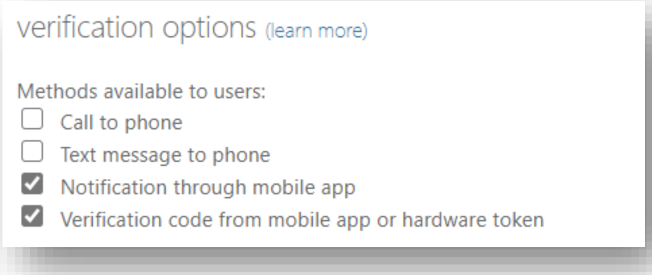
SMS MFA will prevent 99% of Account Takeovers
-Source: Microsoft

Nation-state APT Threat Actors are 24% successful against SMS Common Techniques: SIM-Card Swap, Phone # Porting, MITM, Social Engineering, and more…

Payment Card Industry (PCI): Does not recommend SMS for 2FA

NIST 800-63: SMS is prohibited for 2FA

SMS is enabled by default in Office 365
Patriot recommendation: Disable SMS MFA



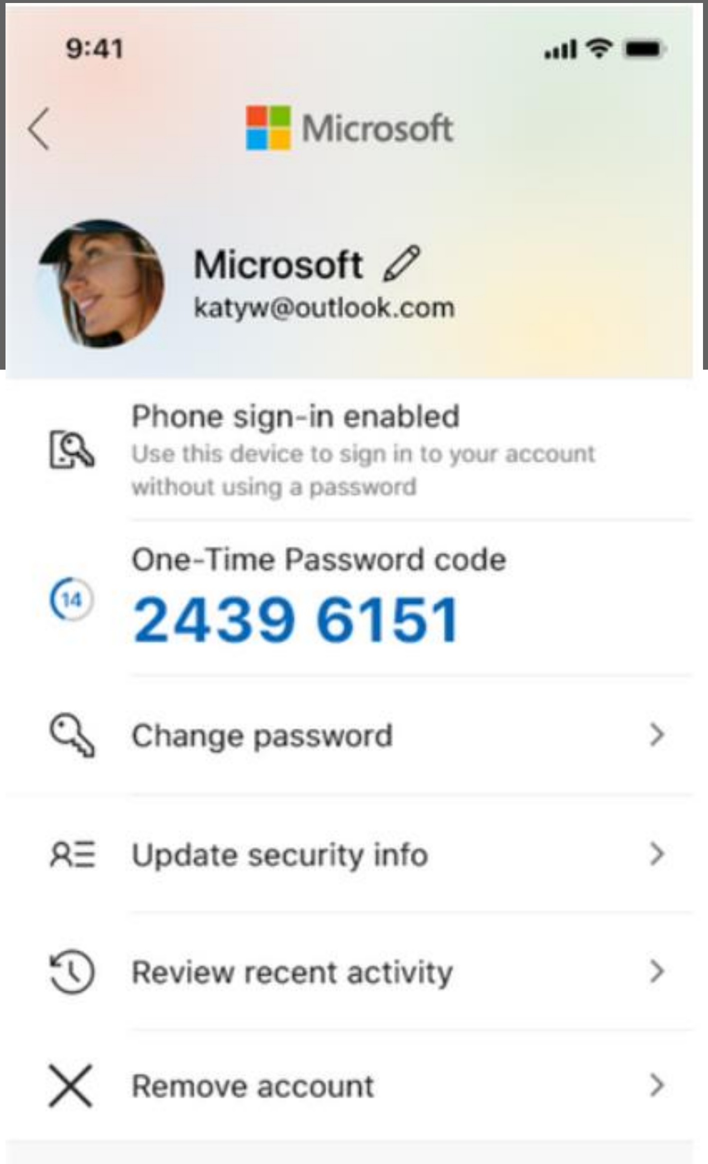
verification options (learn more)

Methods available to users:

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

https://account.activedirectory.windowsazure.com/usermanagement/mfasettings.aspx

Solution #2 Authenticator Apps for Multi-Factor Authentication



Microsoft
katyw@outlook.com

Phone sign-in enabled
Use this device to sign in to your account without using a password

One-Time Password code
2439 6151

Microsoft Authenticator App for iOS or Android

3rd party Authenticator Apps are supported

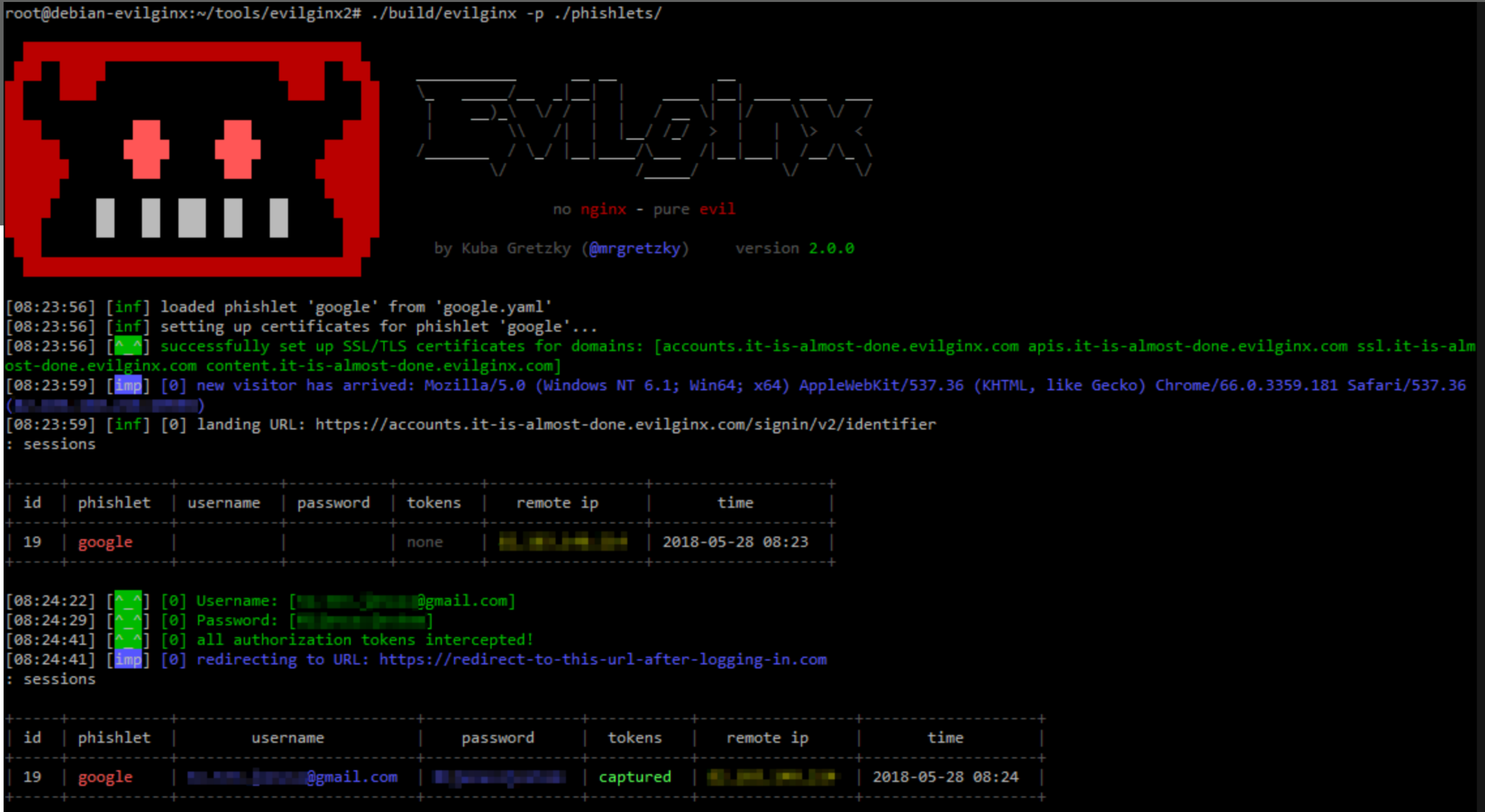
Advantages of MSFT: (1) **Password-less** (1) SSPR built into Mobile App

Benefits: (1) Immune to SIM Swap/Phone Port (2) Eliminate Mobile VPN

Weakness: Man-In-The-Middle Proxy Attacks

PATRIOT
CONSULTING

Threat: Man-In-The-Middle (MFA Bypass)



```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                    ___________      .__.__                 .__
                    \_   _____/__  _|__|  |    ____   ____ |__| ____ ___  ___
                     |    __)_\  \/ /  |  |   / ___\ /    \|  |/    \\  \/  /
                     |        \\   /|  |  |__/ /_/  >   |  \  |   |  \>    <
                    /_______  / \_/ |__|____/\___  /|___|  /__|___|  /__/\_ \
                            \/              /_____/      \/        \/      \/

                                  no nginx - pure evil

                          by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+----------+----------+----------+--------+--------------+------------------+
| id  | phishlet | username | password | tokens |  remote ip   |       time       |
+-----+----------+----------+----------+--------+--------------+------------------+
| 19  | google   |          |          | none   | [redacted]   | 2018-05-28 08:23 |
+-----+----------+----------+----------+--------+--------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+----------+----------------------+--------------+----------+--------------+------------------+
| id  | phishlet |       username       |   password   |  tokens  |  remote ip   |       time       |
+-----+----------+----------------------+--------------+----------+--------------+------------------+
| 19  | google   | [redacted]@gmail.com | [redacted]   | captured | [redacted]   | 2018-05-28 08:24 |
+-----+----------+----------------------+--------------+----------+--------------+------------------+
```

Solution #3 Hardware tokens (typically for BYOD)

Hardware or Software One-Time Passcodes (OATH) Tokens (Approx ~$20 each)

Benefits: Best fit for users who refuse to install apps on their personal phones

100% Cloud with No Server Infrastructure Required

Weakness: Man-In-The-Middle Proxy Attacks

Available from multiple manufacturers:

- DEEPNET (England), Token2 (Switzerland), Yubico (USA)

PATRIOT
CONSULTING

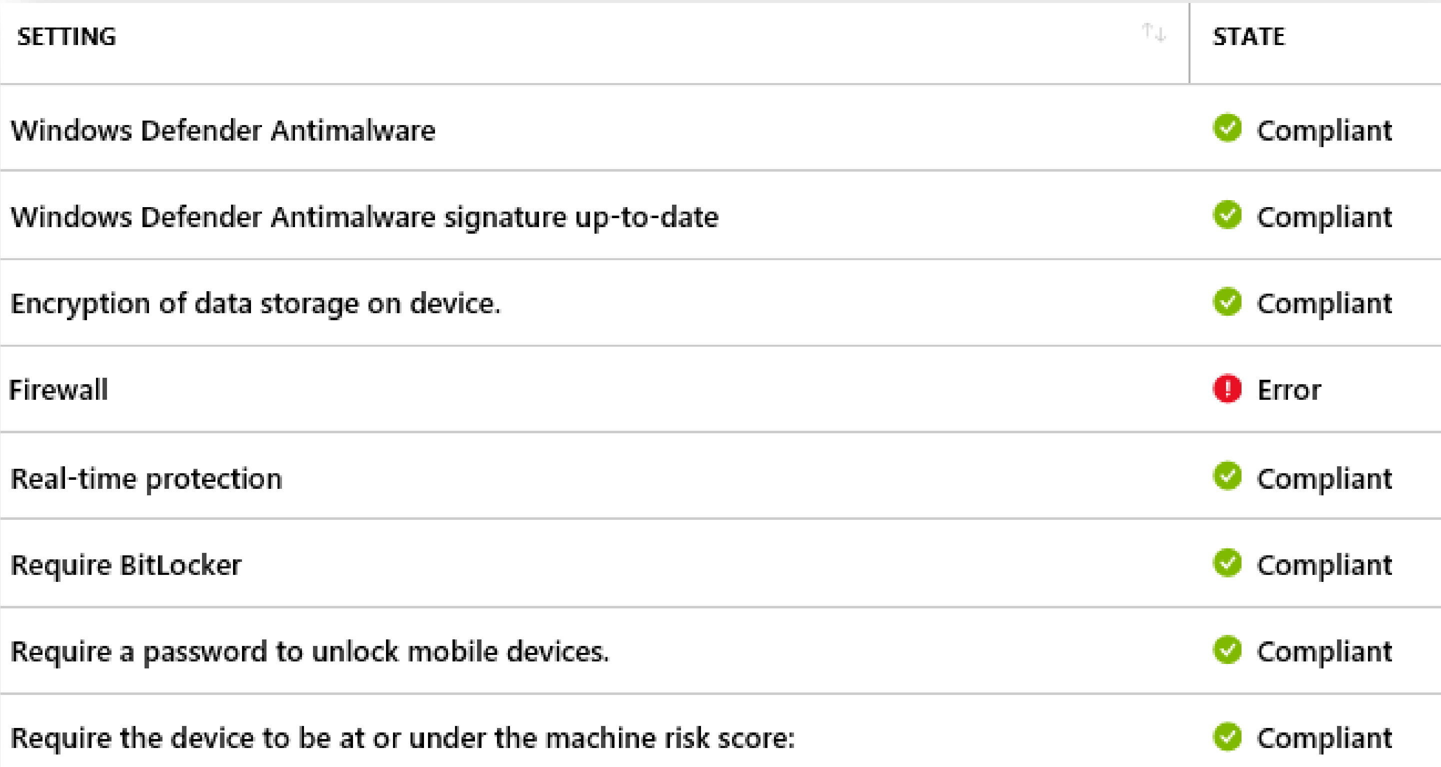
Solution #4 “IP Fencing”

Block all authentication unless it originates from trusted IP networks

Requirement: All Remote users must connect to VPN

Cons:
(1) Not effective for Mobile Devices without ‘Always-on VPN on Mobile’
(2) Not the best user experience to require VPN
(3) Not a ‘Zero Trust’
(4) Not practical for 100% cloud environments

Solution #3 Device Authentication (Option 1: Intune)



SETTING	STATE
Windows Defender Antimalware	✓ Compliant
Windows Defender Antimalware signature up-to-date	✓ Compliant
Encryption of data storage on device.	✓ Compliant
Firewall	❗ Error
Real-time protection	✓ Compliant
Require BitLocker	✓ Compliant
Require a password to unlock mobile devices.	✓ Compliant
Require the device to be at or under the machine risk score:	✓ Compliant

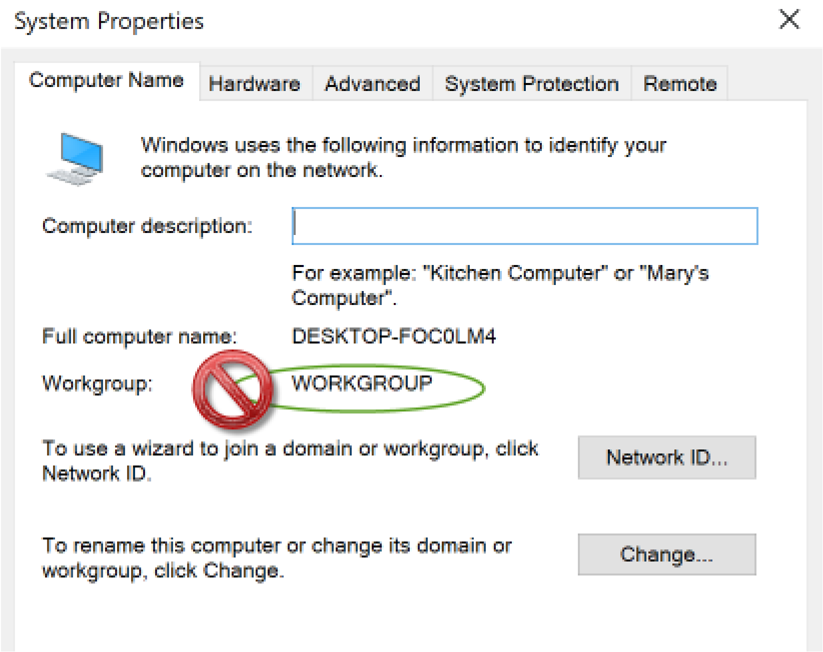
Only allow devices to authenticate if:

1. They are known corporate or personal devices
2. They are healthy and compliant with policies

Benefits:

- **Blocks man-in-the-middle attacks**
- **True Zero Trust**

Solution #4 Device Authentication (Option 2: Verify Domain Join)



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-FOC0LM4

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

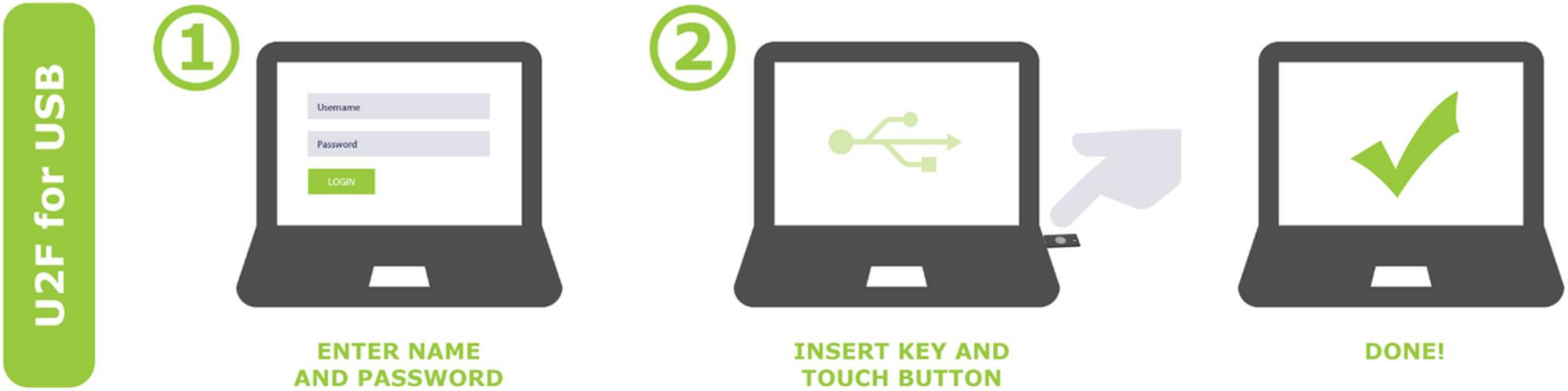
To rename this computer or change its domain or workgroup, click Change.

Block or Restrict Personal Windows Computers

Requires traditional on-premises Active Directory

Cons: (1) Not available for 100% cloud environments
(2) Not available for Mac OSX

Solution #5: U2F Origin Binding



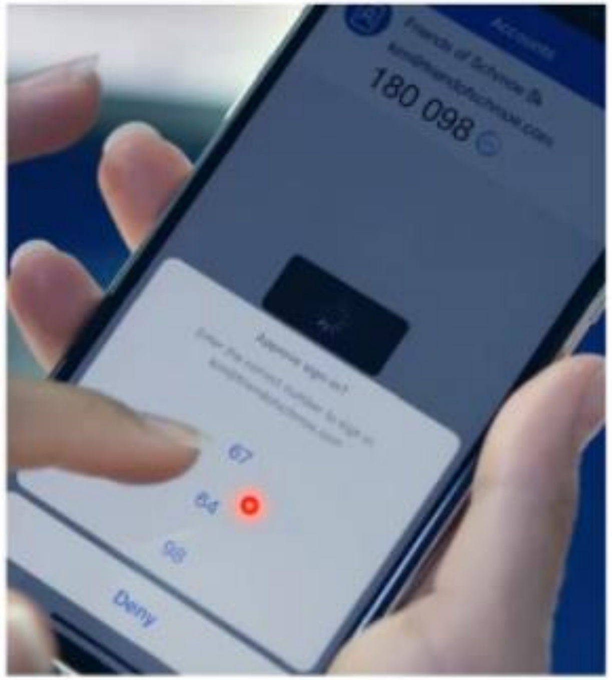
Origin Binding: Defense against Phishing

With the YubiKey, user login is bound to the origin, meaning that only the real site can authenticate with the key. The authentication will fail on the fake site even if the user was fooled into thinking it was real. This greatly mitigates against the increasing volume and sophistication of phishing attacks and stops account takeovers.

Which Passwordless methods work for your users?

Windows Hello for Business

- Information workers with dedicated PC;
- Strong, unphishable credential for sensitive resources
- Microsoft's Premier passwordless experience
- FIDO2 certified



Microsoft Authenticator

- Already using Azure MFA? Easy upgrade to passwordless!
- Best solution for mobile/non-PC users;
- Can be used to bootstrap WHFB.

FIDO2 security keys

- For users accessing shared workstations;
- Simple strong authentication for first line workers;
- Backup/break-glass strong method for Admins

Sample Azure Conditional Access Requirements

Managed device : Domain joined PC, allowed mobile devices on Intune.
Unmanaged device : Workgroup PC, mobile devices that are not compliant.

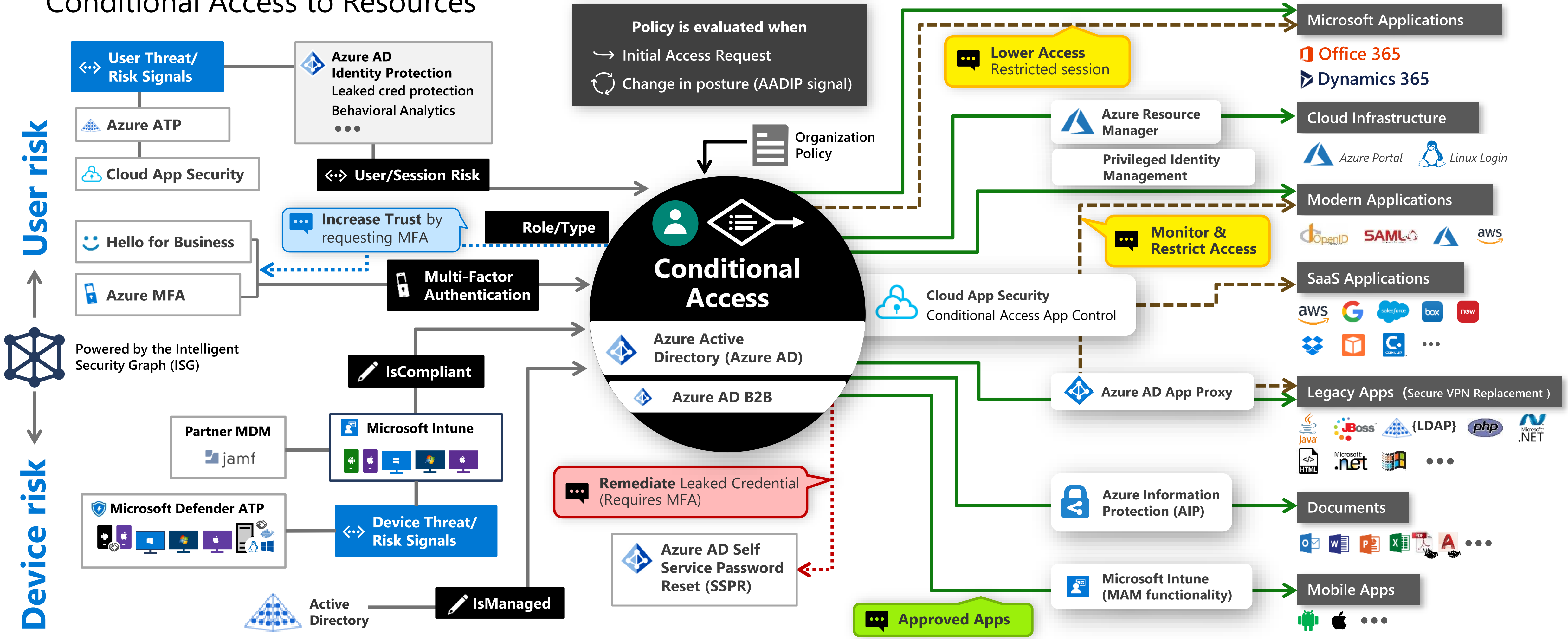
Application/Service	**Corporate Network**		**Public Network**	
	Managed Device	**Unmanaged Device**	**Managed Device**	**Unmanaged Device**
Exchange Online Full Outlook Client	Allow	Block All Access	Require MFA	Block All Access
Exchange Online Outlook on the Web	Allow	Require MFA Block Downloads	Require MFA	Require MFA Block Downloads
SharePoint Online	Allow	Block All Access	Require MFA	Block All Access
OneDrive	Allow	Block All Access	Require MFA	Block All Access
Teams	Allow	Require MFA	Require MFA	Require MFA
Skype for Business	Allow	Require MFA	Require MFA	Require MFA

Zero Trust Access Control

Conditional Access to Resources

Legend

- Full access
- Limited access
- Risk Mitigation
- Remediation Path



User risk

Device risk

Powered by the Intelligent Security Graph (ISG)

User Threat/ Risk Signals

Azure ATP

Cloud App Security

Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
•••

User/Session Risk

Hello for Business

Azure MFA

Increase Trust by requesting MFA

Role/Type

Multi-Factor Authentication

IsCompliant

Partner MDM
jamf

Microsoft Intune

Microsoft Defender ATP

Device Threat/ Risk Signals

Active Directory

IsManaged

Policy is evaluated when
Initial Access Request
Change in posture (AADIP signal)

Organization Policy

Conditional Access

Azure Active Directory (Azure AD)

Azure AD B2B

Remediate Leaked Credential (Requires MFA)

Azure AD Self Service Password Reset (SSPR)

Approved Apps

Lower Access
Restricted session

Azure Resource Manager

Privileged Identity Management

Monitor & Restrict Access

Cloud App Security
Conditional Access App Control

Azure AD App Proxy

Azure Information Protection (AIP)

Microsoft Intune (MAM functionality)

Microsoft Applications
Office 365
Dynamics 365

Cloud Infrastructure
Azure Portal
Linux Login

Modern Applications
OpenID
SAML
aws

SaaS Applications
aws
salesforce
box
now
•••

Legacy Apps (Secure VPN Replacement)
Java
JBoss
{LDAP}
php
.NET
HTML
.net
•••

Documents
•••

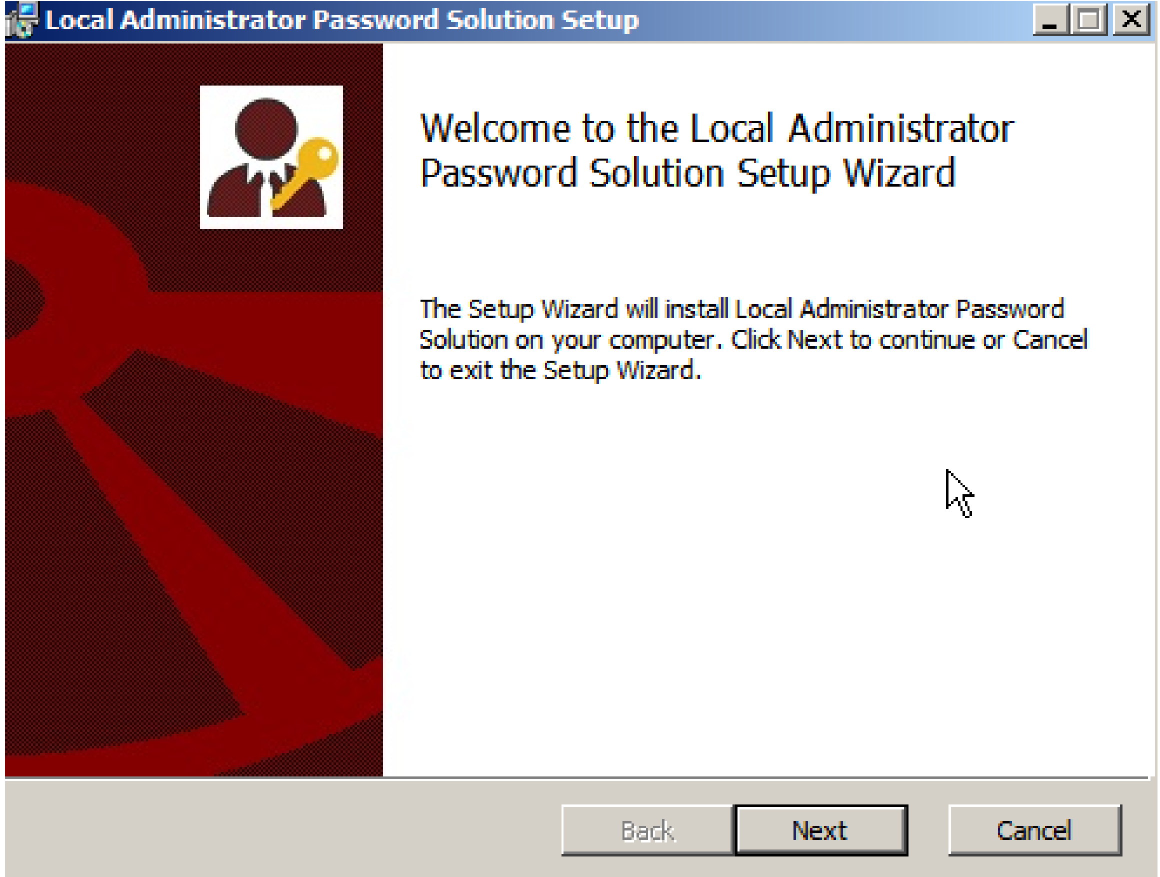
Mobile Apps
•••

Signal
to make an informed decision

Decision
based on organizational policy

Enforcement
of policy across resources

Local Administrator Password Solution (LAPS)



Local Administrator Password Solution Setup

Welcome to the Local Administrator Password Solution Setup Wizard

The Setup Wizard will install Local Administrator Password Solution on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

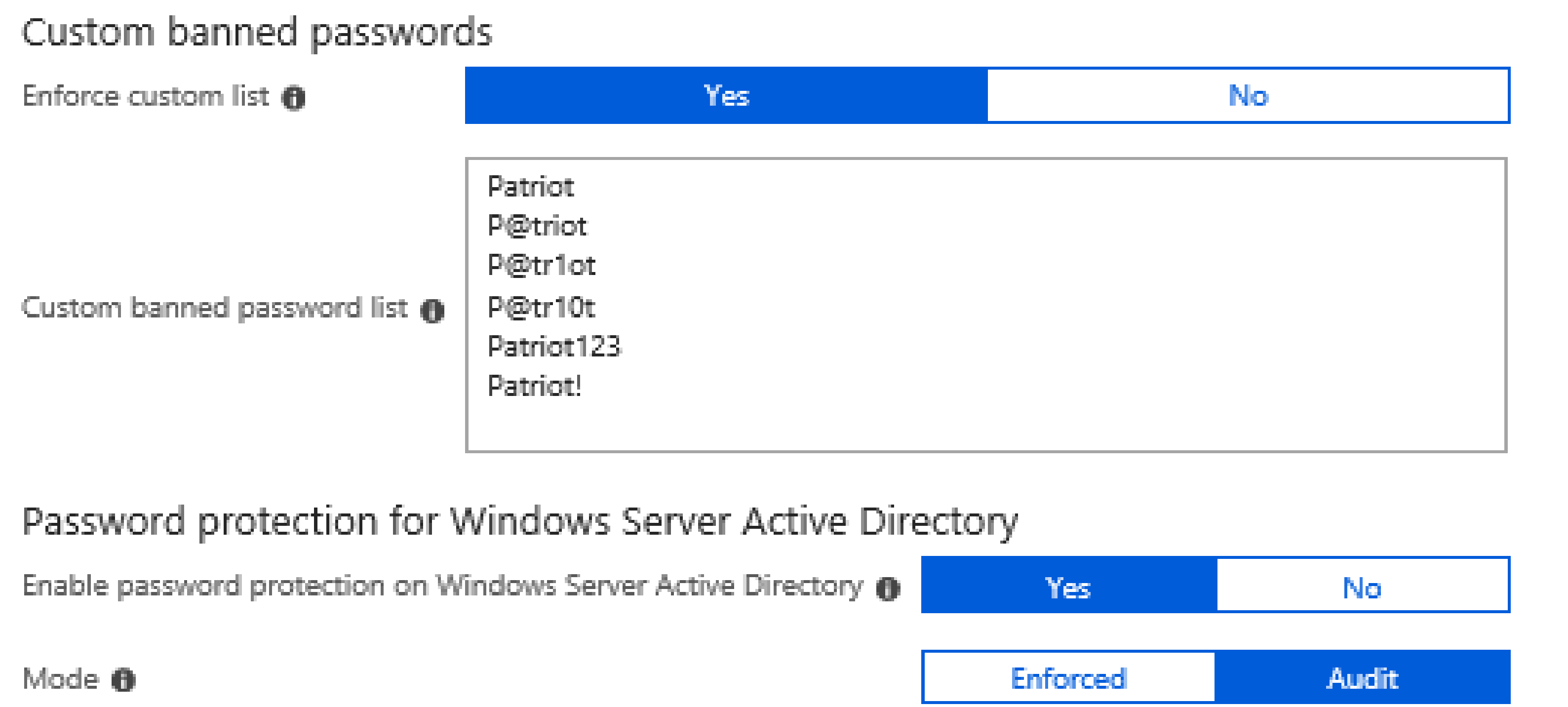
- When the local administrator account has been compromised, attackers can move laterally through the network.
- They can move onto workstations where privileged users such as Domain Admins are logging in and install keystroke loggers or credential stealers to escalate privilege
- LAPS is a free solution that can randomize local admin passwords to prevent this lateral movement.

Ignite 2018 Announcement: LAPS support added for Azure AD joined devices.

Free

PATRIOT CONSULTING

Azure AD Password Protection
Custom Banned Password Lists



Custom banned passwords

Enforce custom list: Yes [✓] | No

Custom banned password list:

```
Patriot
P@triot
P@tr1ot
P@tr10t
Patriot123
Patriot!
```

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes [✓] | No

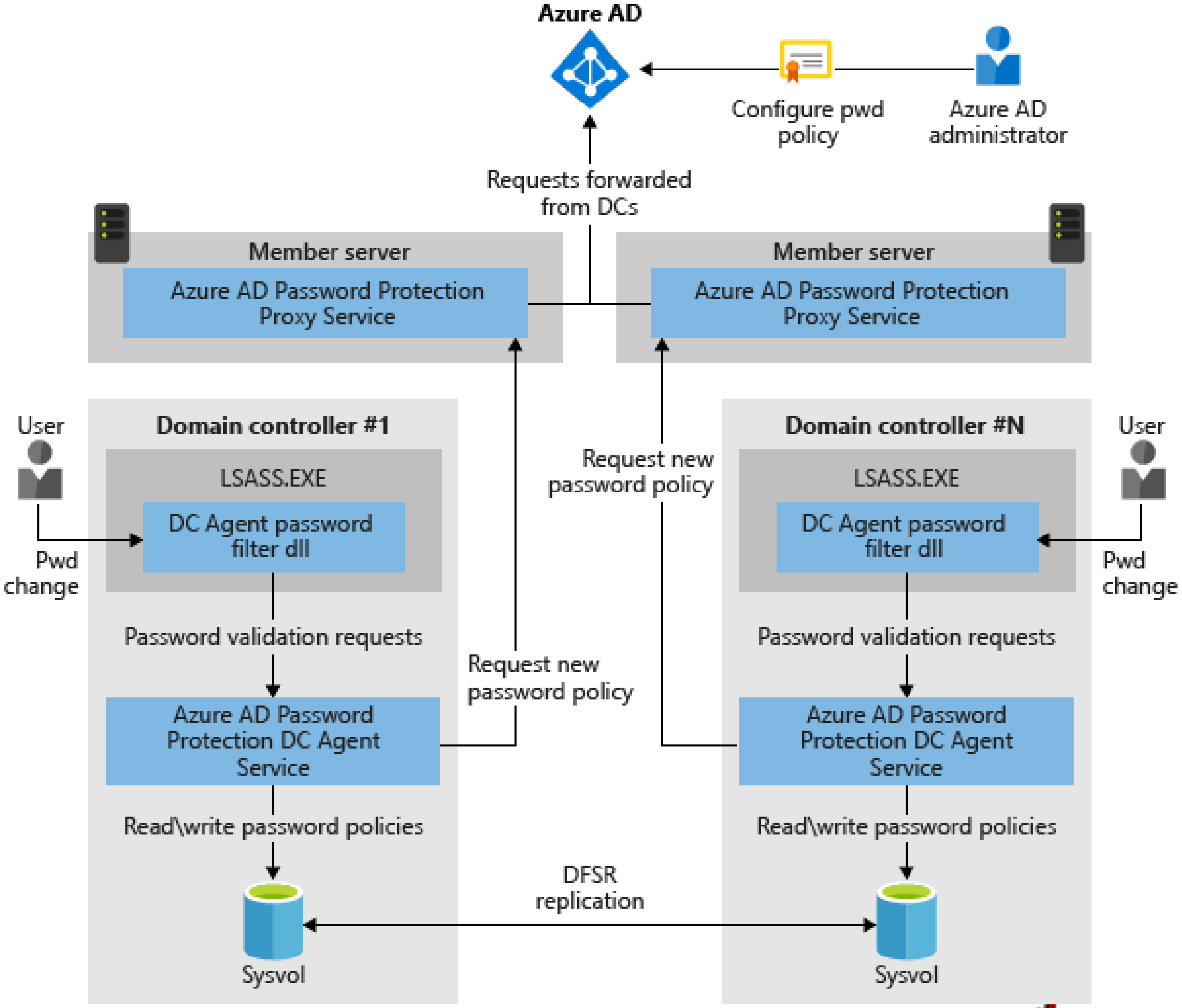
Mode: Enforced | Audit [✓]

EMS E3

PATRIOT
CONSULTING

Azure AD Password Protection Custom Banned Password Lists

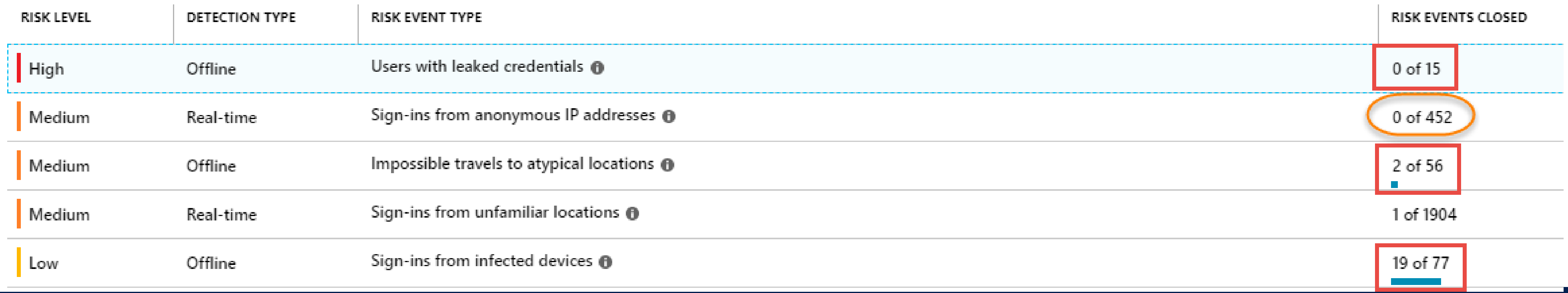
User will see this message:
"Unfortunately, your password contains a word, phrase, or pattern that makes your password easily guessable. Please try again with a different password"



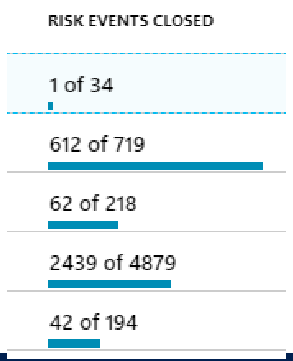
Azure AD
Configure pwd policy
Azure AD administrator
Requests forwarded from DCs
Member server
Azure AD Password Protection Proxy Service
Member server
Azure AD Password Protection Proxy Service
User
Pwd change
Domain controller #1
LSASS.EXE
DC Agent password filter dll
Password validation requests
Azure AD Password Protection DC Agent Service
Read\write password policies
Sysvol
Request new password policy
Request new password policy
DFSR replication
Domain controller #N
LSASS.EXE
DC Agent password filter dll
Password validation requests
Azure AD Password Protection DC Agent Service
Read\write password policies
Sysvol
User
Pwd change

EMS E3

PATRIOT CONSULTING

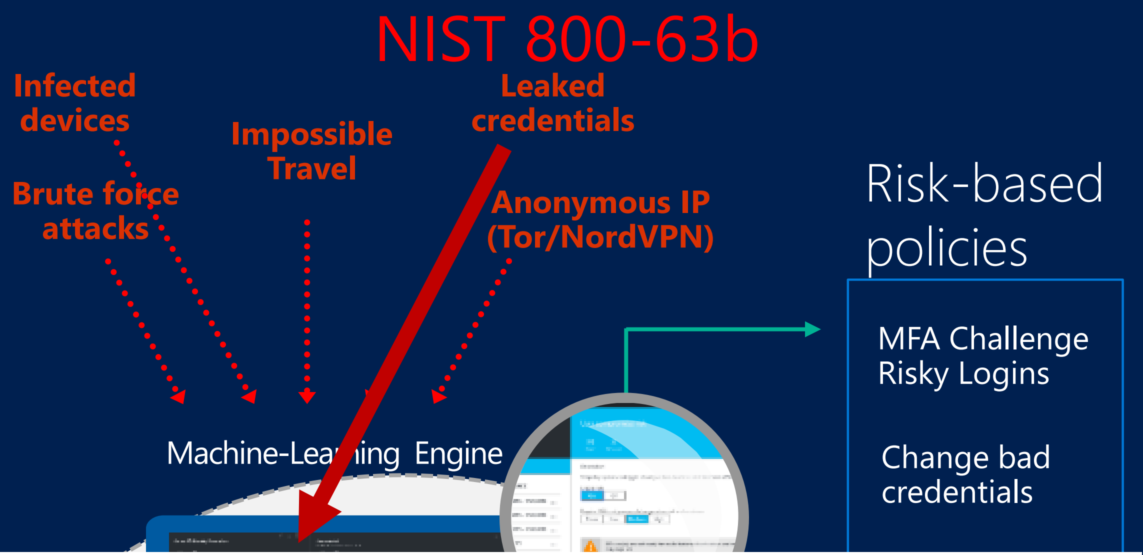


RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED
High	Offline	Users with leaked credentials ⓘ	0 of 15
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	0 of 452
Medium	Offline	Impossible travels to atypical locations ⓘ	2 of 56
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ	1 of 1904
Low	Offline	Sign-ins from infected devices ⓘ	19 of 77



RISK EVENTS CLOSED
1 of 34
612 of 719
62 of 218
2439 of 4879
42 of 194

- Gain insights from a consolidated view of machine learning based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automat protects against suspicious logins and compromised credentials

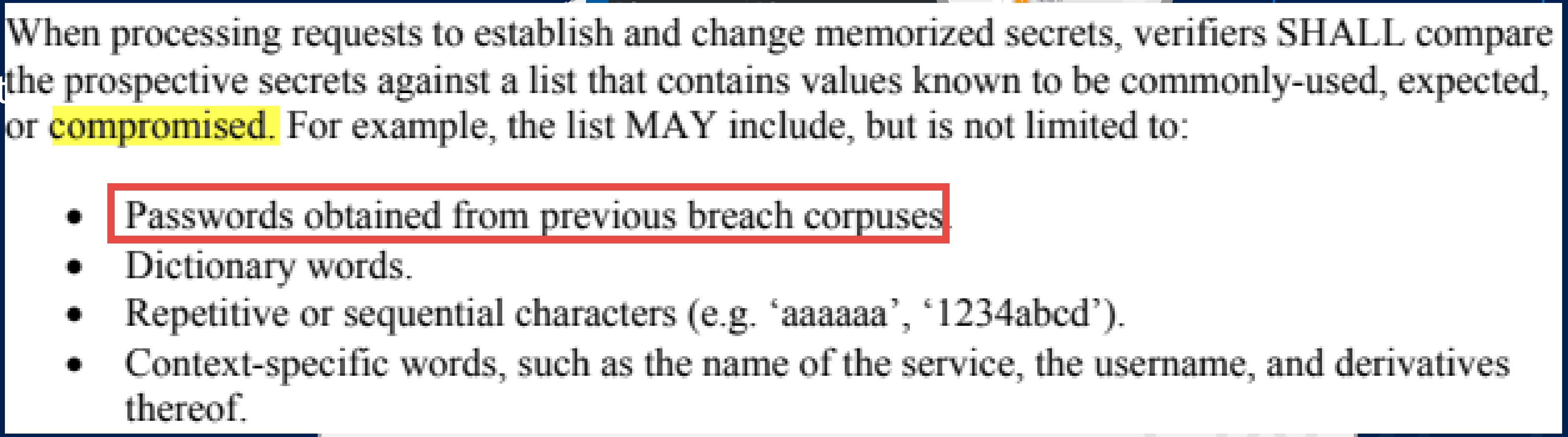


NIST 800-63b

Risk-based policies

MFA Challenge Risky Logins

Change bad credentials



When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised. For example, the list MAY include, but is not limited to:

- Passwords obtained from previous breach corpuses
- Dictionary words.
- Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’).
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

Office 365 Identity Best Practices

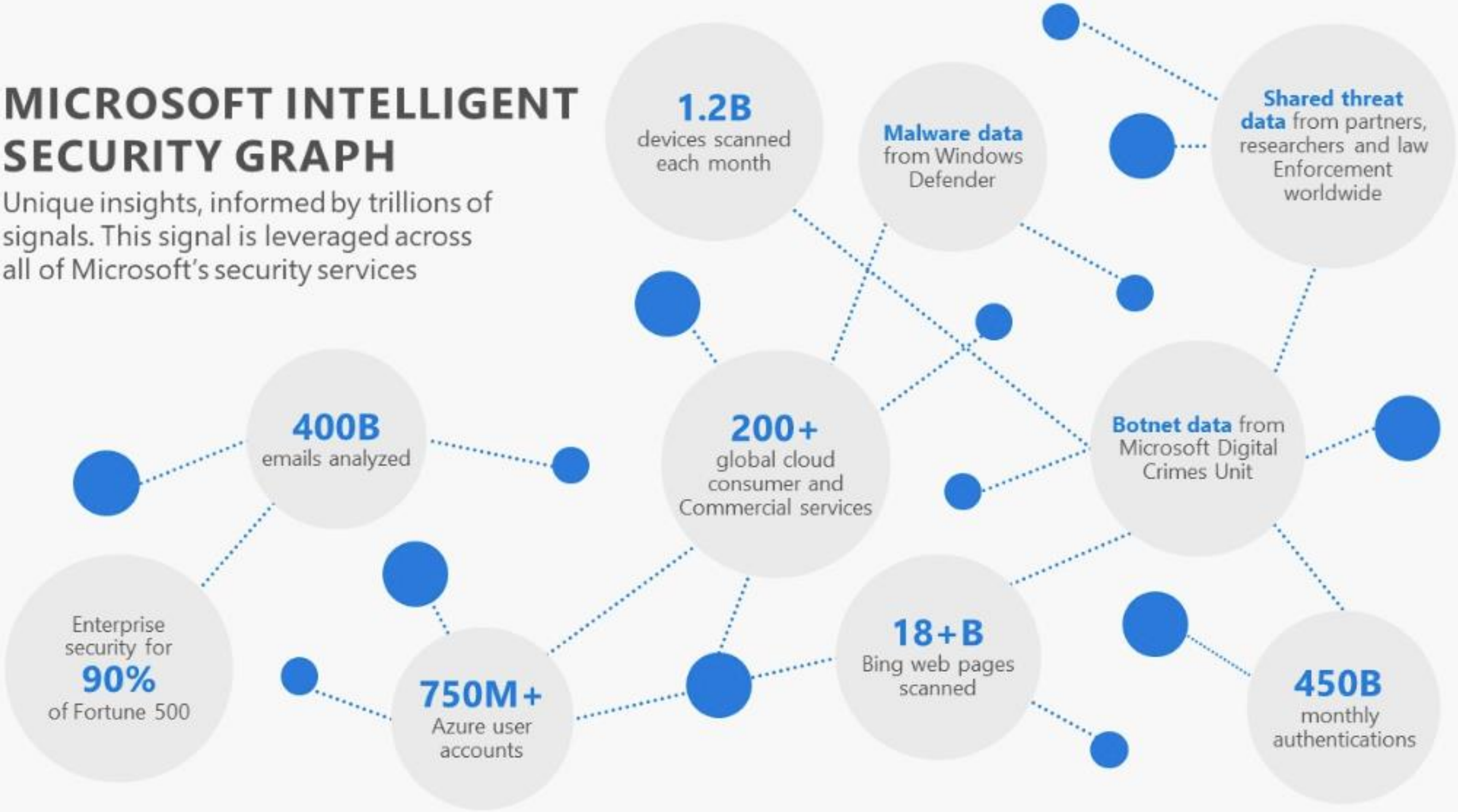
1. GOOD: User-Based MFA
2. BETTER: Passwordless + Device Authentication (Domain Join)
3. **BEST:** Passwordless + Device Compliance + User Behavior + Session Risk

Recommendations

1. Block Legacy Authentication & MFA App Passwords
2. Dynamically Ban Common Passwords
3. Redirect oAuth Requests for Admin Approval
4. Enable Continuous Access Evaluation (Preview)

MICROSOFT INTELLIGENT SECURITY GRAPH

Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services



1.2B devices scanned each month

Malware data from Windows Defender

Shared threat data from partners, researchers and law Enforcement worldwide

400B emails analyzed

200+ global cloud consumer and Commercial services

Botnet data from Microsoft Digital Crimes Unit

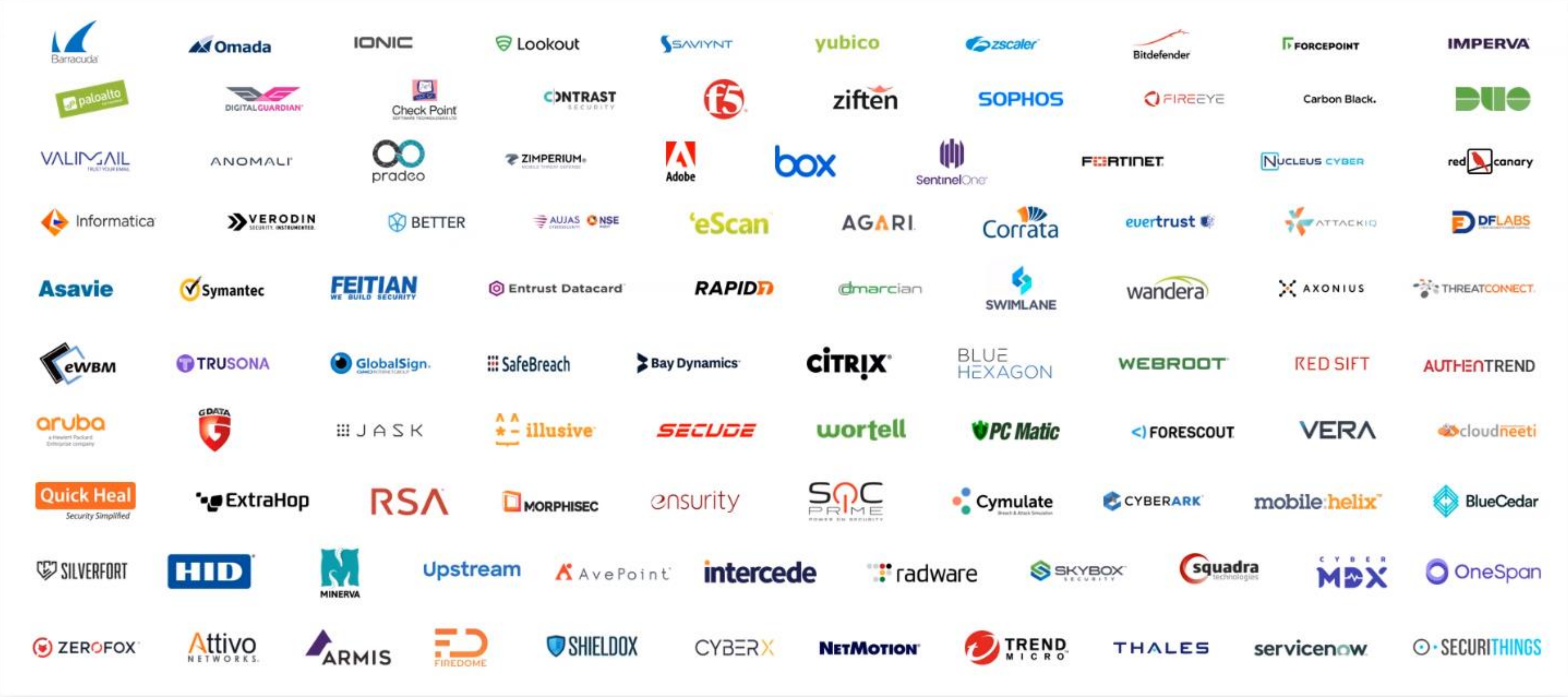
Enterprise security for **90%** of Fortune 500

750M+ Azure user accounts

18+B Bing web pages scanned

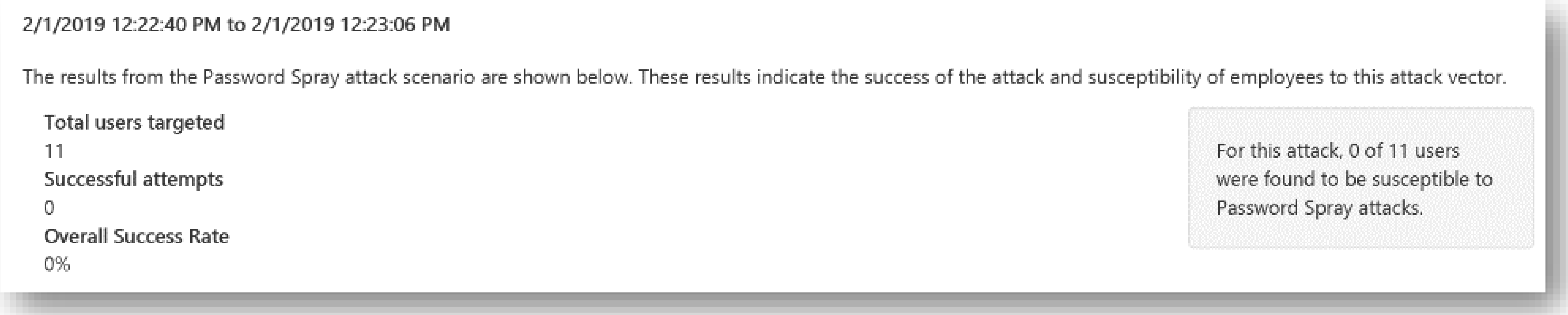
450B monthly authentications

Microsoft Intelligent Security Association



Attack Simulator

- Especially important if you do not have MFA 100% Deployed.
- Check to see which of your users have Passwords found in dictionaries (brute force)
- Check all of your users against a couple of weak passwords (AKA - Password “spray” attacks)



2/1/2019 12:22:40 PM to 2/1/2019 12:23:06 PM

The results from the Password Spray attack scenario are shown below. These results indicate the success of the attack and susceptibility of employees to this attack vector.

Total users targeted
11
Successful attempts
0
Overall Success Rate
0%

For this attack, 0 of 11 users were found to be susceptible to Password Spray attacks.

O365E5

PATRIOT
CONSULTING

Security Issue #2

Spear Phishing

91% of successful data breaches started with a spear-phishing attack [Source: Trend Micro]

92% of malware is delivered by email
[Source: Verizon]

Solution 1: Defender for Office 365 (formerly ATP)

Protection against unknown malware/virus

- Behavioral analysis with machine learning
- Admin alerts

Time of click protection

- Real time protection against Malicious URLs
- 1+Trillion URLs

RISING RISKS

1 IN 10

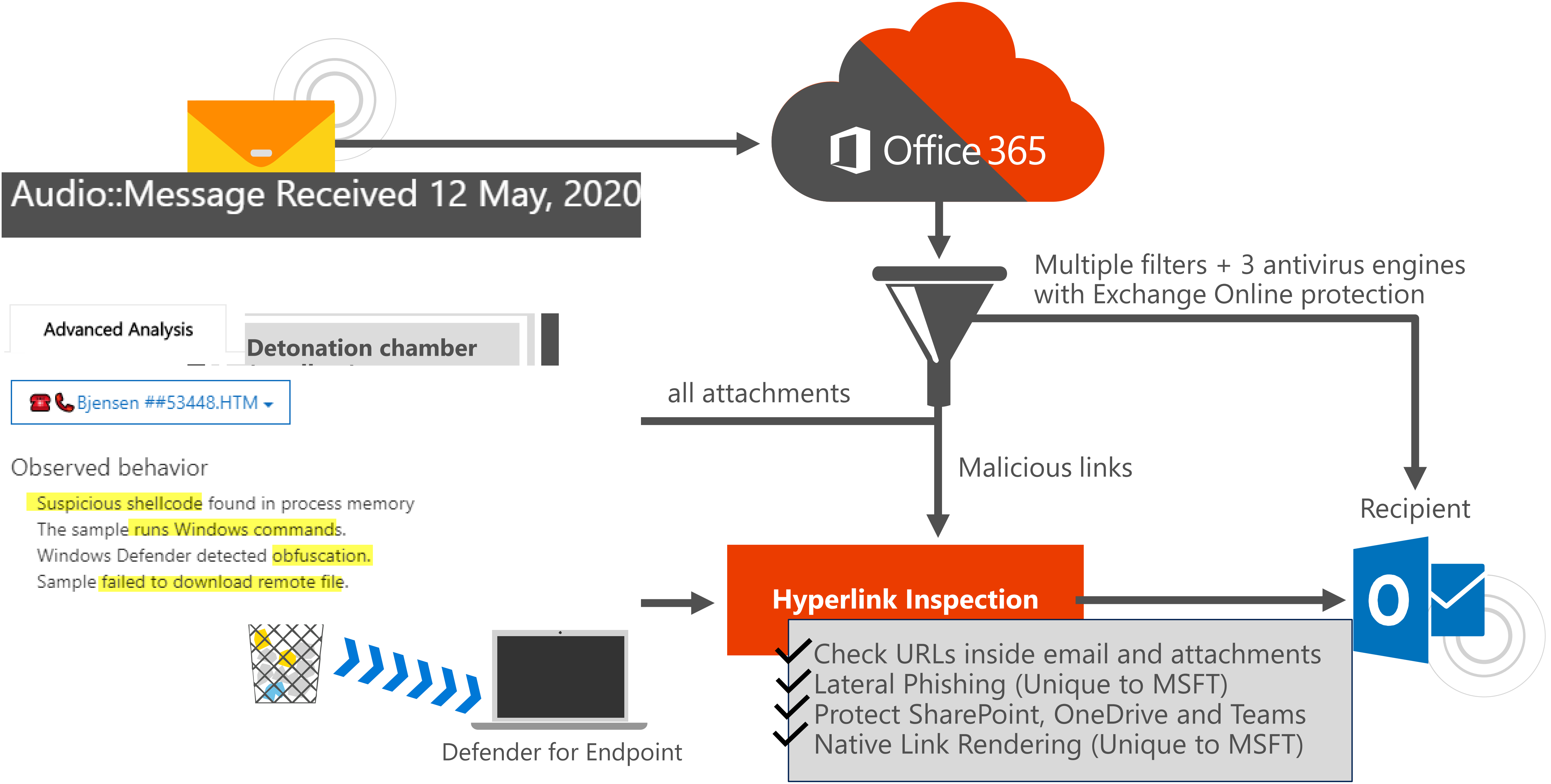
URLs are malicious

Rich reporting and tracing

- Built-in URL trace
- Reports for advanced threats

ATP or O365 E5

Service architecture



Audio::Message Received 12 May, 2020

Advanced Analysis

Detonation chamber

☎📞Bjensen ##53448.HTM ▾

Observed behavior

Suspicious shellcode found in process memory

The sample runs Windows commands.

Windows Defender detected obfuscation.

Sample failed to download remote file.

Hyperlink Inspection

- ✓ Check URLs inside email and attachments
- ✓ Lateral Phishing (Unique to MSFT)
- ✓ Protect SharePoint, OneDrive and Teams
- ✓ Native Link Rendering (Unique to MSFT)

Office 365
Multiple filters + 3 antivirus engines with Exchange Online protection
all attachments
Malicious links
Recipient
Defender for Endpoint

Spear – Phishing Example: "CEO Fraud"

From: Real CEO's Full Name
Sent: Monday, March 21, 2016 9:53 AM
To: (Unsuspecting End-User – Probably in Accounting Department) <AccountingClerk@contoso.com>
Subject: RE: Invoice Payment

Jane,
I need you to process an urgent payment, which needs to go out today as a same value day payment. Let me know when you are set to proceed, so i can have the account information forwarded to you once received.
Awaiting your response.
Regards
Thanks.

Hidden Header Records:
Reply-To: <reply_r@aol.com> (Attacker's address)
Mail-Reply-To: reply_r@aol.com (Attacker's address)

Solution #2 DMARC

Domain-based Message Authentication, Reporting & Conformance”
– RFC 7489 (3/18/2015)

Put Simply: it’s a DNS ‘TXT’ record that tells email gateways to reject emails that did not originate from authorized senders

Sample DMARC TXT Record in External DNS Zone: contoso.com
"v=DMARC1; p=reject; rua=mailto:dmarcagg@contoso.com“

Free

How DMARC protects against "CEO Fraud"

('aka Business Email Compromise')

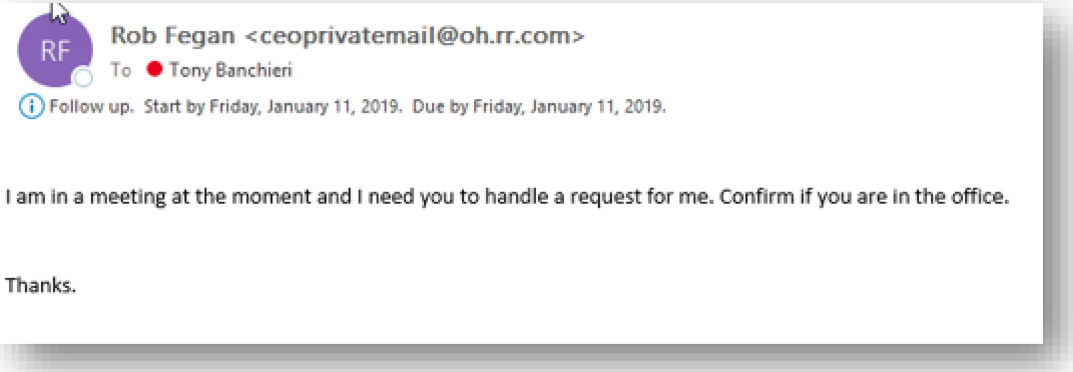
RFC 5322.From Protected by DMARC

From: "Jack Johnson" <jack.johnson@contoso.com>
Sent: Monday, March 21, 2016 9:53 AM
To: (Unsuspecting End-User – Probably in Accounting Department) <AccountingClerk@contoso.com>
Subject: RE: Invoice Payment

Key Point:
Sender Policy Framework (SPF) protects the RFC 5321.MailFrom Field
DMARC protects against the RFC 5322.From field (Display Address)

Anti-Phishing and Anti-Impersonation

Anti-impersonation detects identical names in the from field



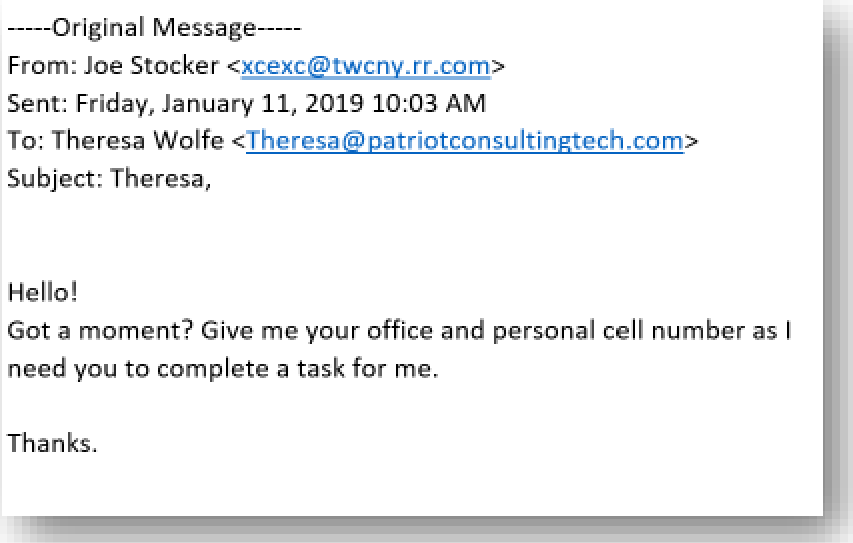
Rob Fegan <ceoprivatemail@oh.rr.com>

To ● Tony Banchieri

ⓘ Follow up. Start by Friday, January 11, 2019. Due by Friday, January 11, 2019.

I am in a meeting at the moment and I need you to handle a request for me. Confirm if you are in the office.

Thanks.



-----Original Message-----
From: Joe Stocker <xcexc@twcny.rr.com>
Sent: Friday, January 11, 2019 10:03 AM
To: Theresa Wolfe <Theresa@patriotconsultingtech.com>
Subject: Theresa,

Hello!
Got a moment? Give me your office and personal cell number as I need you to complete a task for me.

Thanks.

Anti-phishing detects slight changes in domains ***you own***

CEO Identity = Joe@Contoso.com

Spoofs Detected = Joe@C0ntoso.com

Anti-Impersonation Features

Display protected by Anti-Impersonation

Misspelled domain name detected by Anti-Impersonati

From: "Jack Johnson" <jack.johnson@conttoso.com>
Sent: Monday, March 21, 2016 9:53 AM
To: (Unsuspecting End-User – Probably in Accounting Department)
<AccountingClerk@contoso.com>
Subject: RE: Invoice Payment

Key Points:

- **DMARC only helps when you own the domain being spoofed. It can't help you when the attacker buys a misspelled domain name. That is why you need anti-impersonation, part of the Anti-Phish policy.**
- **Anti-Impersonation helps because attackers are aware of DMARC and are trying to evade it.**

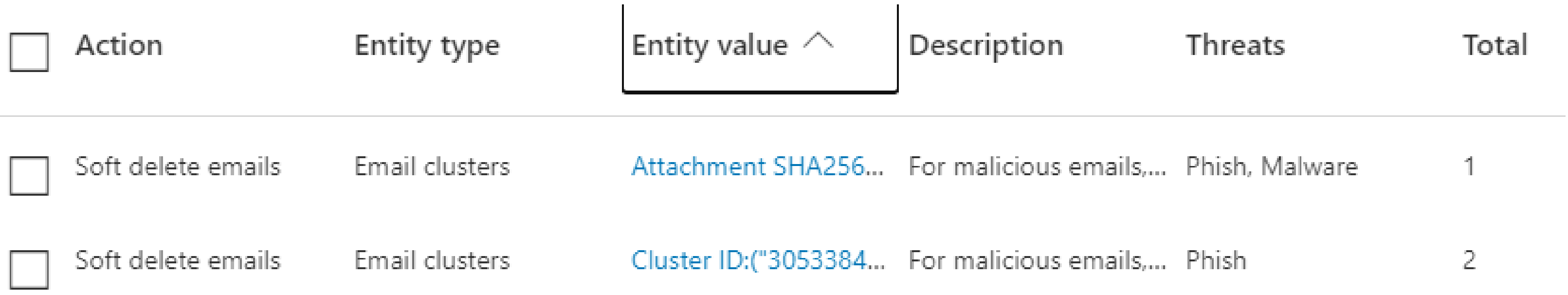
Automated Investigation and Response (AIR)

After a potentially malicious URL click is detected in email, automated playbooks will launch investigations.

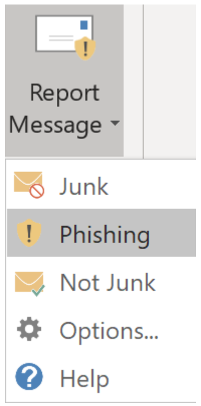
They're based on input from Security Operations and Incident Response teams, including those who help defend Microsoft and our customers assets.

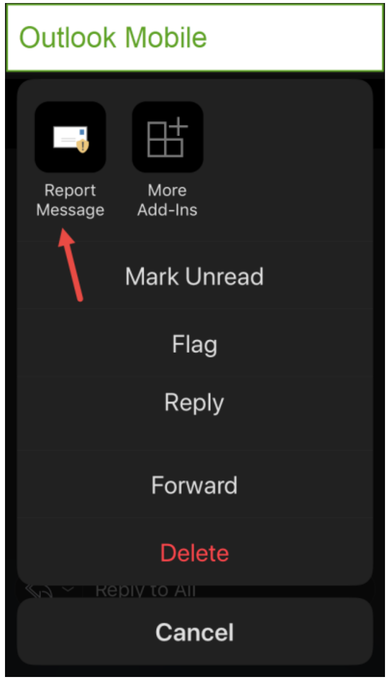
How it works:

- User-reported phish message from the Outlook Add-in “Report Phish”
- Admin views correlation with other threats and is presented with recommended actions
- Admin purges emails (no PowerShell required)



□	Action	Entity type	Entity value ^	Description	Threats	Total
□	Soft delete emails	Email clusters	Attachment SHA256...	For malicious emails,...	Phish, Malware	1
□	Soft delete emails	Email clusters	Cluster ID:("3053384...	For malicious emails,...	Phish	2





M365 E5 or M365 E5 Security Bundle

Phishing Simulator

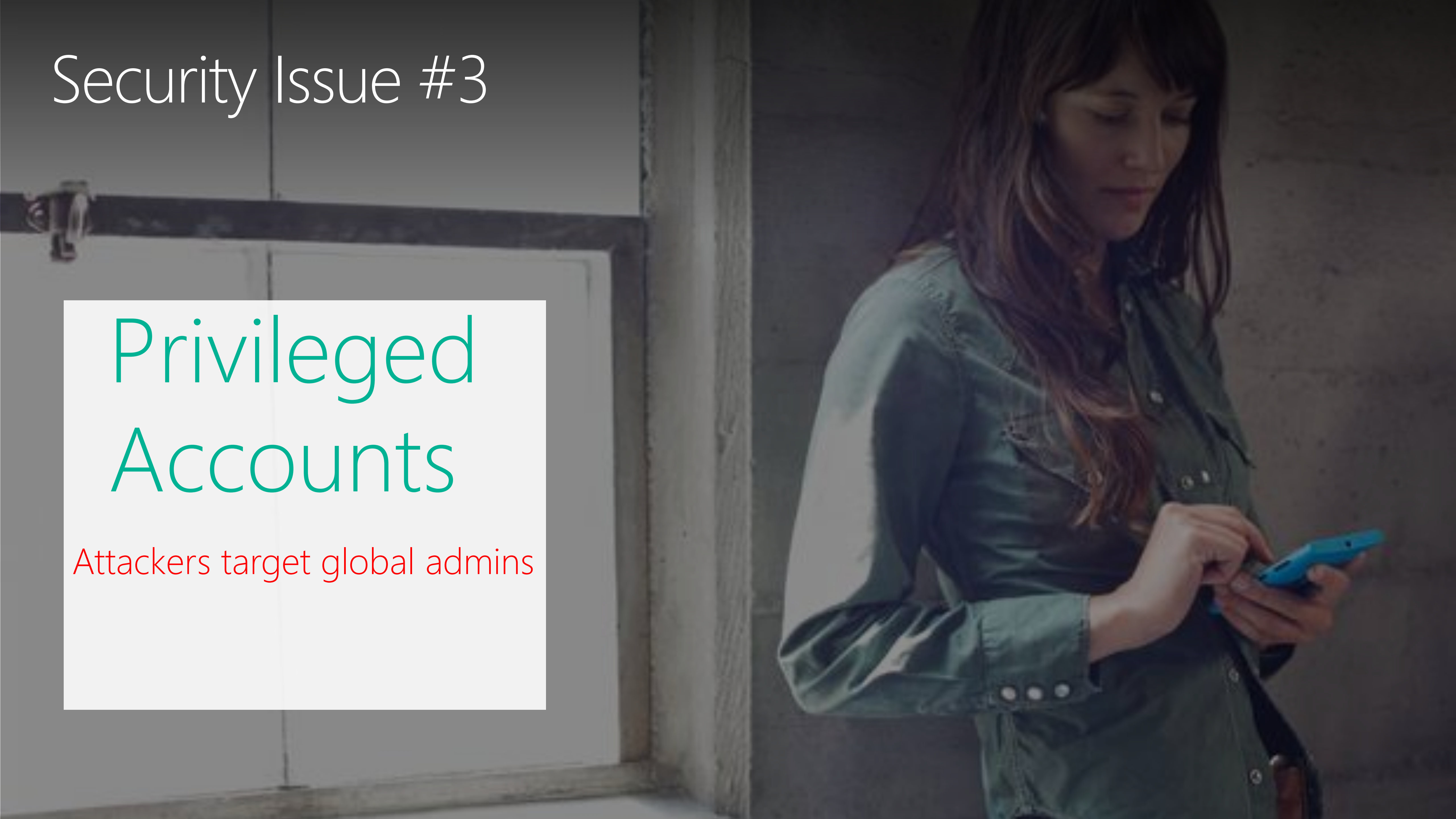
Simulates phishing attacks, available in Threat Intelligence license or E5 license

Send emails that spoof your CEO Identity = Joe@Contoso.com

Get a report of which users clicked on the link, and of those, how many entered their O365 credentials

O365 E5

Security Issue #3



Privileged Accounts

Attackers target global admins

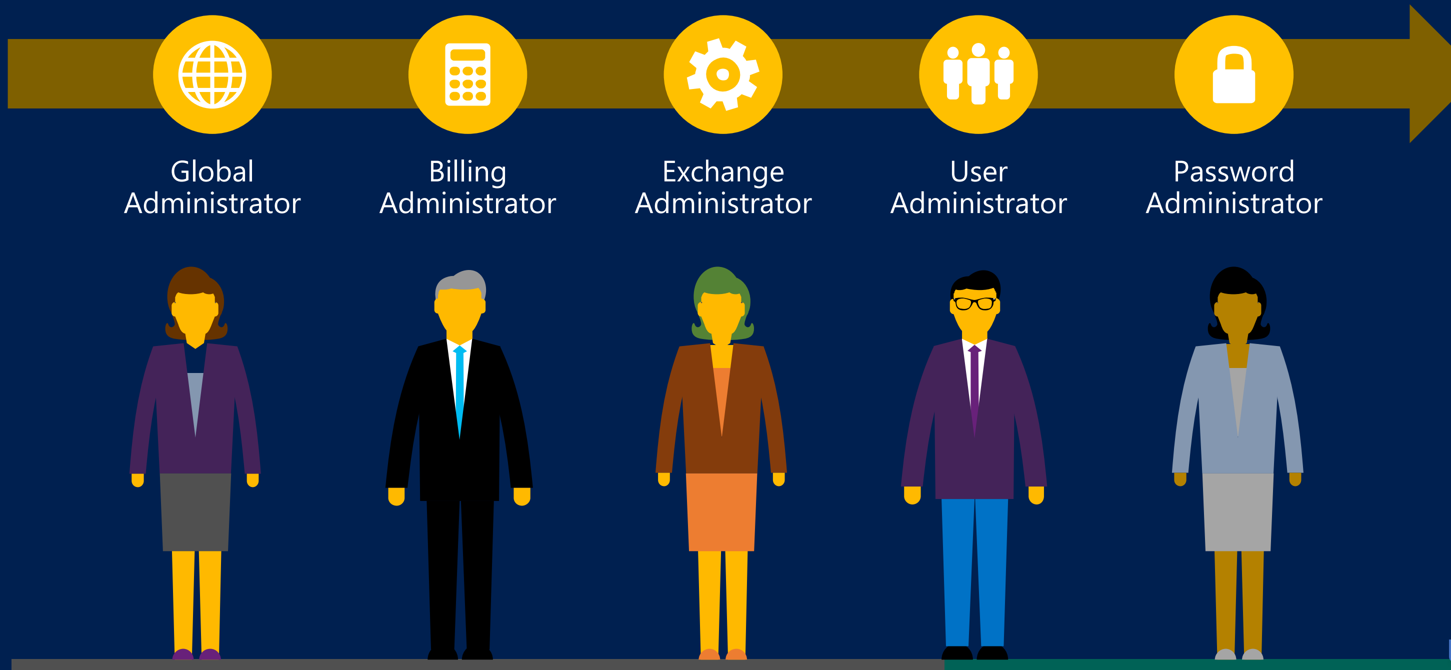
CLOUD-POWERED PROTECTION

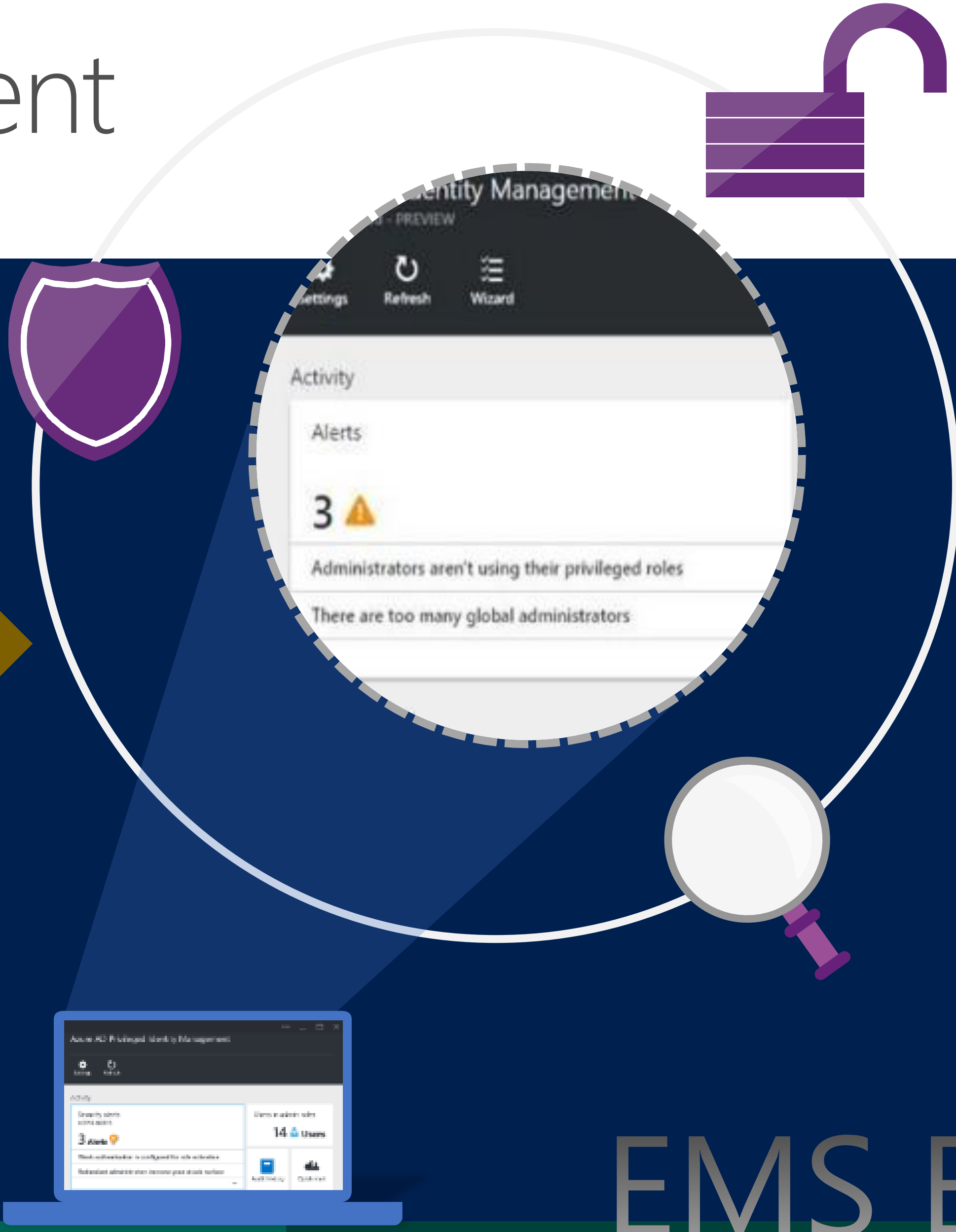
Privileged Identity Management

Discover, restrict, and monitor privileged identities

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

Provides more visibility through alerts, audit reports and access reviews





Activity

Alerts

3

Administrators aren't using their privileged roles

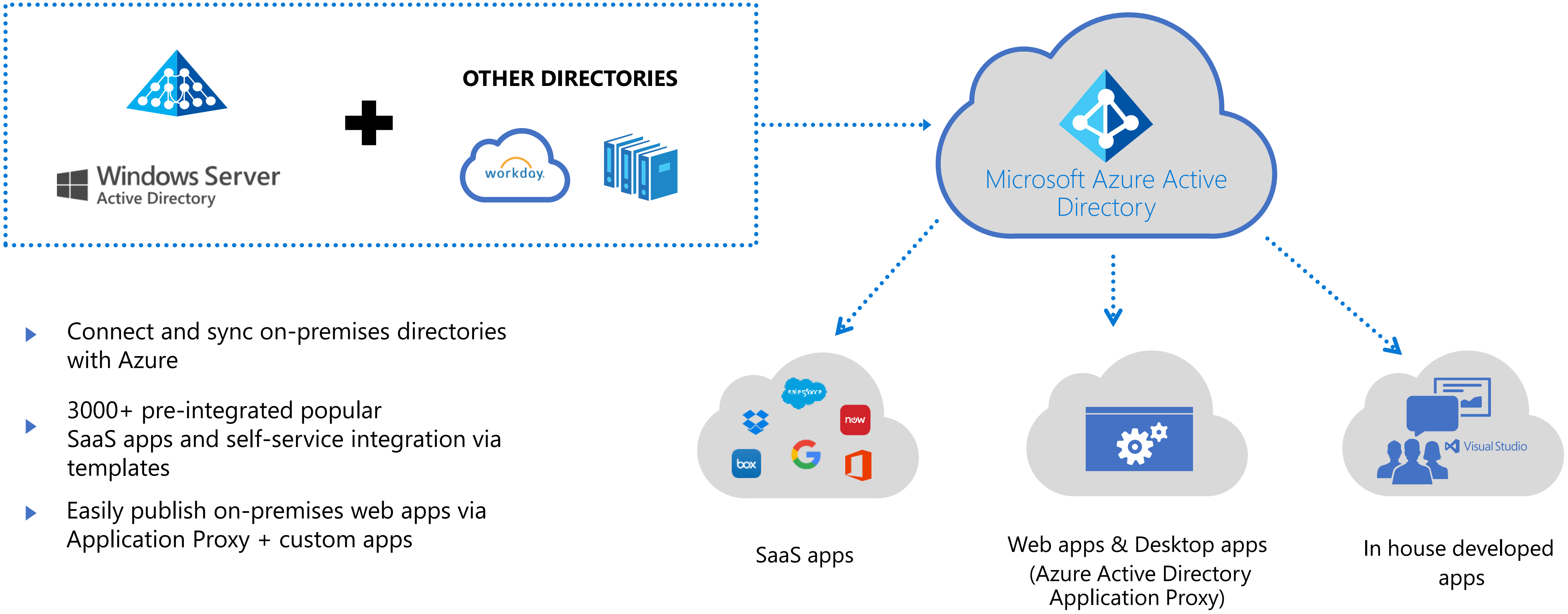
There are too many global administrators

EMS E5

Security Issue #4

Enable Single Sign-On (SSO)

Single sign-on to any application



Windows Server Active Directory

OTHER DIRECTORIES

Microsoft Azure Active Directory

SaaS apps

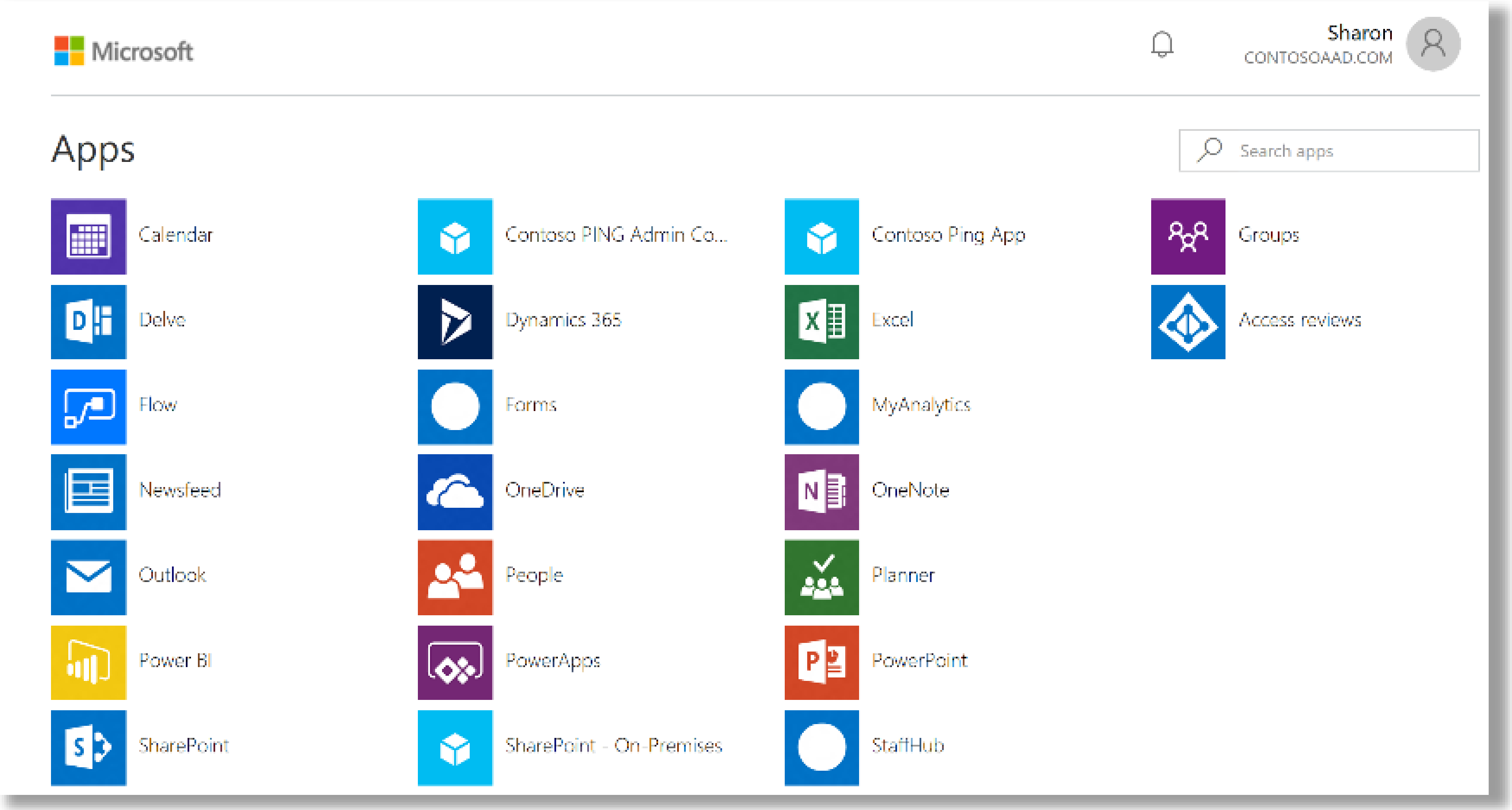
Web apps & Desktop apps (Azure Active Directory Application Proxy)

In house developed apps

- Connect and sync on-premises directories with Azure
- 3000+ pre-integrated popular SaaS apps and self-service integration via templates
- Easily publish on-premises web apps via Application Proxy + custom apps

Universal SSO is now free (4/30/2020)

Access all your applications



Microsoft

Sharon
CONTOSOAAD.COM

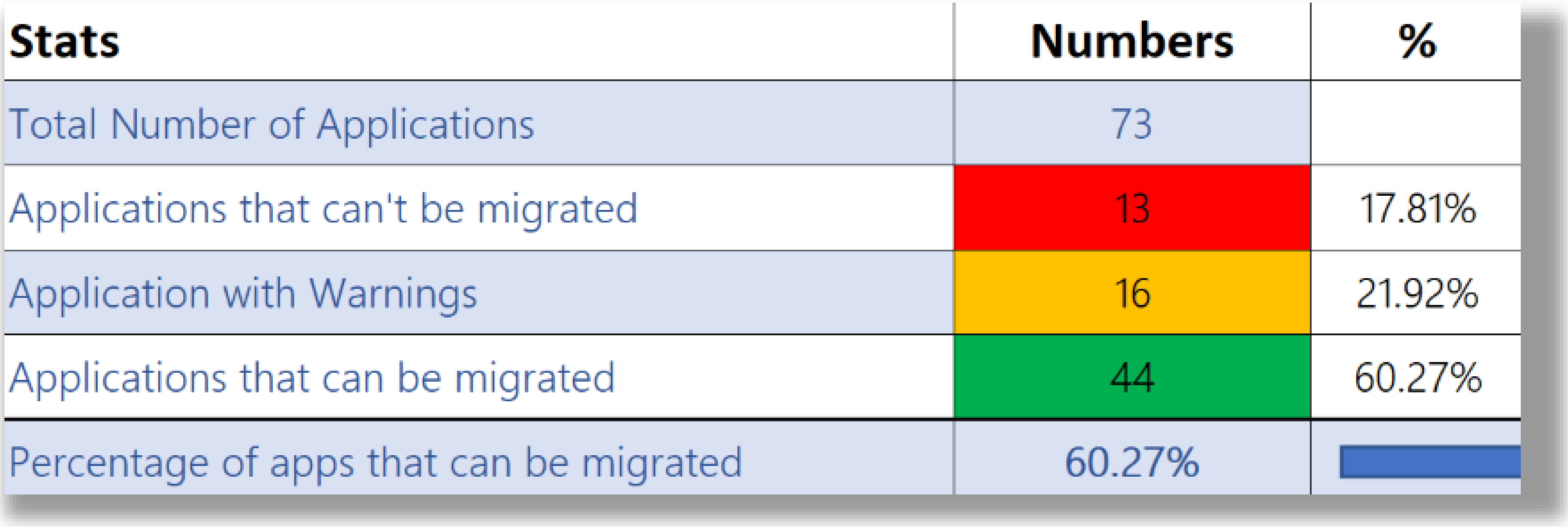
Apps

Search apps

Calendar	Contoso PING Admin Co...	Contoso Ping App	Groups
Delve	Dynamics 365	Excel	Access reviews
Flow	Forms	MyAnalytics	
Newsfeed	OneDrive	OneNote	
Outlook	People	Planner	
Power BI	PowerApps	PowerPoint	
SharePoint	SharePoint - On-Premises	StaffHub	

ADFS to Azure AD App Migration Tool

1. **Collect** app configurations from ADFS
2. **Analyze** app configurations
3. **Report** migration feasibility



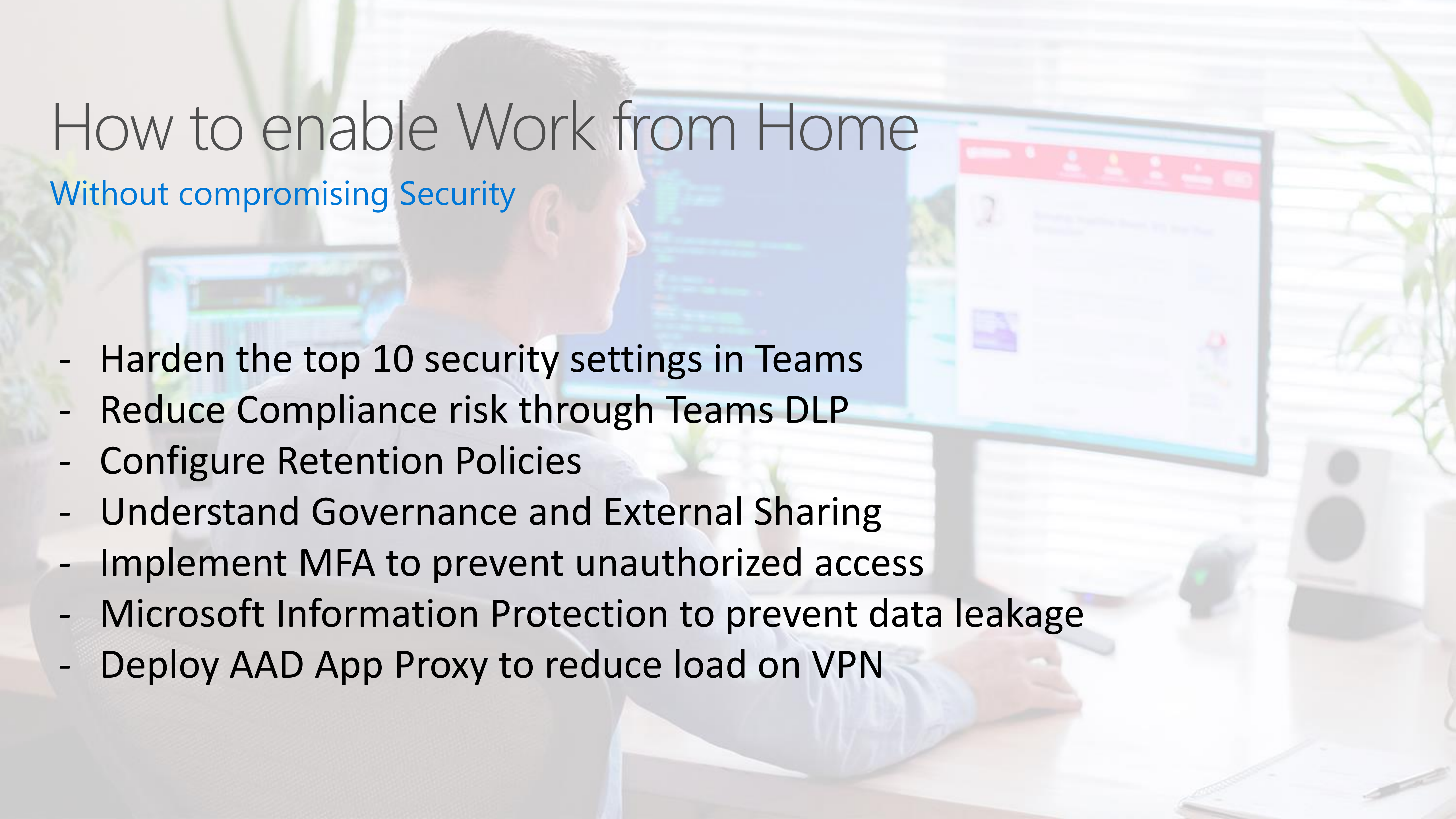
Stats	Numbers	%
Total Number of Applications	73	
Applications that can't be migrated	13	17.81%
Application with Warnings	16	21.92%
Applications that can be migrated	44	60.27%
Percentage of apps that can be migrated	60.27%	▬

Security Issue #5

Enable Work from Home Securely

How to enable Work from Home

Without compromising Security



- Harden the top 10 security settings in Teams
- Reduce Compliance risk through Teams DLP
- Configure Retention Policies
- Understand Governance and External Sharing
- Implement MFA to prevent unauthorized access
- Microsoft Information Protection to prevent data leakage
- Deploy AAD App Proxy to reduce load on VPN

Top 10 Settings to review in Teams

1. Data Loss Prevention
2. Retention
3. External Sharing
4. Conditional Access (MFA)
5. Encryption (Prevent data leakage with Information Protection)
6. Group Creation (self-service or restricted)
7. 3rd party cloud storage
8. 3rd party app integration
9. Auditing
10. Guest Access

Offer

SecureAudit365 for Teams

by Patriot Consulting

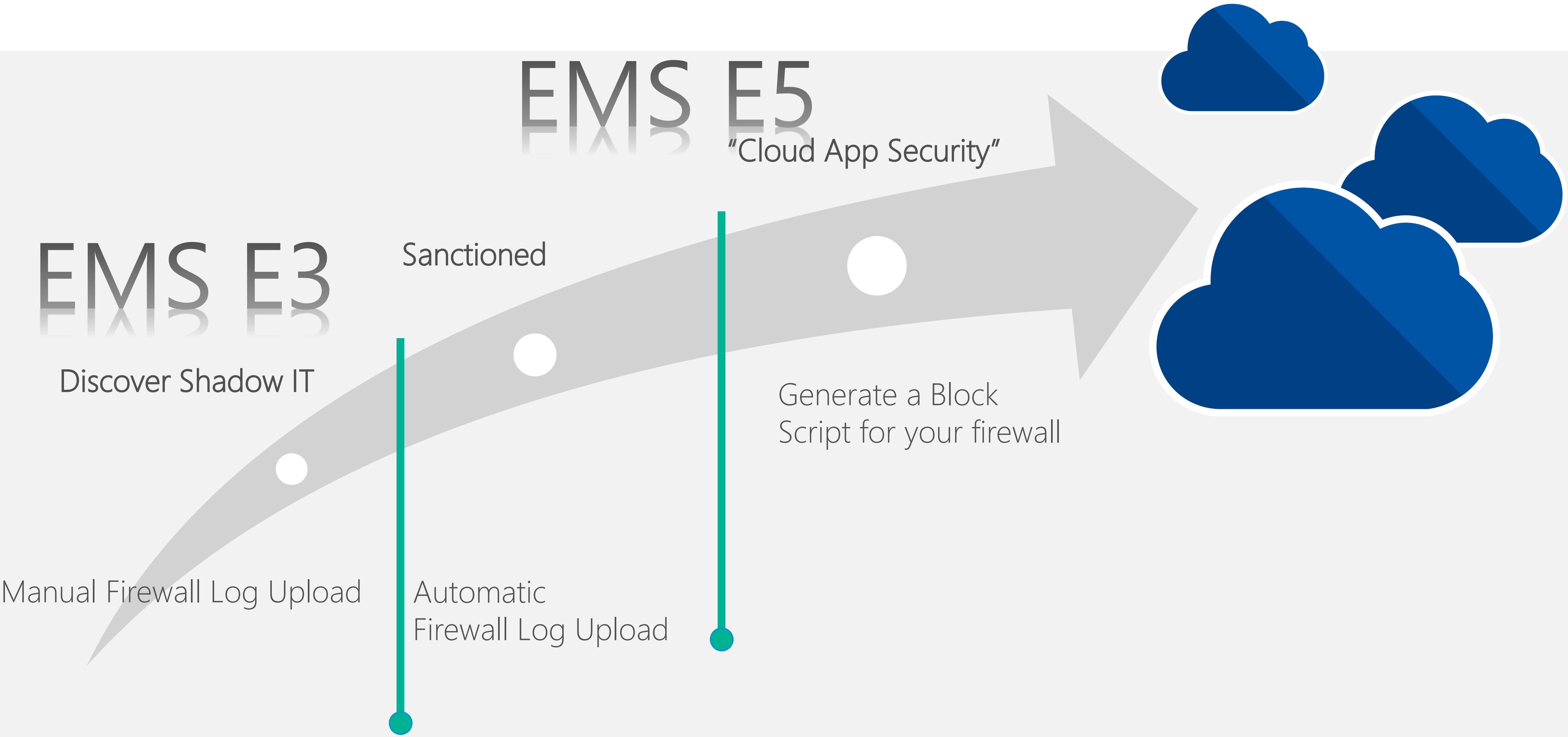
Patriot SecureAudit365 for Teams

- Harden over 100 Teams Security Settings
- Reduce Compliance risk through Teams DLP
- Configure Retention Policies
- Governance and External Sharing
- Network Optimization Best Practices
- Prevent unauthorized access with MFA
- Prevent data leakage with Information Protection
- Adoption and Rollout guidance
- Training Videos and Quick Start Guides

Security Issue #6

Shadow IT

Discover Shadow IT with Cloud App Security



EMS E3

Discover Shadow IT

Manual Firewall Log Upload

Sanctioned

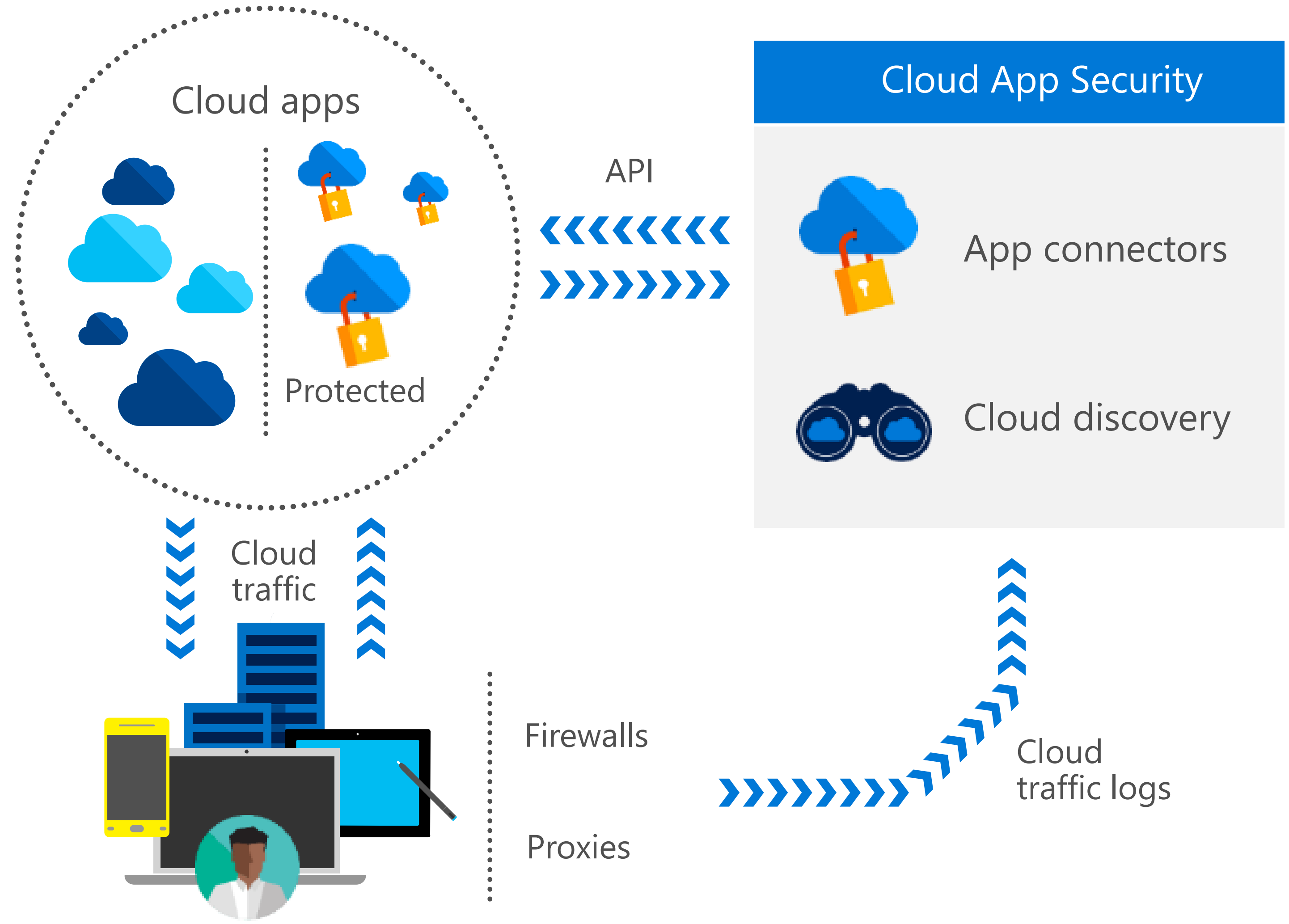
Automatic
Firewall Log Upload

EMS E5

"Cloud App Security"

Generate a Block
Script for your firewall

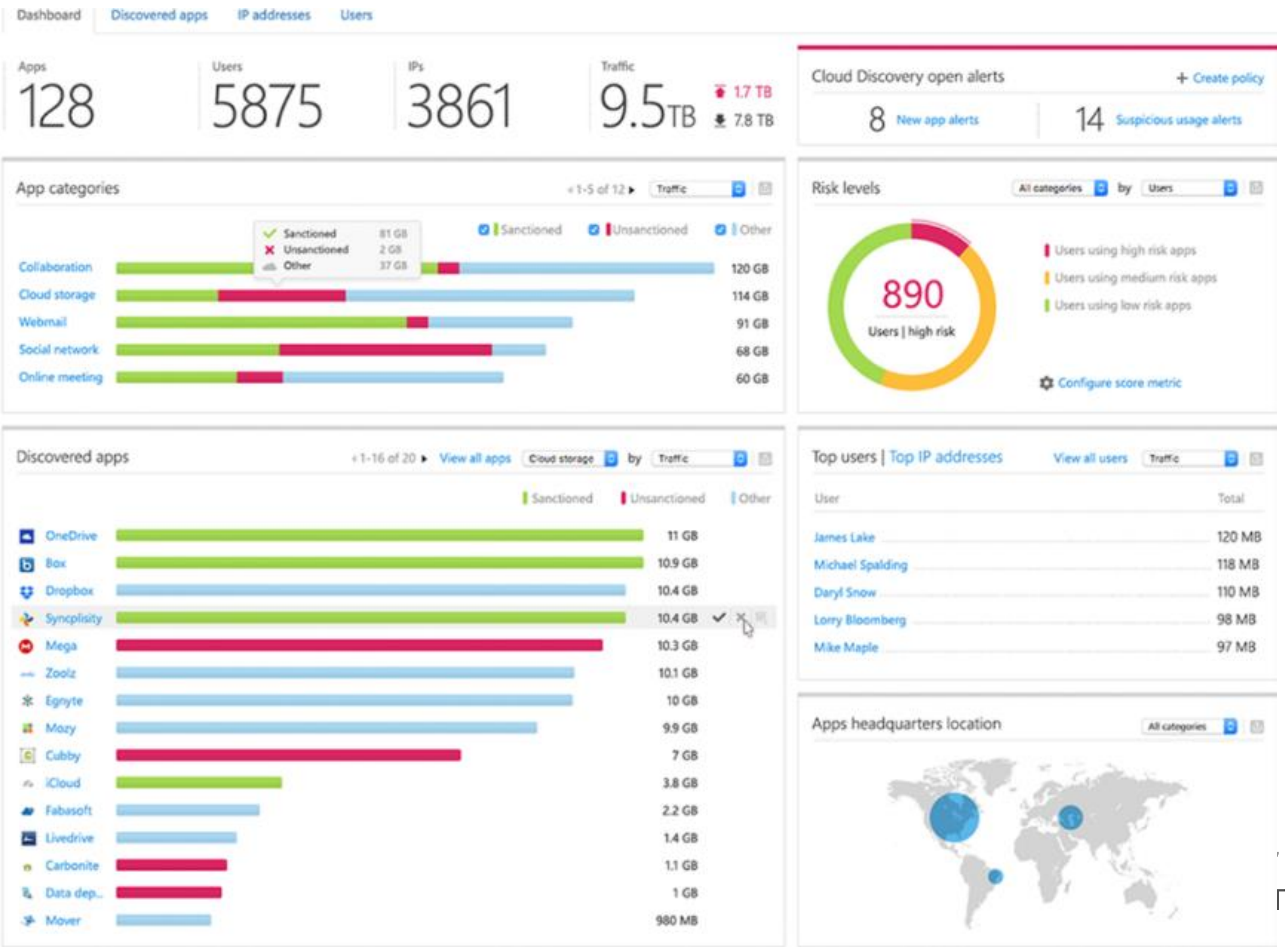
Discover Shadow IT



Your organization from any location

Can you spot the problem?

Issue: Remote Workers bypass Firewalls



Dashboard | Discovered apps | IP addresses | Users

Apps	Users	IPs	Traffic
128	5875	3861	9.5TB (↑ 1.7 TB, ↓ 7.8 TB)

Cloud Discovery open alerts + Create policy

8 New app alerts | 14 Suspicious usage alerts

App categories ◂ 1-5 of 12 ▸ Traffic

☑ Sanctioned ☑ Unsanctioned ☑ Other

✓ Sanctioned 81 GB
✕ Unsanctioned 2 GB
Other 37 GB

Category	Total
Collaboration	120 GB
Cloud storage	114 GB
Webmail	91 GB
Social network	68 GB
Online meeting	60 GB

Risk levels All categories by Users

890 Users \| high risk

- Users using high risk apps
- Users using medium risk apps
- Users using low risk apps

⚙ Configure score metric

Discovered apps ◂ 1-16 of 20 ▸ View all apps Cloud storage by Traffic

Sanctioned | Unsanctioned | Other

App	Traffic
OneDrive	11 GB
Box	10.9 GB
Dropbox	10.4 GB
Syncplisity	10.4 GB
Mega	10.3 GB
Zoolz	10.1 GB
Egnyte	10 GB
Mozy	9.9 GB
Cubby	7 GB
iCloud	3.8 GB
Fabasoft	2.2 GB
Livedrive	1.4 GB
Carbonite	1.1 GB
Data dep...	1 GB
Mover	980 MB

Top users \| Top IP addresses View all users Traffic

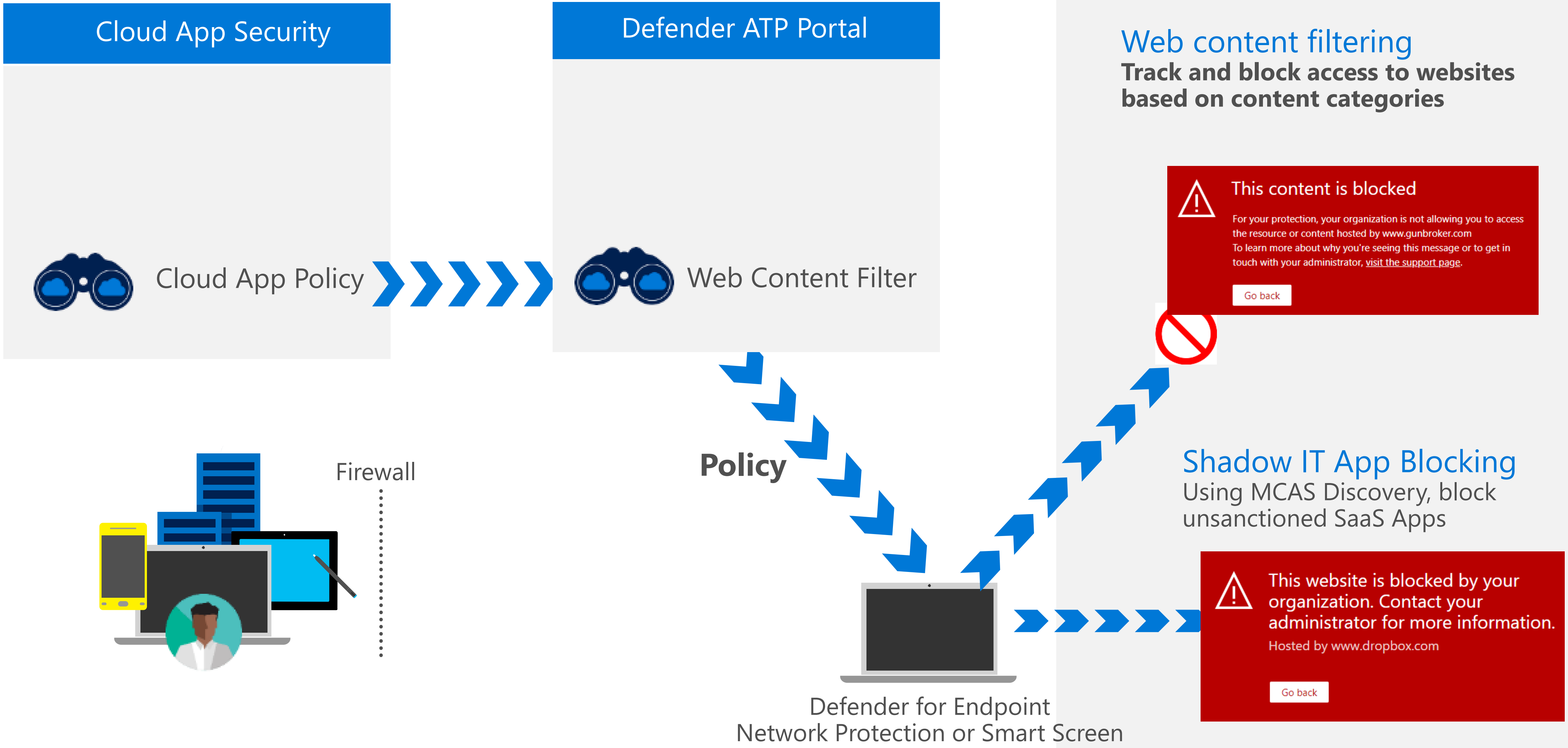
User	Total
James Lake	120 MB
Michael Spalding	118 MB
Daryl Snow	110 MB
Lorry Bloomberg	98 MB
Mike Maple	97 MB

Apps headquarters location All categories

TP

Did you know you had that much data being sent to Iran??

App and Web Content Blocking



Web content filtering

Track and block access to websites based on content categories

This content is blocked

For your protection, your organization is not allowing you to access the resource or content hosted by www.gunbroker.com

To learn more about why you're seeing this message or to get in touch with your administrator, visit the support page.

Shadow IT App Blocking

Using MCAS Discovery, block unsanctioned SaaS Apps

This website is blocked by your organization. Contact your administrator for more information.

Hosted by www.dropbox.com

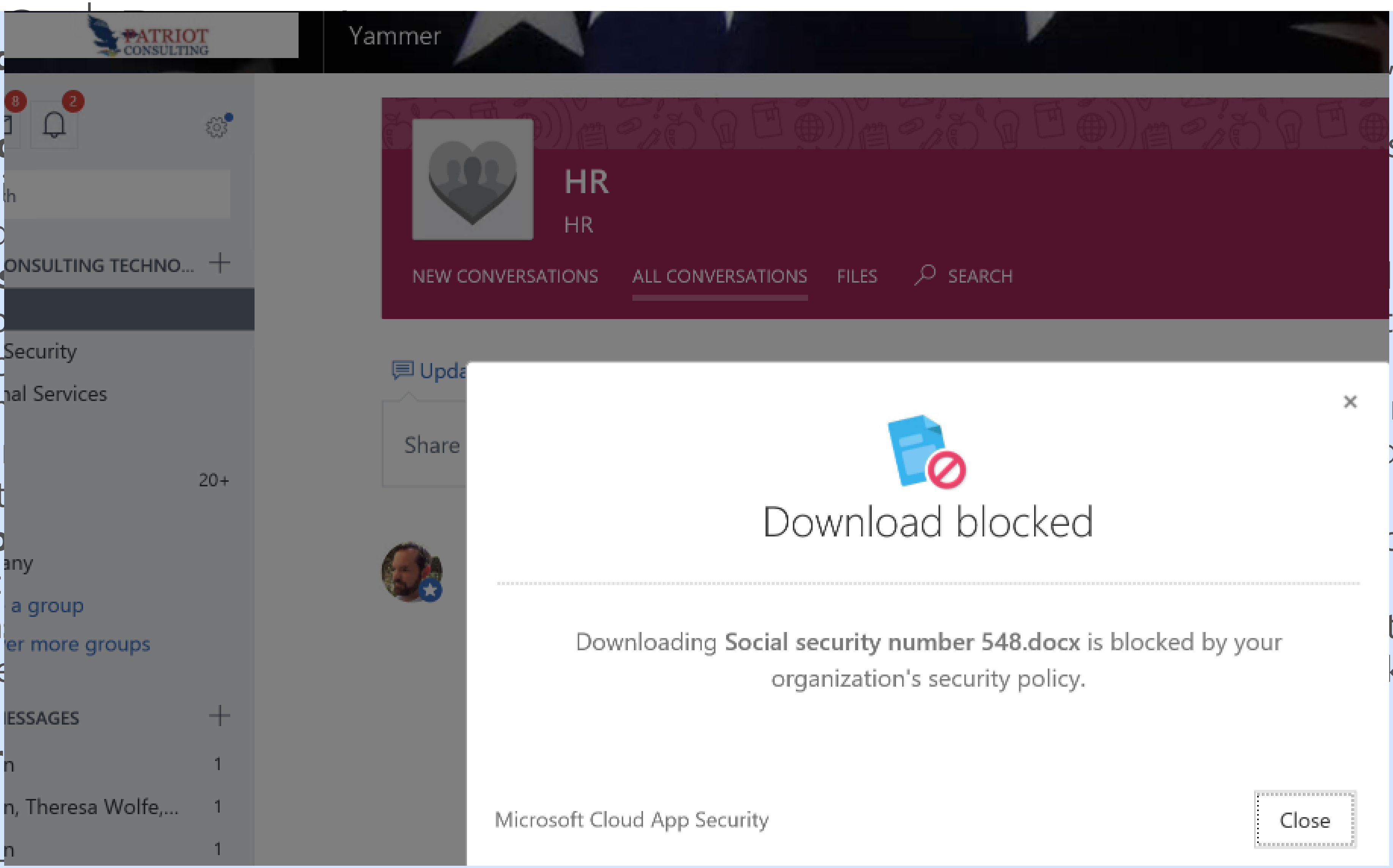
Supported firewalls and proxy servers

Palo Alto
Cisco ASA
Fortinet Fortigate

Barracuda - Web App Firewall (W3C)
Blue Coat Proxy SG - Access log (W3C)
Check Point
Cisco IronPort WSA
Cisco ScanSafe
Cisco Meraki – URLs log
Clavister NGFW (Syslog)
Dell Sonicwall

Juniper SRX
Juniper SSG
McAfee Secure Web Gateway
Microsoft Forefront Threat Management Gateway (W3C)
Sophos SG
Sophos Cyberoam
Squid (Common)
Squid (Native)
Websense Web Security Solutions - Investigative (CSV/CEF)
Zscaler

Block on upload or d , on
unmanaged devices.
Protect on downloa s to be
protected via encrypt
authenticated, if the c
Monitor low-trust u logged
from within the sessio
conditions, session po
Block access: You can r from
non-corporate netwo do not
have a client certificat
Create read-only mo ode to
specific apps for spec
Restrict user session t is not
part of your corporate ked or
protected.
Block Copy/Paste or
Block PII data (even



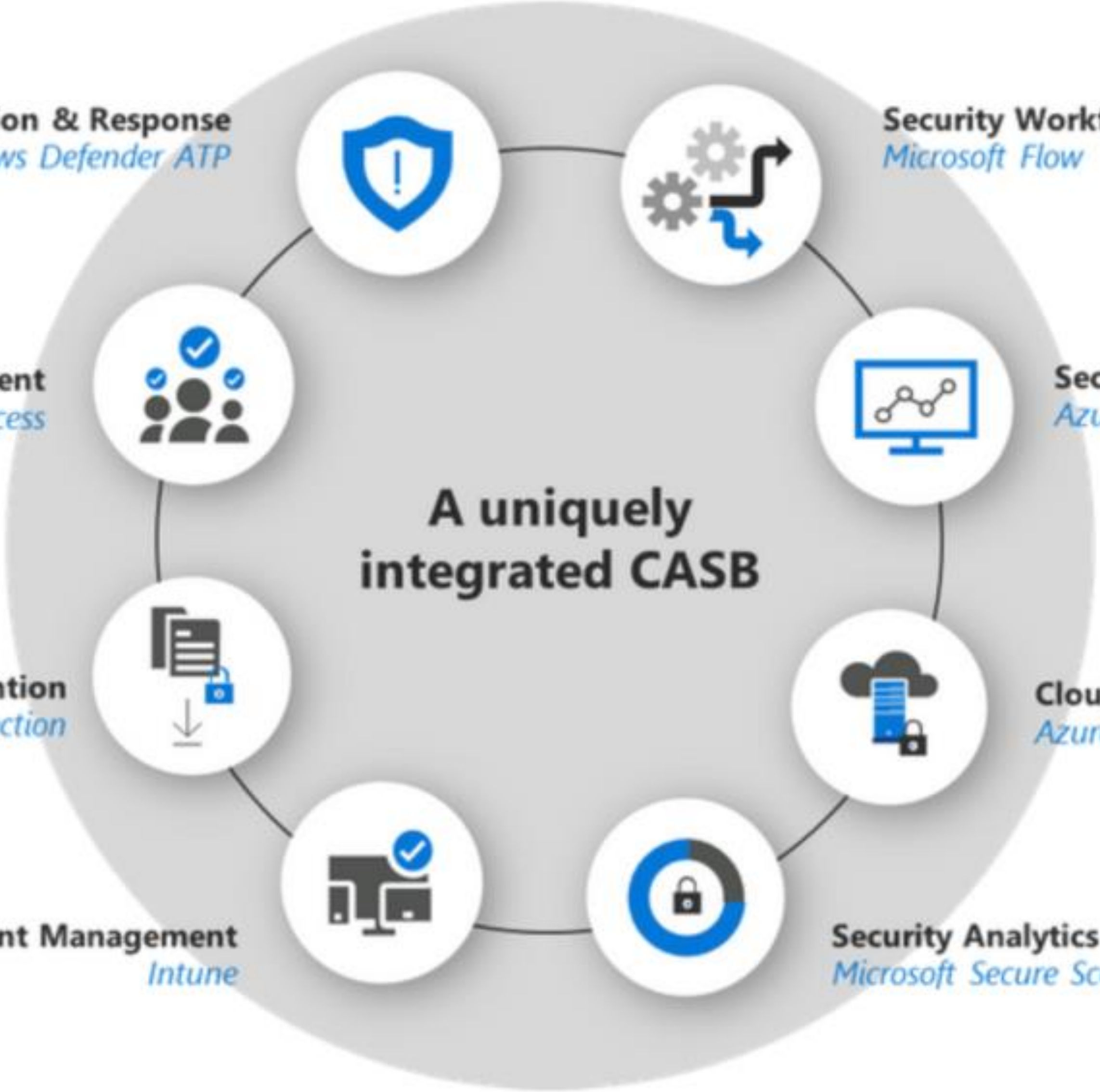
Download blocked

Downloading **Social security number 548.docx** is blocked by your organization's security policy.

Microsoft Cloud App Security

ALL SaaS apps are supported

CASB Integration with other MSFT Products



A uniquely integrated CASB

Endpoint Detection & Response
Windows Defender ATP

Security Workflow automation
Microsoft Flow

Identity & Access Management
Azure AD & Conditional Access

Security incident & event management (SIEM)
Azure Sentinel

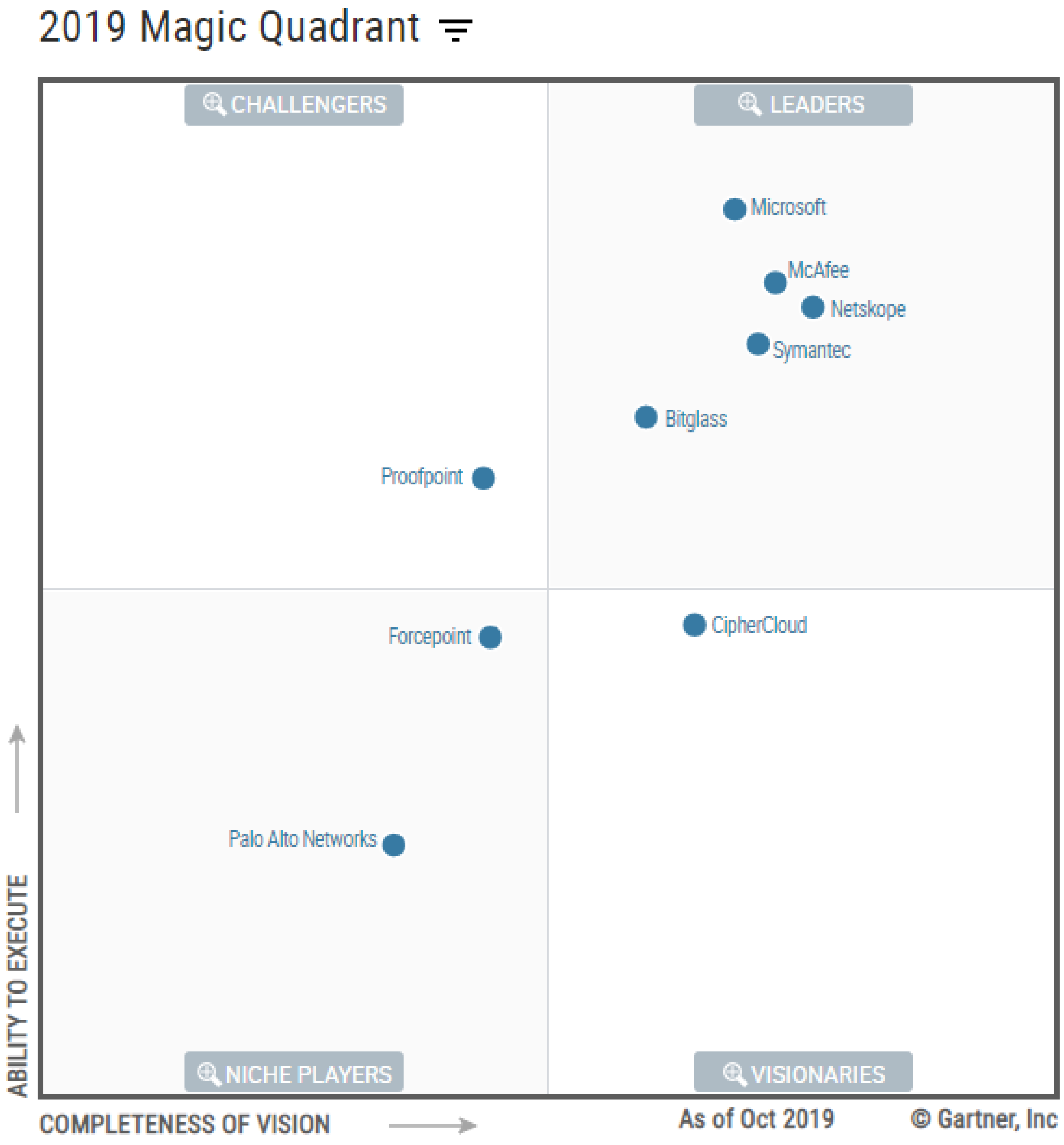
Data Loss Prevention
Azure Information Protection

Cloud Security Posture Management (IaaS)
Azure Security Center

Unified Endpoint Management
Intune

Security Analytics & Guidance
Microsoft Secure Score

Latest Gartner Magic Quadrant for CASB (Oct 2019)



Security Issue #7

Detecting Intrusions

200 days. That's the average time an attacker goes undetected.

There are two kinds of companies:
- Those that have been hacked…
- And those that don't know that they have been hacked!

Microsoft Cloud App Security

It's like an Intrusion Prevention System for Azure AD Identities

THREAT DETECTION

Identify high-risk and abnormal usage, security incidents, and threats

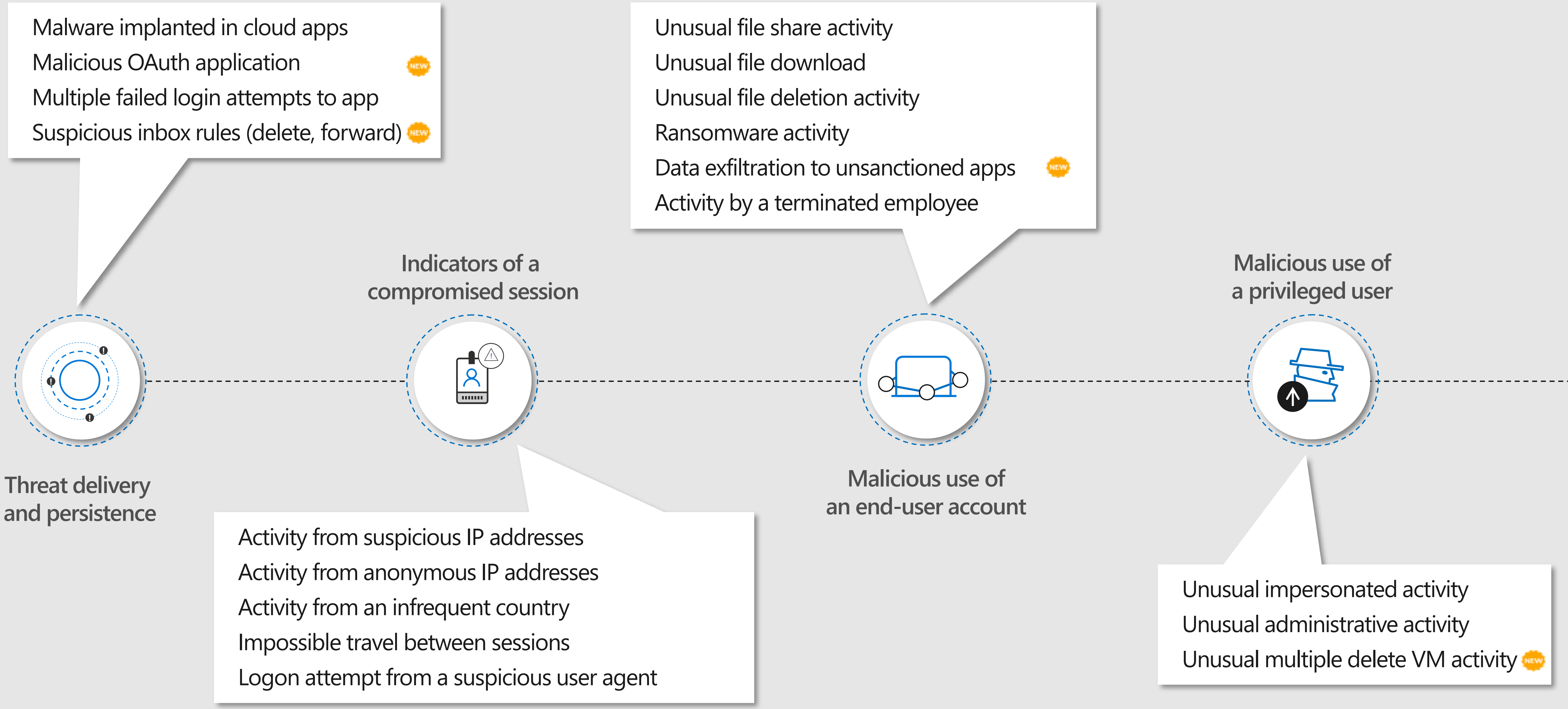
ENHANCED CONTROL

Shape your Office 365 environment with granular security controls and policies

DISCOVERY AND INSIGHTS

Gain enhanced visibility and context into your Office 365 usage and shadow IT – no agents required.

Microsoft Cloud App Security – Detections across apps



Threat delivery and persistence

- Malware implanted in cloud apps
- Malicious OAuth application NEW
- Multiple failed login attempts to app
- Suspicious inbox rules (delete, forward) NEW

Indicators of a compromised session

- Activity from suspicious IP addresses
- Activity from anonymous IP addresses
- Activity from an infrequent country
- Impossible travel between sessions
- Logon attempt from a suspicious user agent

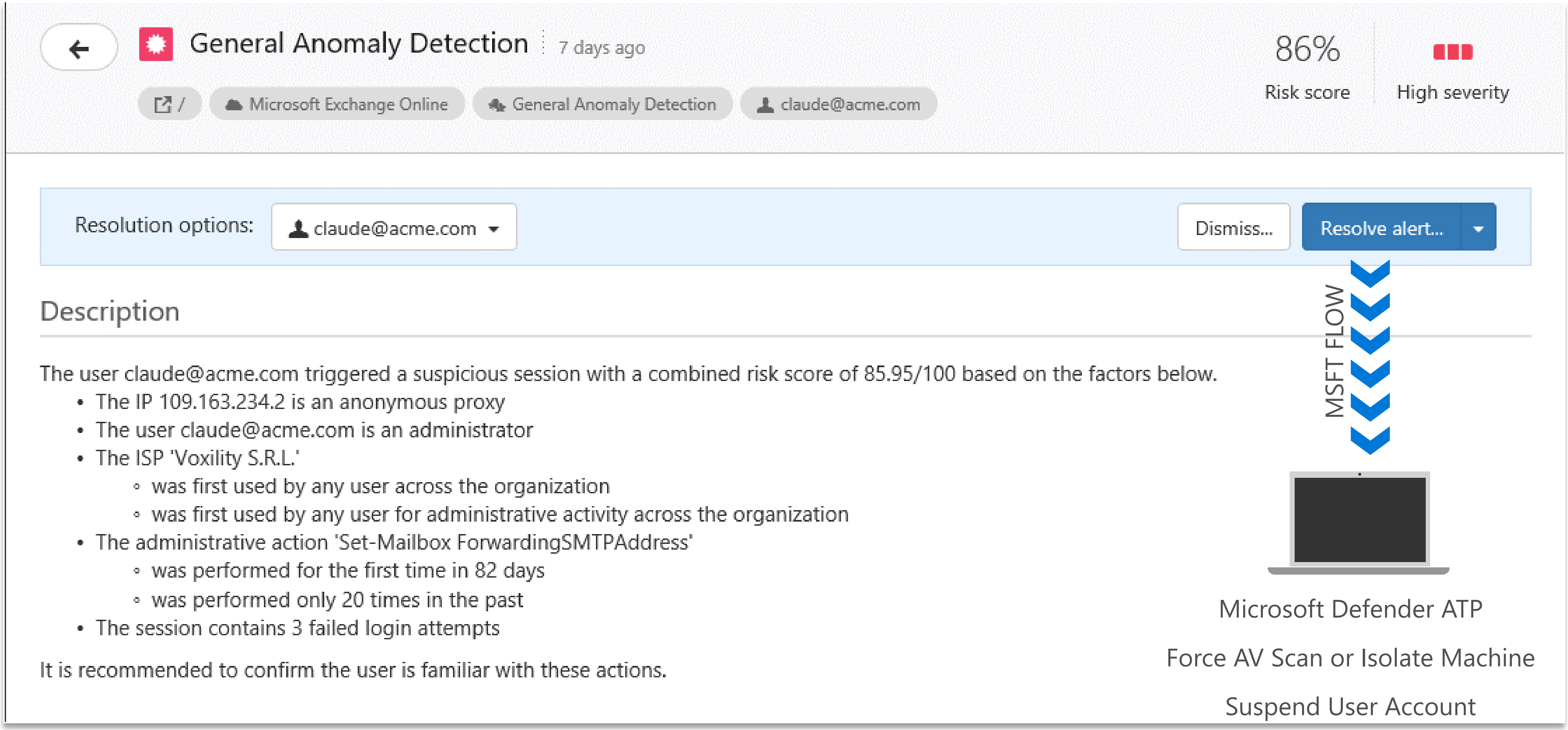
Malicious use of an end-user account

- Unusual file share activity
- Unusual file download
- Unusual file deletion activity
- Ransomware activity
- Data exfiltration to unsanctioned apps NEW
- Activity by a terminated employee

Malicious use of a privileged user

- Unusual impersonated activity
- Unusual administrative activity
- Unusual multiple delete VM activity NEW

Sample Anomaly Alert



Description

The user claude@acme.com triggered a suspicious session with a combined risk score of 85.95/100 based on the factors below.

- The IP 109.163.234.2 is an anonymous proxy
- The user claude@acme.com is an administrator
- The ISP 'Voxility S.R.L.'
  - was first used by any user across the organization
  - was first used by any user for administrative activity across the organization
- The administrative action 'Set-Mailbox ForwardingSMTPAddress'
  - was performed for the first time in 82 days
  - was performed only 20 times in the past
- The session contains 3 failed login attempts

It is recommended to confirm the user is familiar with these actions.

Microsoft Defender ATP

Force AV Scan or Isolate Machine

Suspend User Account

How do we detect breaches in on-premises Active Directory?

DETECT ATTACKS BEFORE THEY CAUSE DAMAGE

Defender for Identity

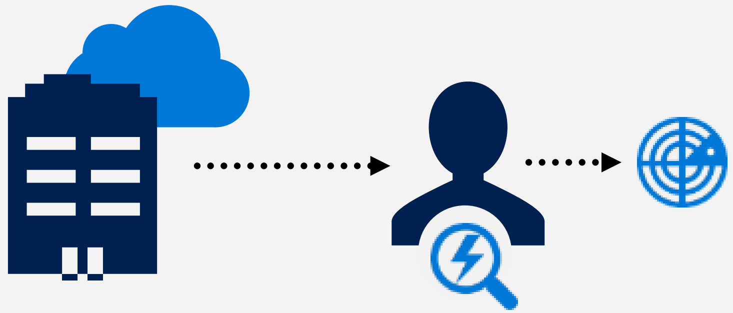
A behavioral and signature-based IDS agent for AD Domain Controllers

Behavioral Analytics

Detection of advanced attacks and security risks

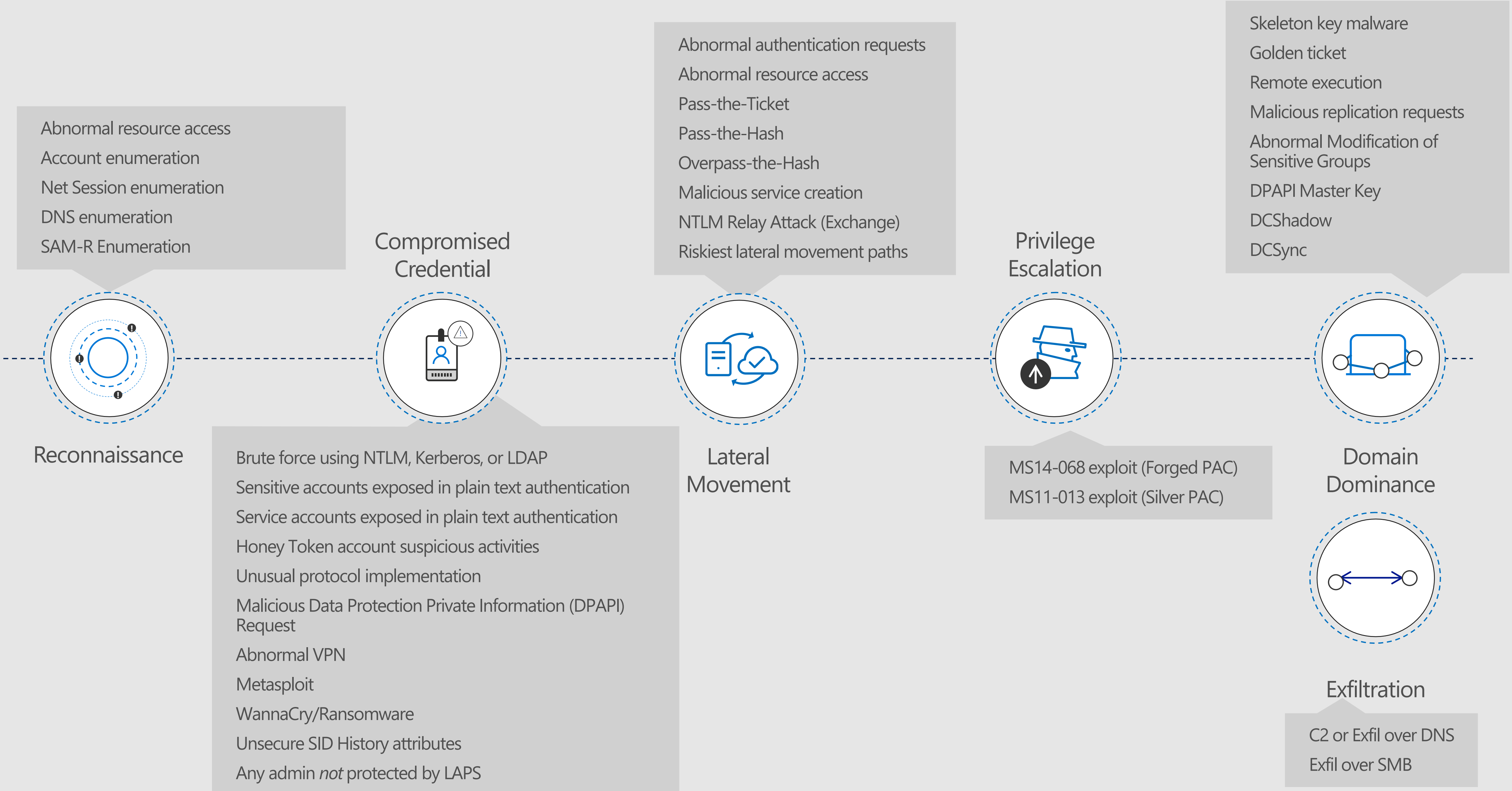
Advanced Threat Detection

No Server Infrastructure Required
Only a Lightweight Agent on DC's
All behavioral data is stored in Azure
Tight integration with MCAS & Defender for Endpoint



EMS E5

Detection Capabilities



Reconnaissance

- Abnormal resource access
- Account enumeration
- Net Session enumeration
- DNS enumeration
- SAM-R Enumeration

Compromised Credential

- Brute force using NTLM, Kerberos, or LDAP
- Sensitive accounts exposed in plain text authentication
- Service accounts exposed in plain text authentication
- Honey Token account suspicious activities
- Unusual protocol implementation
- Malicious Data Protection Private Information (DPAPI) Request
- Abnormal VPN
- Metasploit
- WannaCry/Ransomware
- Unsecure SID History attributes
- Any admin *not* protected by LAPS

Lateral Movement

- Abnormal authentication requests
- Abnormal resource access
- Pass-the-Ticket
- Pass-the-Hash
- Overpass-the-Hash
- Malicious service creation
- NTLM Relay Attack (Exchange)
- Riskiest lateral movement paths

Privilege Escalation

- MS14-068 exploit (Forged PAC)
- MS11-013 exploit (Silver PAC)

Domain Dominance

- Skeleton key malware
- Golden ticket
- Remote execution
- Malicious replication requests
- Abnormal Modification of Sensitive Groups
- DPAPI Master Key
- DCShadow
- DCSync

Exfiltration

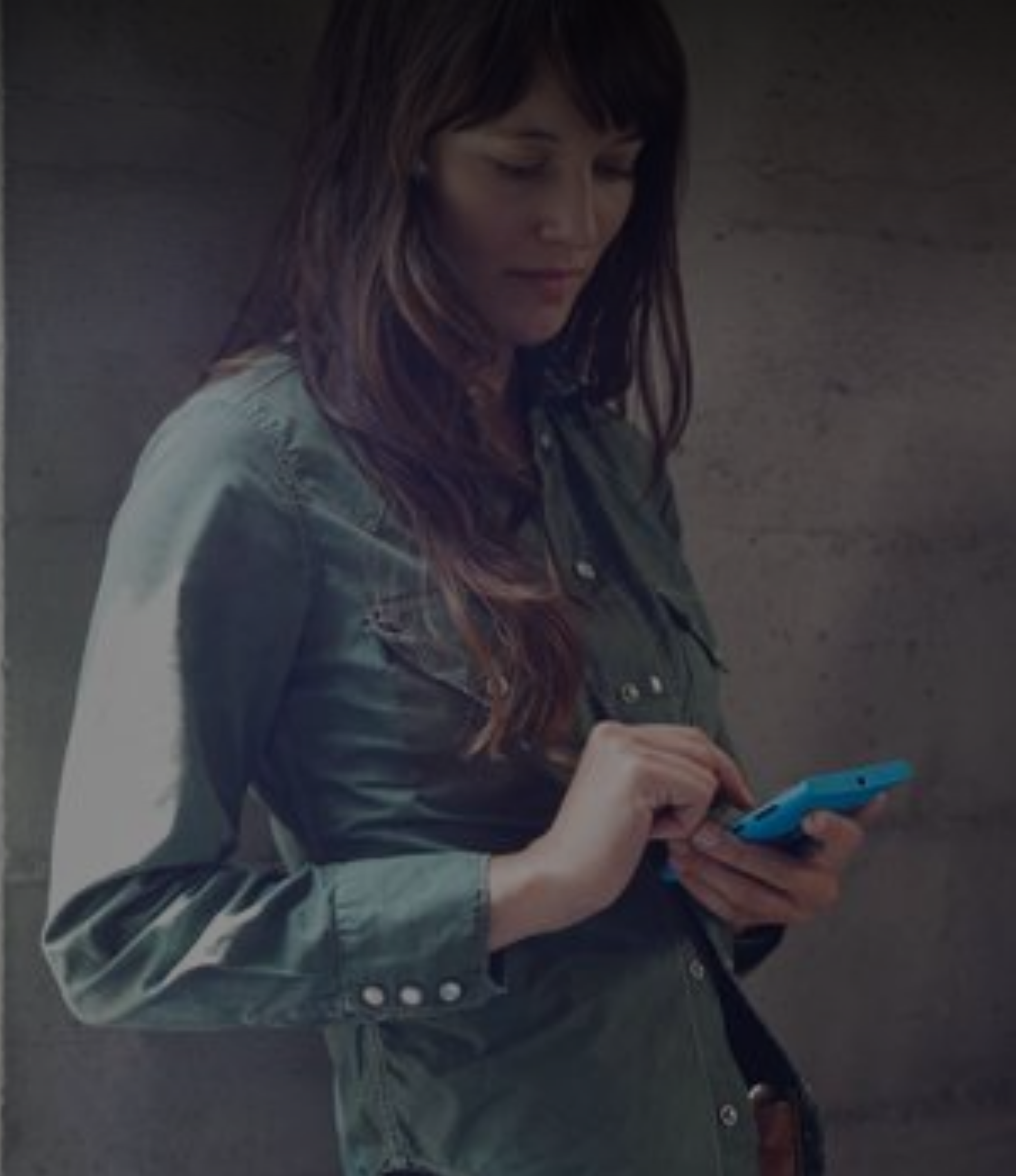
- C2 or Exfil over DNS
- Exfil over SMB

Security Issue #8

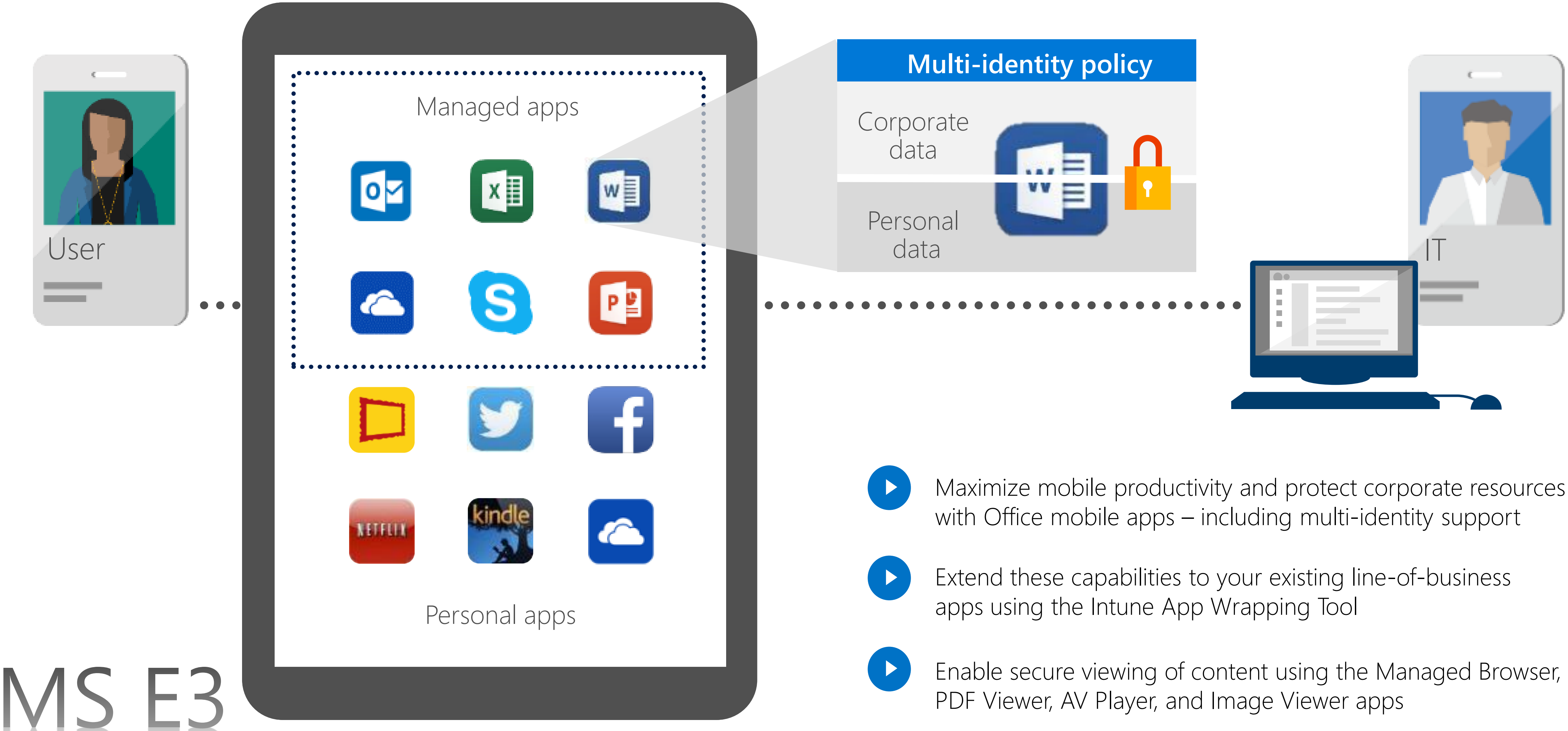
Employee Exits

BYOD use case:
How do I wipe business data from a personally owned mobile phone or tablet?

CYOD use case:
Do you allow personal apps on corporate phones?
How do you prevent leaks to those personal apps?



Intune App Protection (formerly 'MAM')



- Maximize mobile productivity and protect corporate resources with Office mobile apps – including multi-identity support
- Extend these capabilities to your existing line-of-business apps using the Intune App Wrapping Tool
- Enable secure viewing of content using the Managed Browser, PDF Viewer, AV Player, and Image Viewer apps

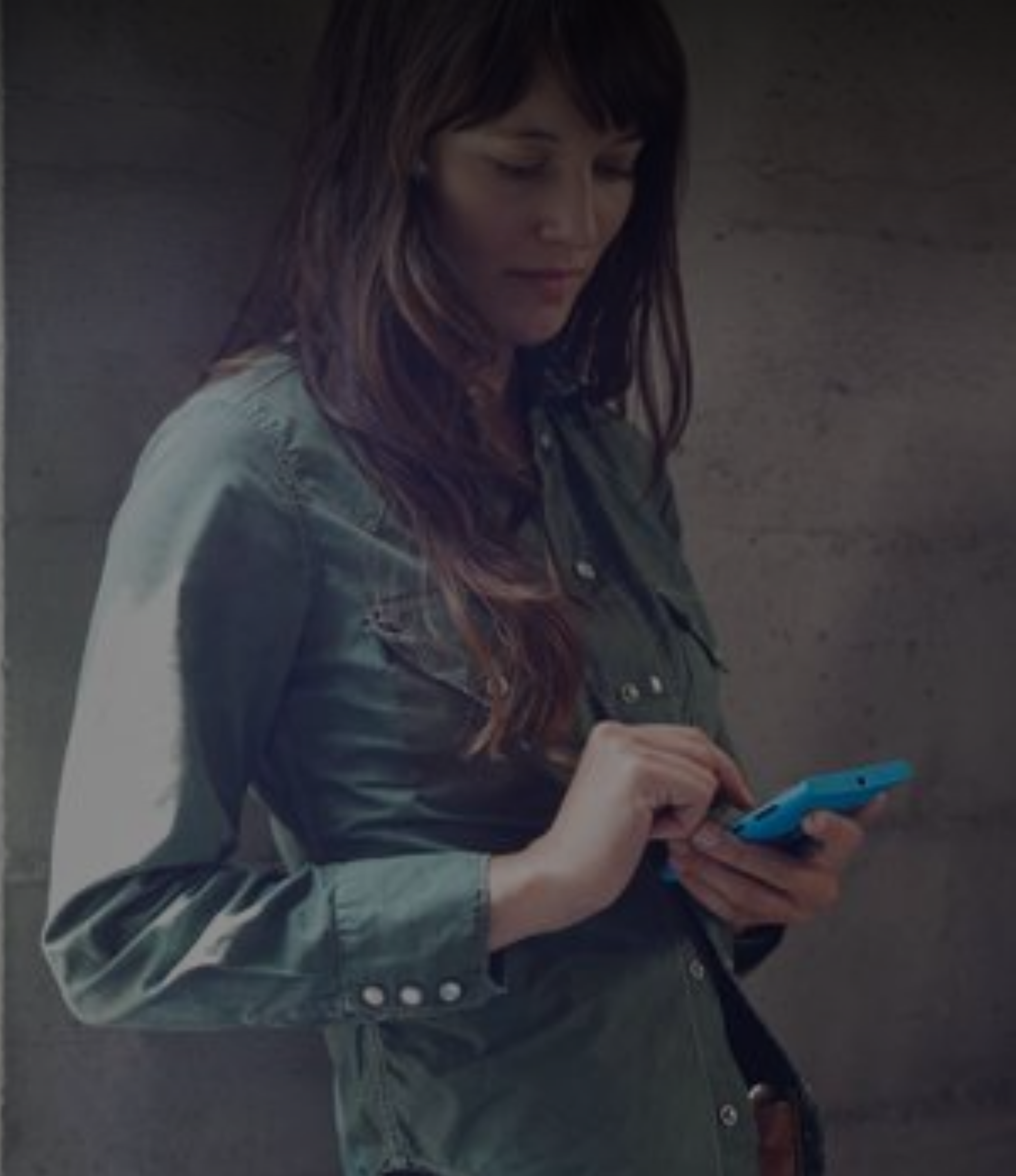
EMS E3

Security Issue #9

Advanced Persistent Threats (APT)

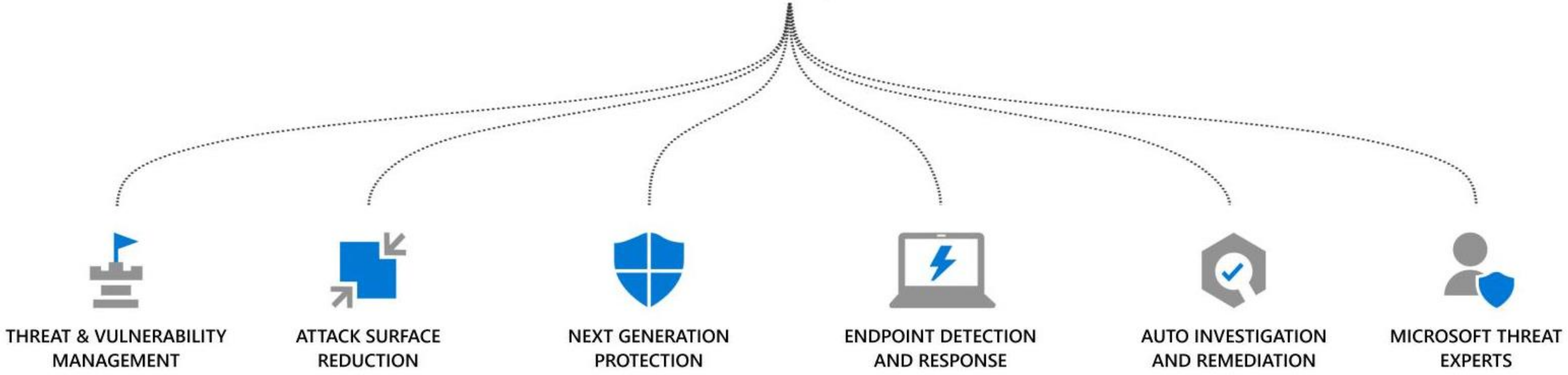
10% of viruses get by antivirus “blacklists’

Polymorphic worms eat up blacklists



Microsoft Defender for Endpoint

Built in. Cloud-powered.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

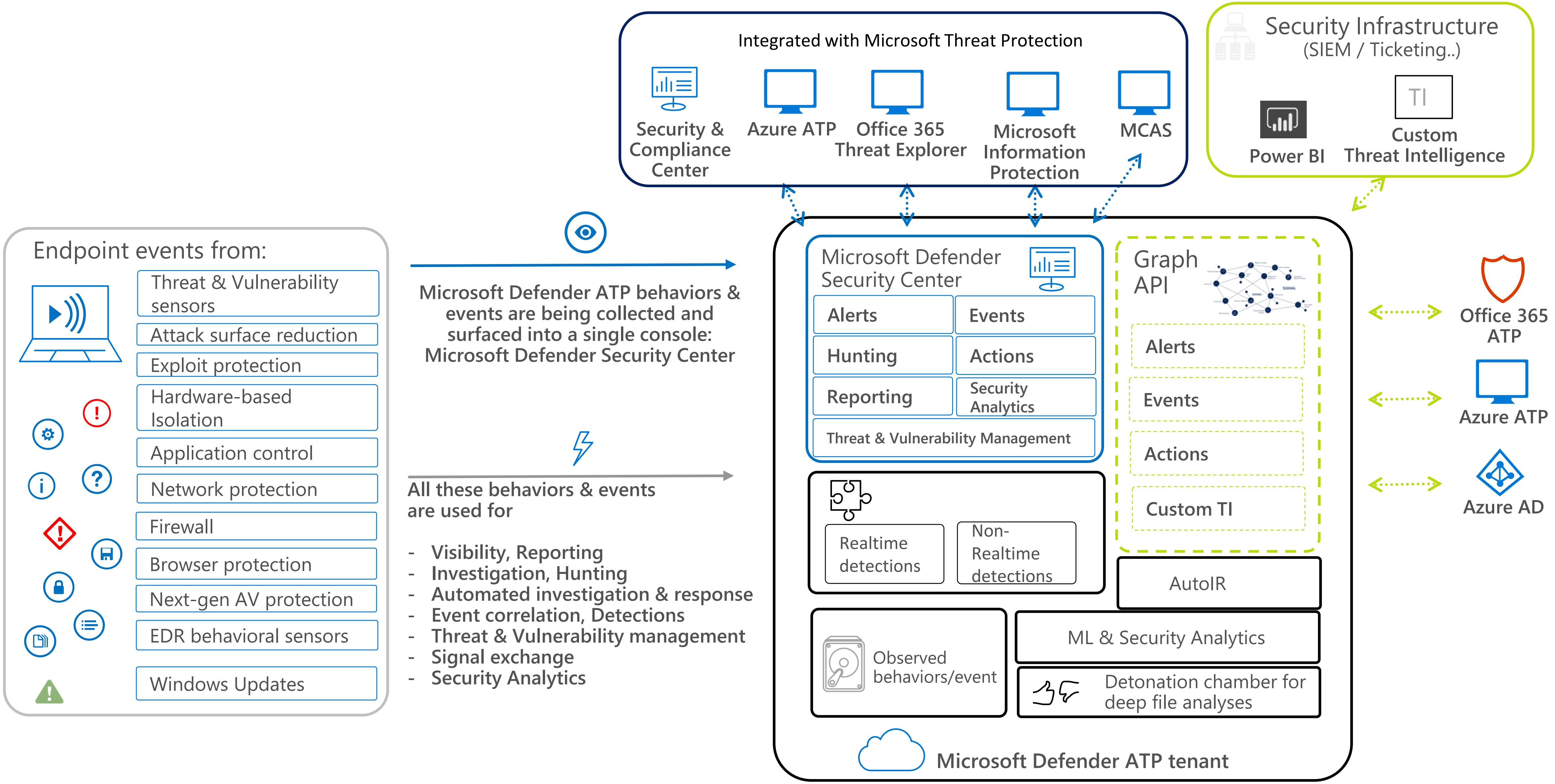
NEXT GENERATION PROTECTION

ENDPOINT DETECTION AND RESPONSE

AUTO INVESTIGATION AND REMEDIATION

MICROSOFT THREAT EXPERTS

Microsoft Defender for Endpoint Architecture



Endpoint events from:

- Threat & Vulnerability sensors
- Attack surface reduction
- Exploit protection
- Hardware-based Isolation
- Application control
- Network protection
- Firewall
- Browser protection
- Next-gen AV protection
- EDR behavioral sensors
- Windows Updates

Microsoft Defender ATP behaviors & events are being collected and surfaced into a single console: Microsoft Defender Security Center

All these behaviors & events are used for

- Visibility, Reporting
- Investigation, Hunting
- Automated investigation & response
- Event correlation, Detections
- Threat & Vulnerability management
- Signal exchange
- Security Analytics

Integrated with Microsoft Threat Protection

Security & Compliance Center

Azure ATP

Office 365 Threat Explorer

Microsoft Information Protection

MCAS

Security Infrastructure (SIEM / Ticketing..)

Power BI

Custom Threat Intelligence

Microsoft Defender Security Center

- Alerts
- Events
- Hunting
- Actions
- Reporting
- Security Analytics
- Threat & Vulnerability Management

Graph API

- Alerts
- Events
- Actions
- Custom TI

Realtime detections

Non-Realtime detections

AutoIR

Observed behaviors/event

ML & Security Analytics

Detonation chamber for deep file analyses

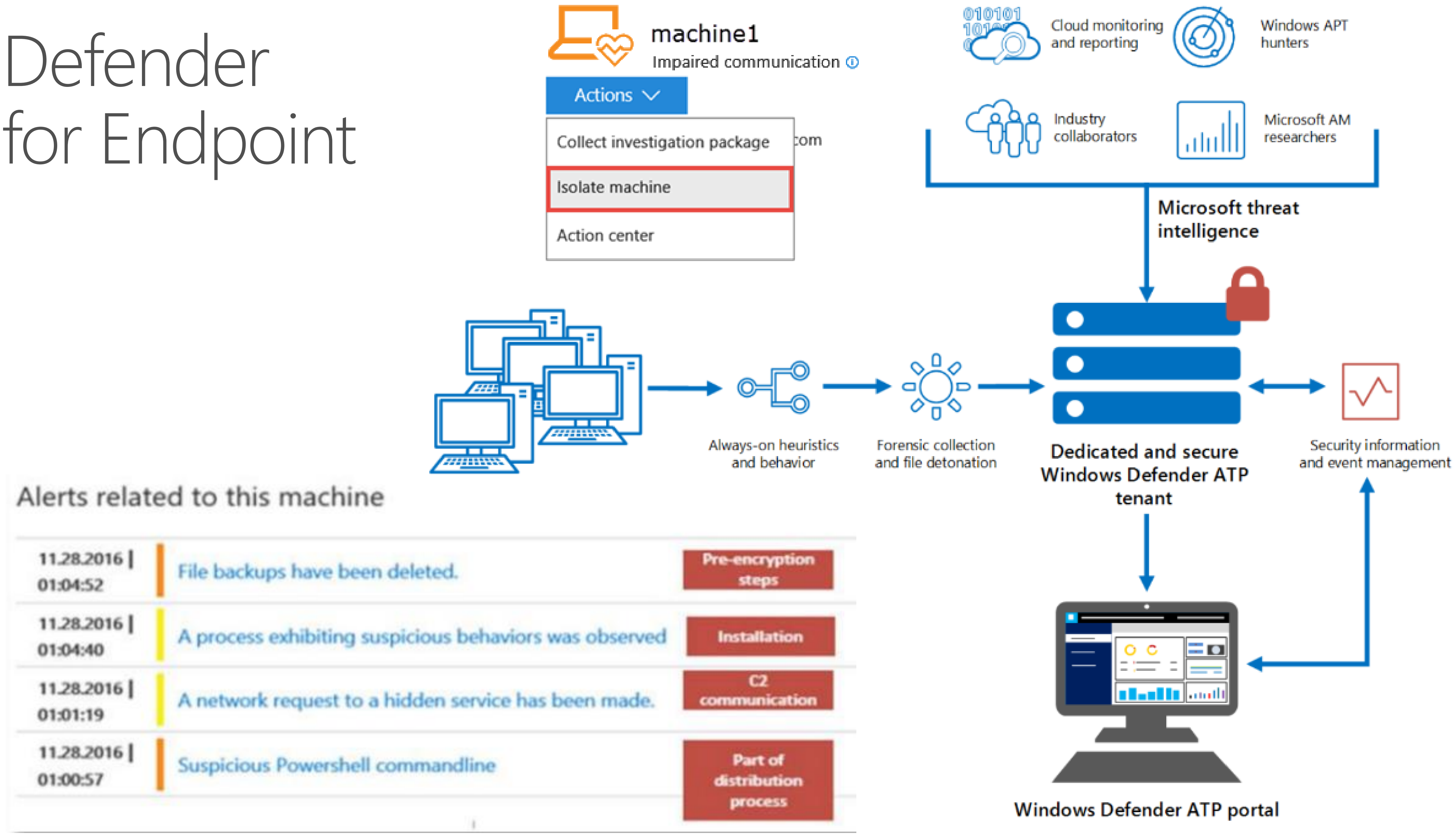
Microsoft Defender ATP tenant

Office 365 ATP

Azure ATP

Azure AD

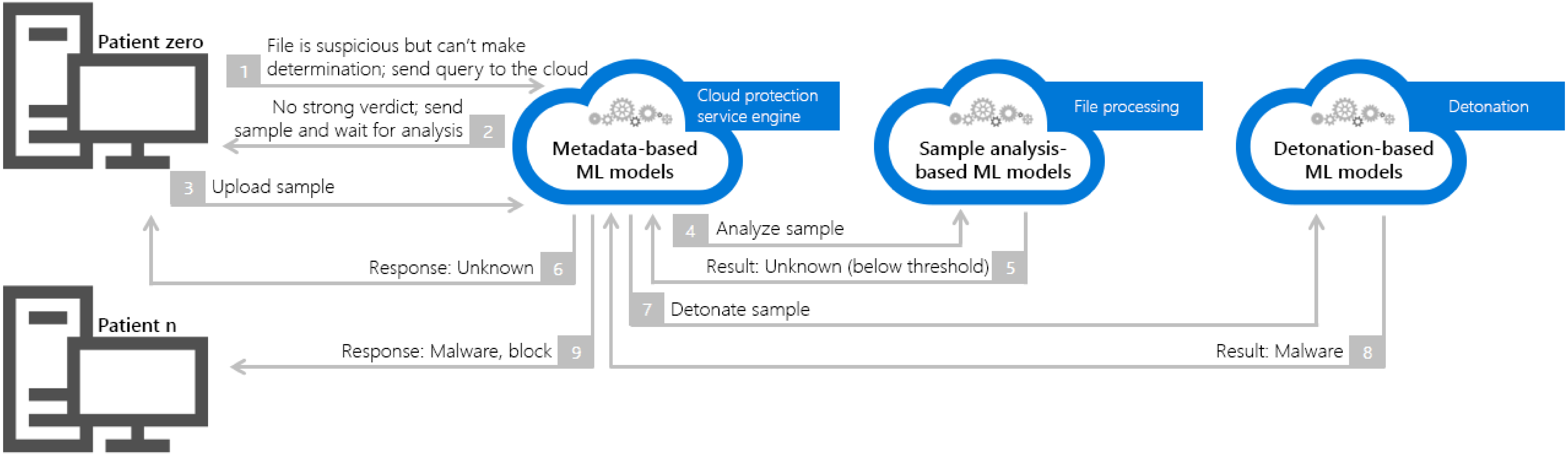
Defender for Endpoint


machine1
Impaired communication
Actions
Collect investigation package
Isolate machine
Action center
com
Cloud monitoring and reporting
Windows APT hunters
Industry collaborators
Microsoft AM researchers
Microsoft threat intelligence
Always-on heuristics and behavior
Forensic collection and file detonation
Dedicated and secure Windows Defender ATP tenant
Security information and event management
Windows Defender ATP portal

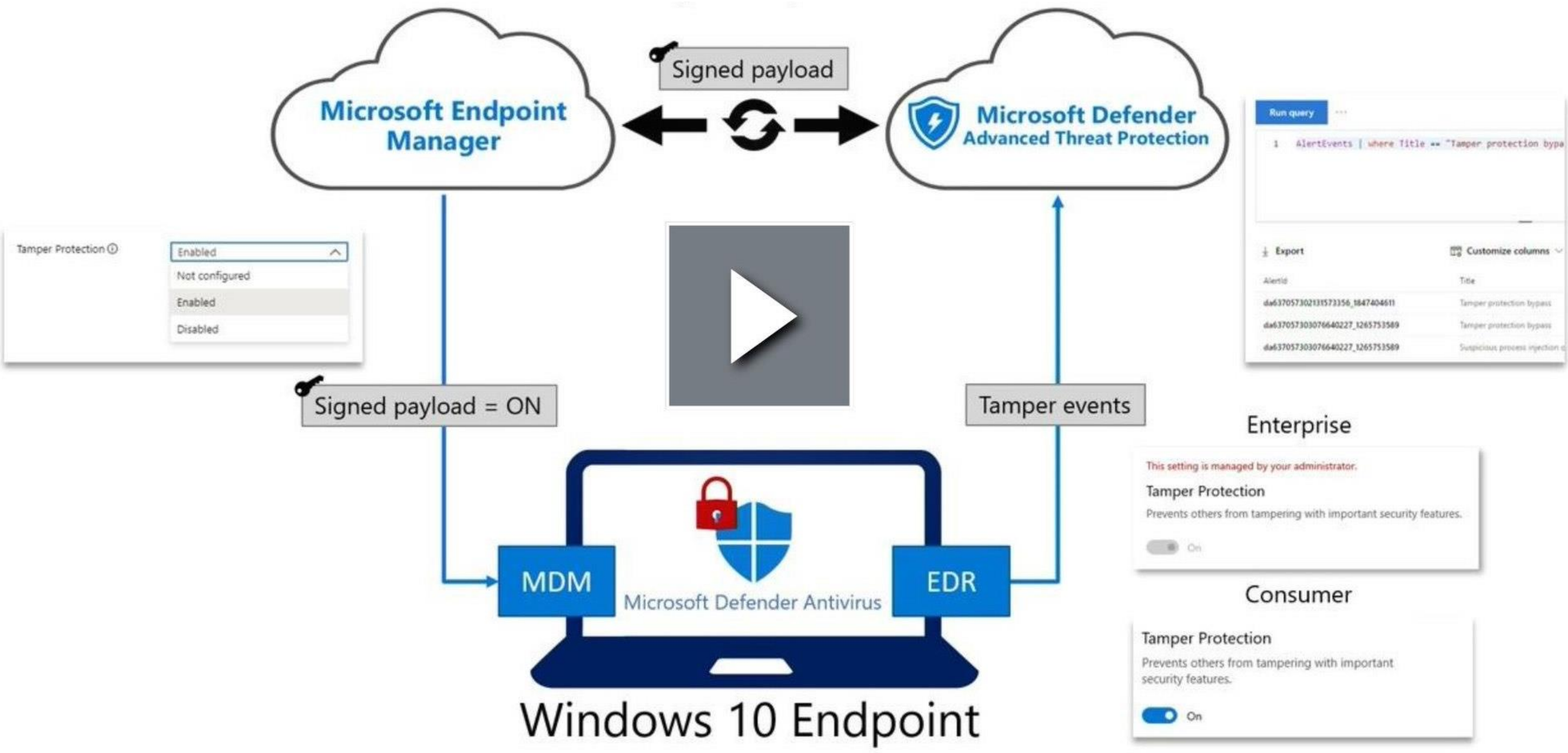
Alerts related to this machine

11.28.2016 | 01:04:52	File backups have been deleted.	Pre-encryption steps
11.28.2016 | 01:04:40	A process exhibiting suspicious behaviors was observed	Installation
11.28.2016 | 01:01:19	A network request to a hidden service has been made.	C2 communication
11.28.2016 | 01:00:57	Suspicious Powershell commandline	Part of distribution process

Machine Learning & Block at First Site


Patient zero
1 File is suspicious but can't make determination; send query to the cloud
No strong verdict; send sample and wait for analysis 2
3 Upload sample
Cloud protection service engine
Metadata-based ML models
File processing
Sample analysis-based ML models
Detonation
Detonation-based ML models
4 Analyze sample
Result: Unknown (below threshold) 5
Response: Unknown 6
7 Detonate sample
Patient n
Response: Malware, block 9
Result: Malware 8

Tamper Protection prevents malware or even local administrators from disabling Antivirus



Microsoft Endpoint Manager

Signed payload

Microsoft Defender Advanced Threat Protection

Tamper Protection ⓘ

Enabled

Not configured

Enabled

Disabled

Signed payload = ON

Tamper events

MDM

Microsoft Defender Antivirus

EDR

Windows 10 Endpoint

Run query ···

```
AlertEvents | where Title == "Tamper protection bypa
```

Export

Customize columns

AlertId	Title
da637057302131573356_1847404611	Tamper protection bypass
da637057303076640227_1265753589	Tamper protection bypass
da637057303076640227_1265753589	Suspicious process injection o

Enterprise

This setting is managed by your administrator.

Tamper Protection

Prevents others from tampering with important security features.

On

Consumer

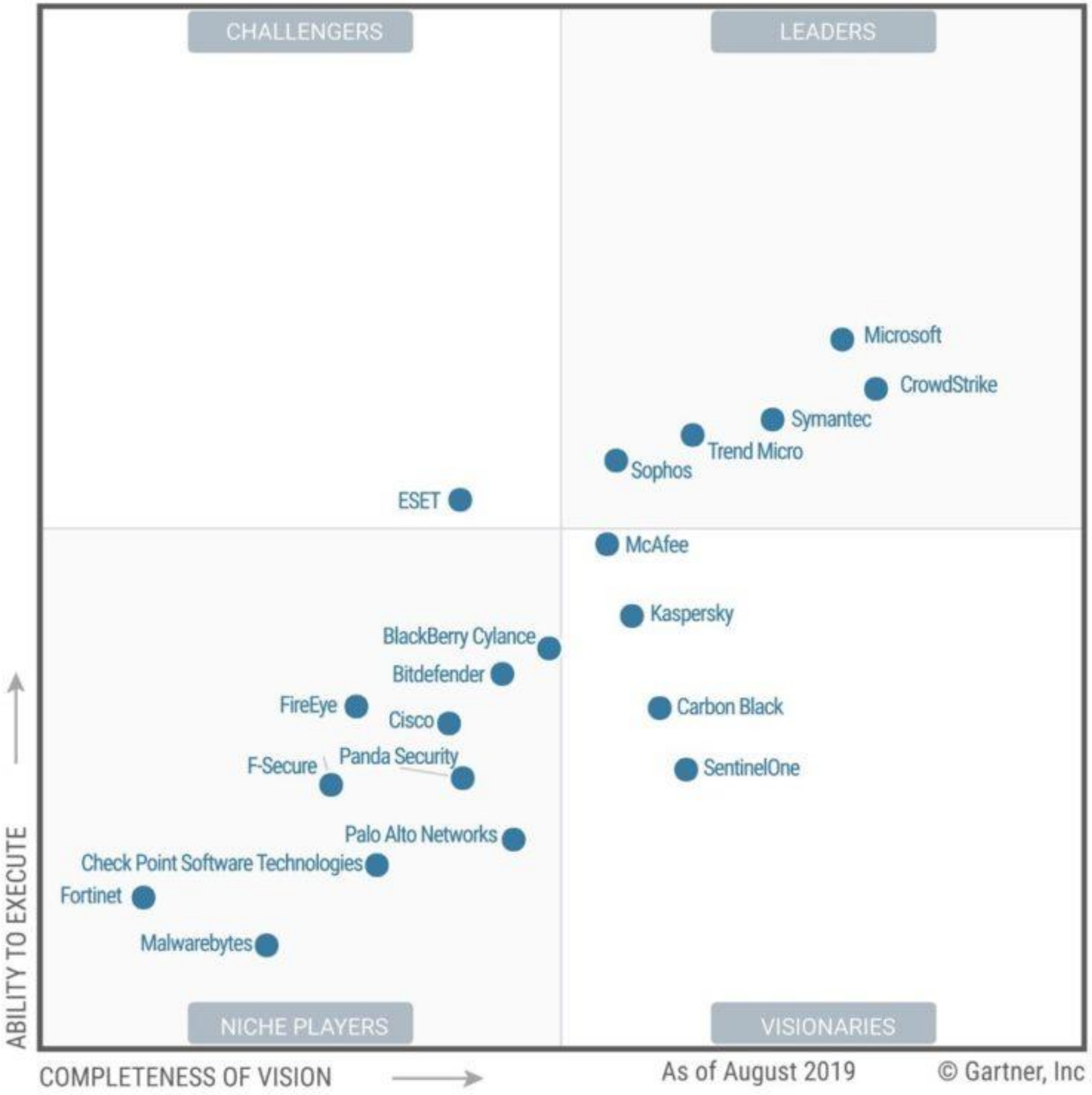
Tamper Protection

Prevents others from tampering with important security features.

On

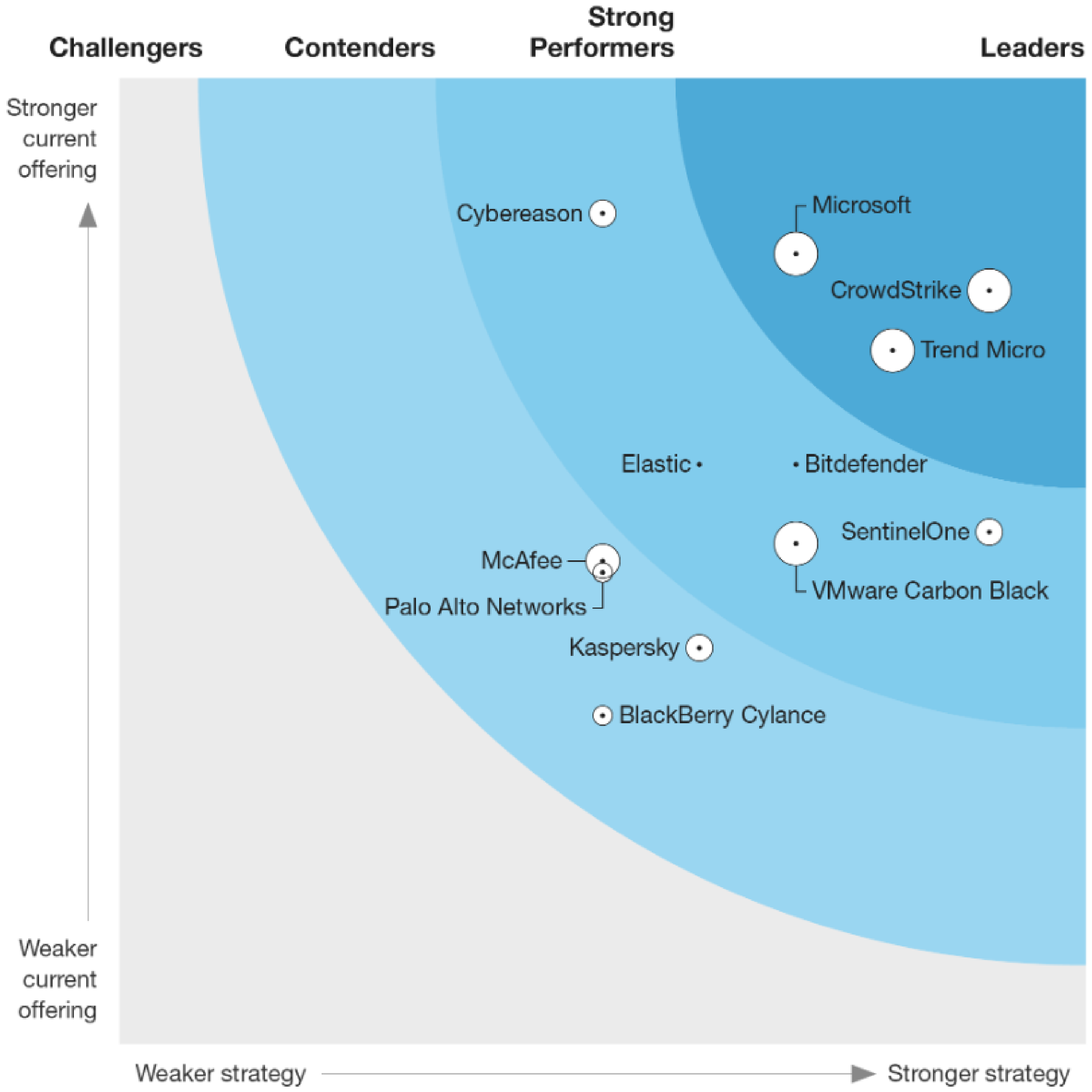
Latest Gartner Magic Quadrant for Endpoint Protection

Figure 1. Magic Quadrant for Endpoint Protection Platforms



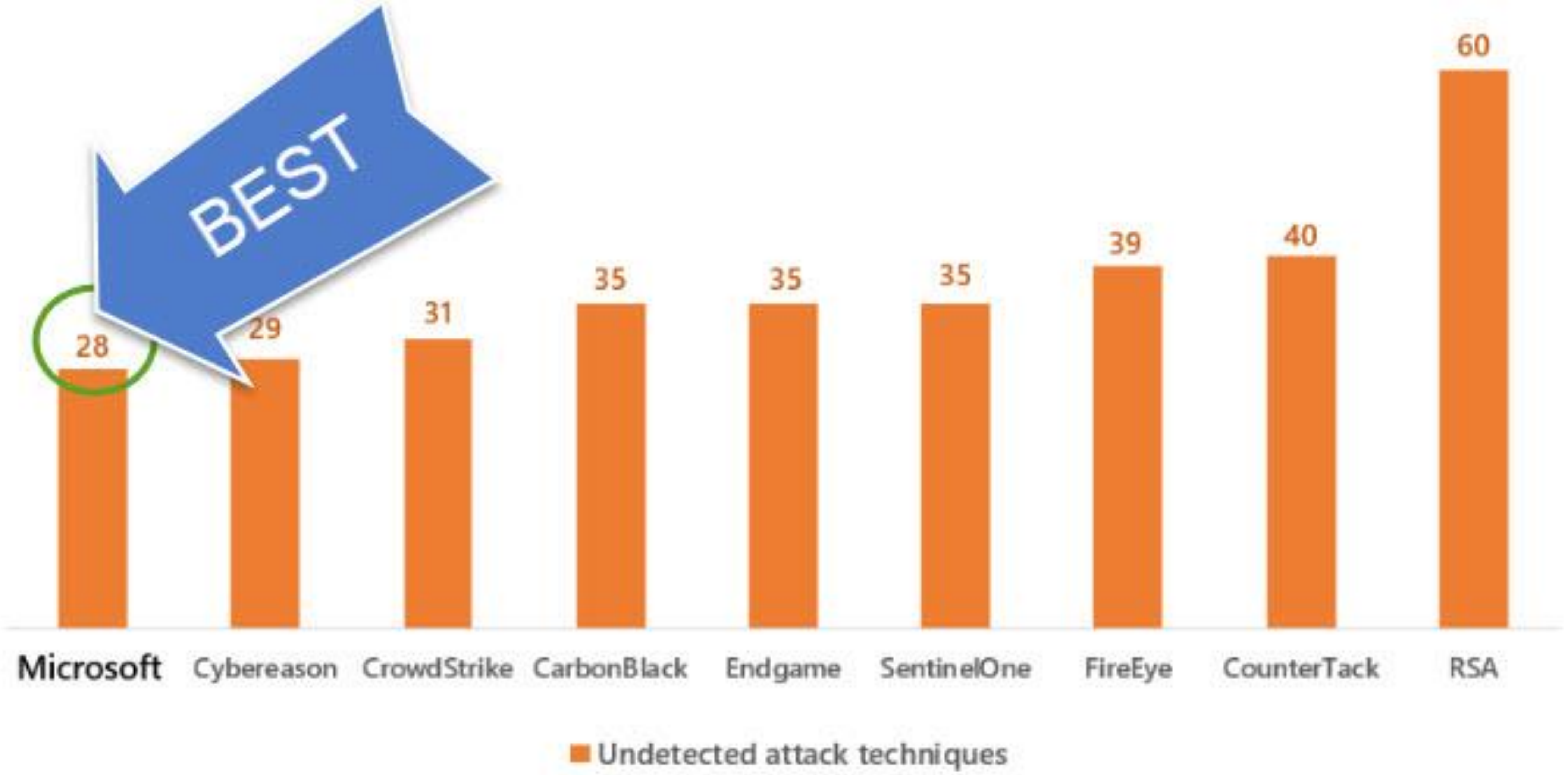
Source: Gartner (August 2019)

Latest Forrester Endpoint Security (Q1 2020)



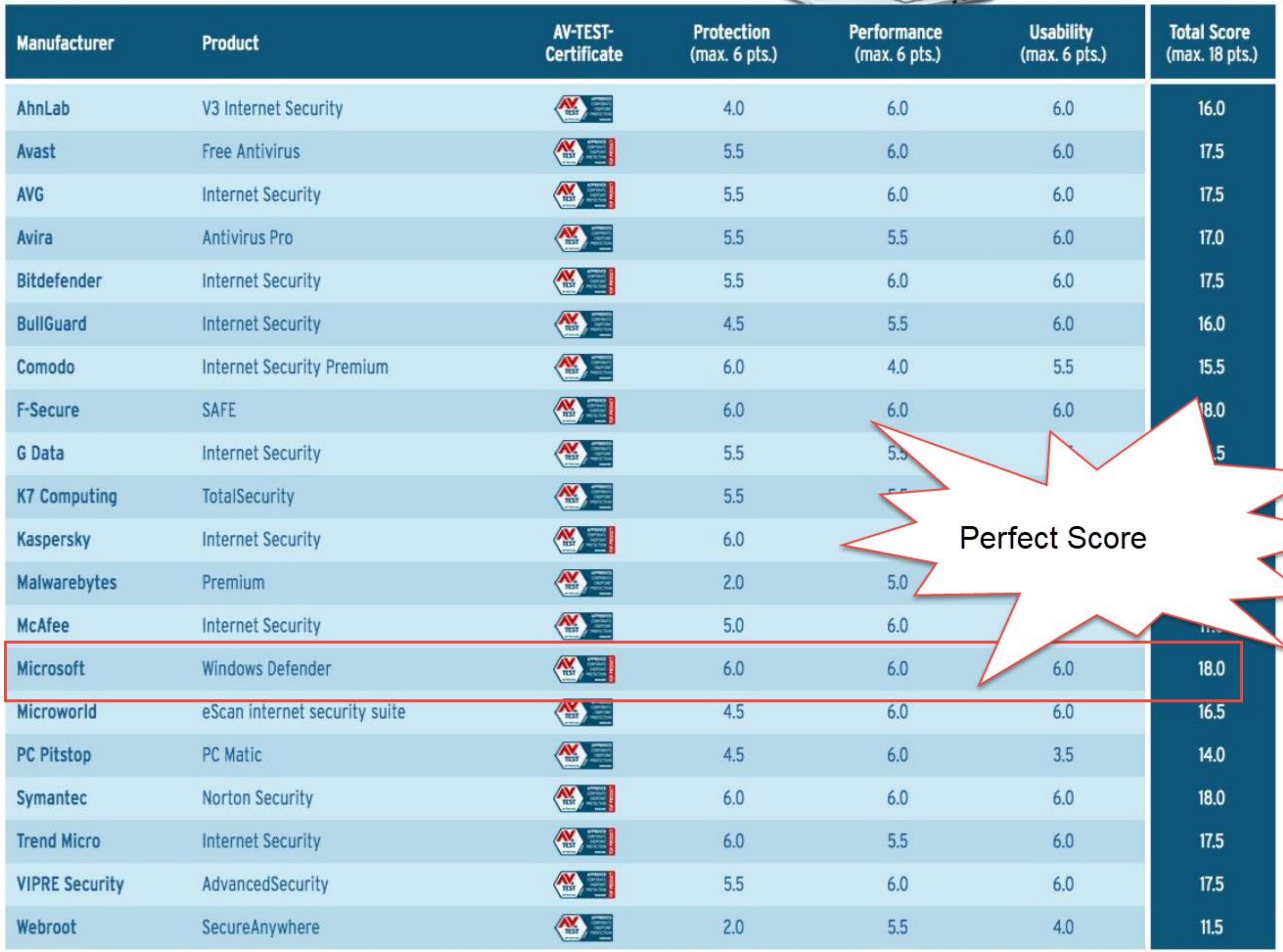
How does it compare to others?

Windows Defender ATP had the fewest number of misses (i.e., undetected red team activity) among all solutions evaluated.

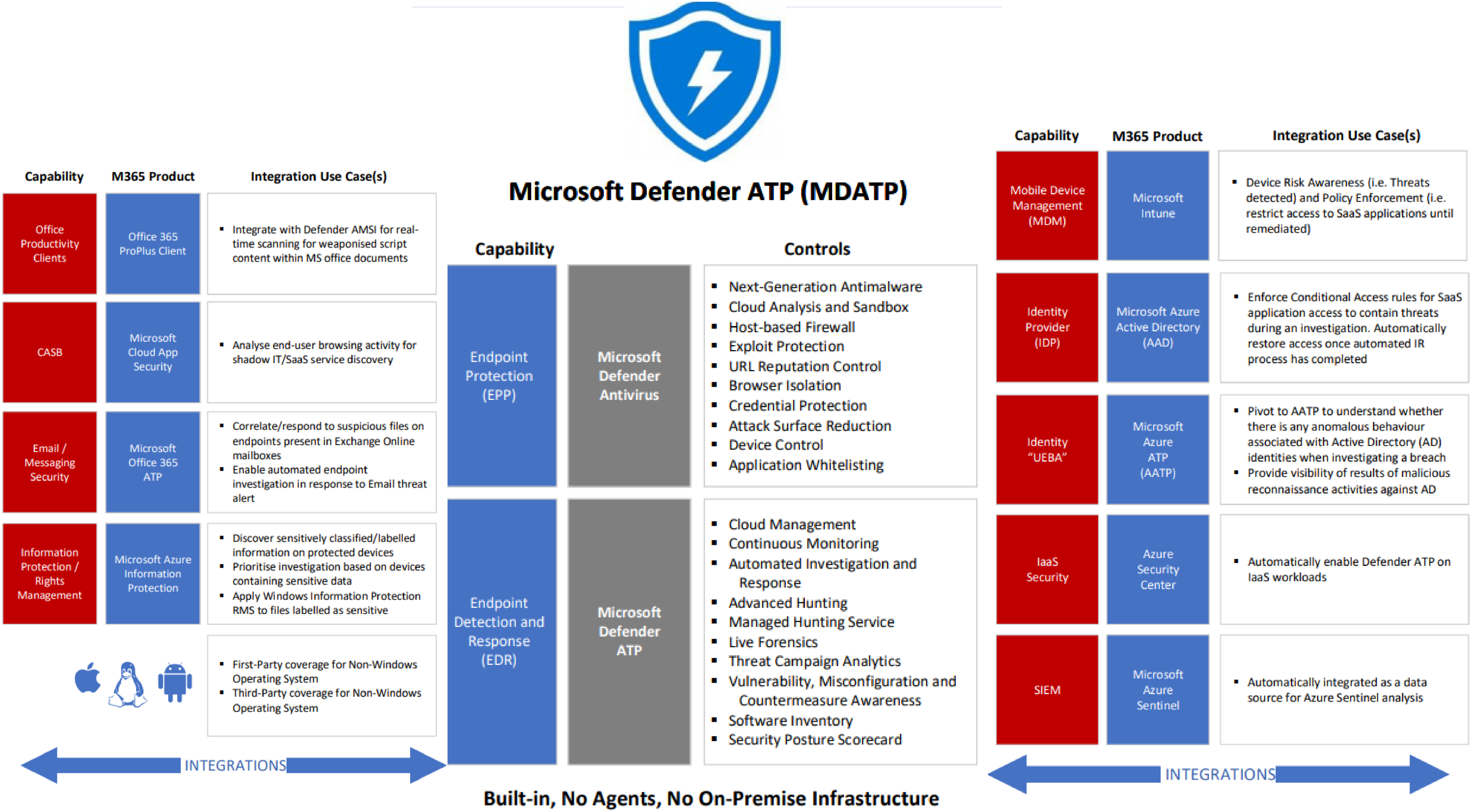


AVTEST Gives Defender for endpoint Perfect Scores (190 Malware Samples)

HOME USER WINDOWS



Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Total Score (max. 18 pts.)
AhnLab	V3 Internet Security		4.0	6.0	6.0	16.0
Avast	Free Antivirus		5.5	6.0	6.0	17.5
AVG	Internet Security		5.5	6.0	6.0	17.5
Avira	Antivirus Pro		5.5	5.5	6.0	17.0
Bitdefender	Internet Security		5.5	6.0	6.0	17.5
BullGuard	Internet Security		4.5	5.5	6.0	16.0
Comodo	Internet Security Premium		6.0	4.0	5.5	15.5
F-Secure	SAFE		6.0	6.0	6.0	18.0
G Data	Internet Security		5.5	5.5		[illegible]
K7 Computing	TotalSecurity		5.5	[illegible]		
Kaspersky	Internet Security		6.0			
Malwarebytes	Premium		2.0	5.0		
McAfee	Internet Security		5.0	6.0		[illegible]
Microsoft	Windows Defender		6.0	6.0	6.0	18.0
Microworld	eScan internet security suite		4.5	6.0	6.0	16.5
PC Pitstop	PC Matic		4.5	6.0	3.5	14.0
Symantec	Norton Security		6.0	6.0	6.0	18.0
Trend Micro	Internet Security		6.0	5.5	6.0	17.5
VIPRE Security	AdvancedSecurity		5.5	6.0	6.0	17.5
Webroot	SecureAnywhere		2.0	5.5	4.0	11.5



Microsoft Defender ATP (MDATP)

Capability	M365 Product	Integration Use Case(s)
Office Productivity Clients	Office 365 ProPlus Client	▪ Integrate with Defender AMSI for real-time scanning for weaponised script content within MS office documents
CASB	Microsoft Cloud App Security	▪ Analyse end-user browsing activity for shadow IT/SaaS service discovery
Email / Messaging Security	Microsoft Office 365 ATP	▪ Correlate/respond to suspicious files on endpoints present in Exchange Online mailboxes ▪ Enable automated endpoint investigation in response to Email threat alert
Information Protection / Rights Management	Microsoft Azure Information Protection	▪ Discover sensitively classified/labelled information on protected devices ▪ Prioritise investigation based on devices containing sensitive data ▪ Apply Windows Information Protection RMS to files labelled as sensitive
🍎 🐧 🤖		▪ First-Party coverage for Non-Windows Operating System ▪ Third-Party coverage for Non-Windows Operating System

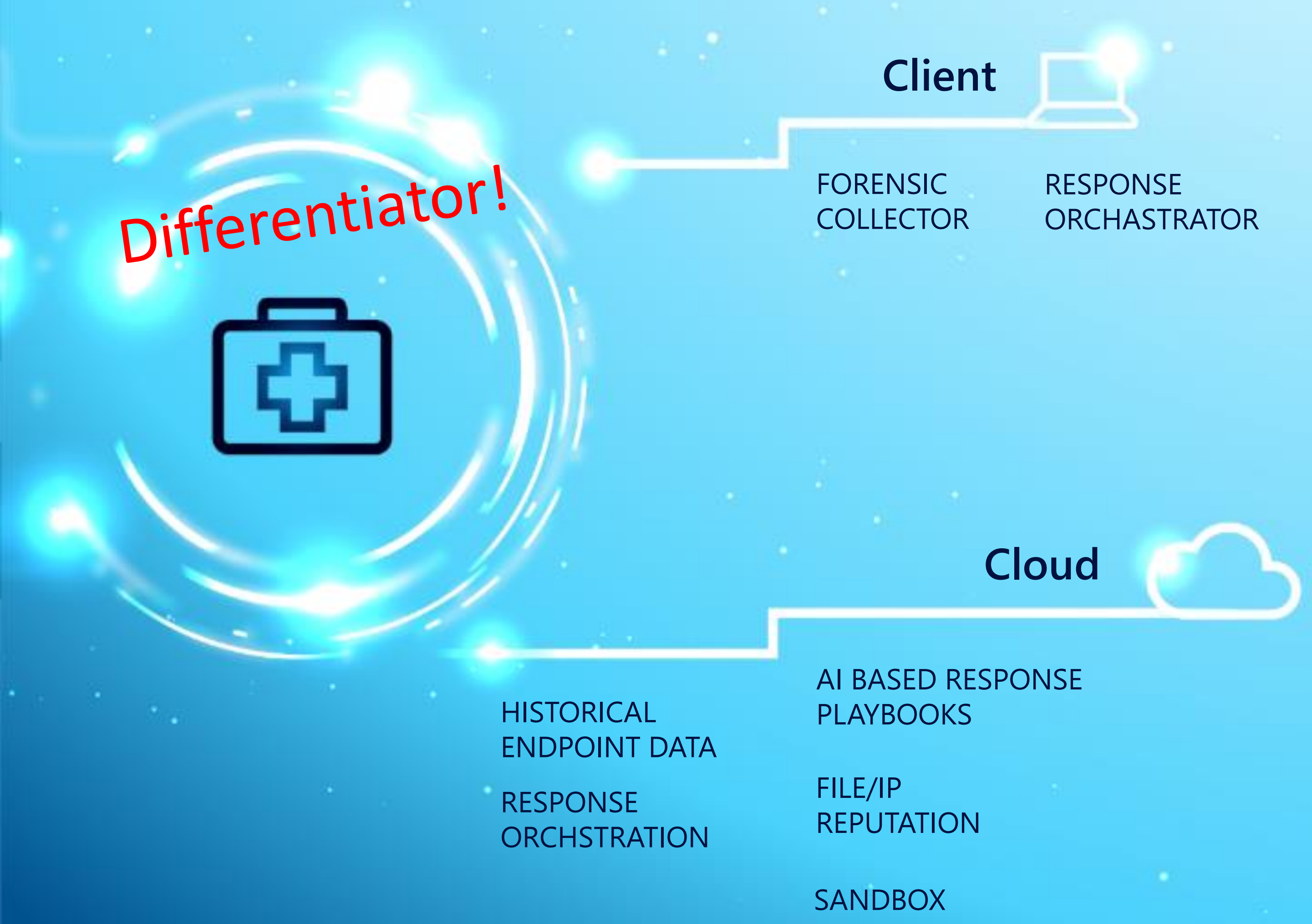
Capability		Controls
Endpoint Protection (EPP)	Microsoft Defender Antivirus	▪ Next-Generation Antimalware ▪ Cloud Analysis and Sandbox ▪ Host-based Firewall ▪ Exploit Protection ▪ URL Reputation Control ▪ Browser Isolation ▪ Credential Protection ▪ Attack Surface Reduction ▪ Device Control ▪ Application Whitelisting
Endpoint Detection and Response (EDR)	Microsoft Defender ATP	▪ Cloud Management ▪ Continuous Monitoring ▪ Automated Investigation and Response ▪ Advanced Hunting ▪ Managed Hunting Service ▪ Live Forensics ▪ Threat Campaign Analytics ▪ Vulnerability, Misconfiguration and Countermeasure Awareness ▪ Software Inventory ▪ Security Posture Scorecard

Capability	M365 Product	Integration Use Case(s)
Mobile Device Management (MDM)	Microsoft Intune	▪ Device Risk Awareness (i.e. Threats detected) and Policy Enforcement (i.e. restrict access to SaaS applications until remediated)
Identity Provider (IDP)	Microsoft Azure Active Directory (AAD)	▪ Enforce Conditional Access rules for SaaS application access to contain threats during an investigation. Automatically restore access once automated IR process has completed
Identity "UEBA"	Microsoft Azure ATP (AATP)	▪ Pivot to AATP to understand whether there is any anomalous behaviour associated with Active Directory (AD) identities when investigating a breach ▪ Provide visibility of results of malicious reconnaissance activities against AD
IaaS Security	Azure Security Center	▪ Automatically enable Defender ATP on IaaS workloads
SIEM	Microsoft Azure Sentinel	▪ Automatically integrated as a data source for Azure Sentinel analysis

Built-in, No Agents, No On-Premise Infrastructure

AUTOMATED INVESTIGATION & REMEDIATION

From alert to remediation in minutes at scale



Differentiator!

Client

FORENSIC COLLECTOR

RESPONSE ORCHASTRATOR

Cloud

HISTORICAL ENDPOINT DATA

RESPONSE ORCHSTRATION

AI BASED RESPONSE PLAYBOOKS

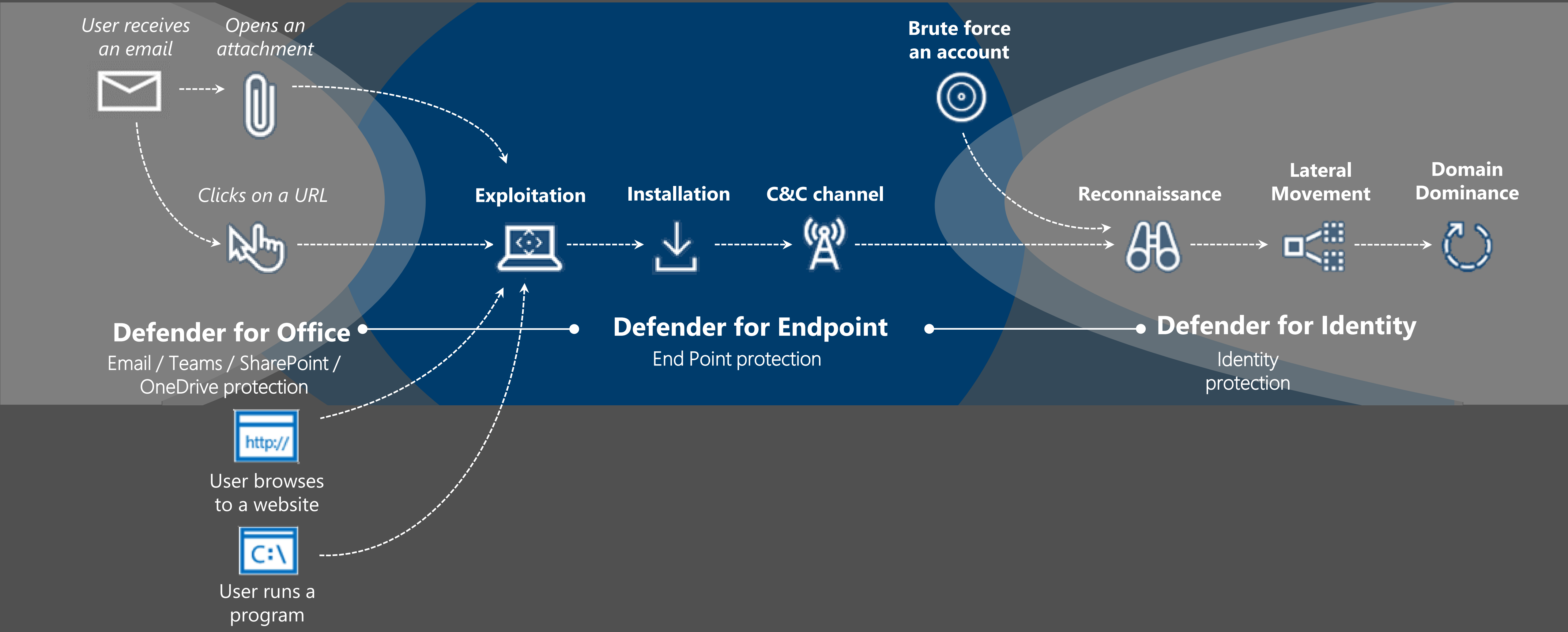
FILE/IP REPUTATION

SANDBOX

- AI-based automatic investigation of alerts
- Expand an incident scope across multiple alerts and endpoints
- Automatic remediation actions
- Respond and resolve breaches more quickly
- Reduce the load on security operations team
- Bridge the skill gap
- Driven by Artificial Intelligence

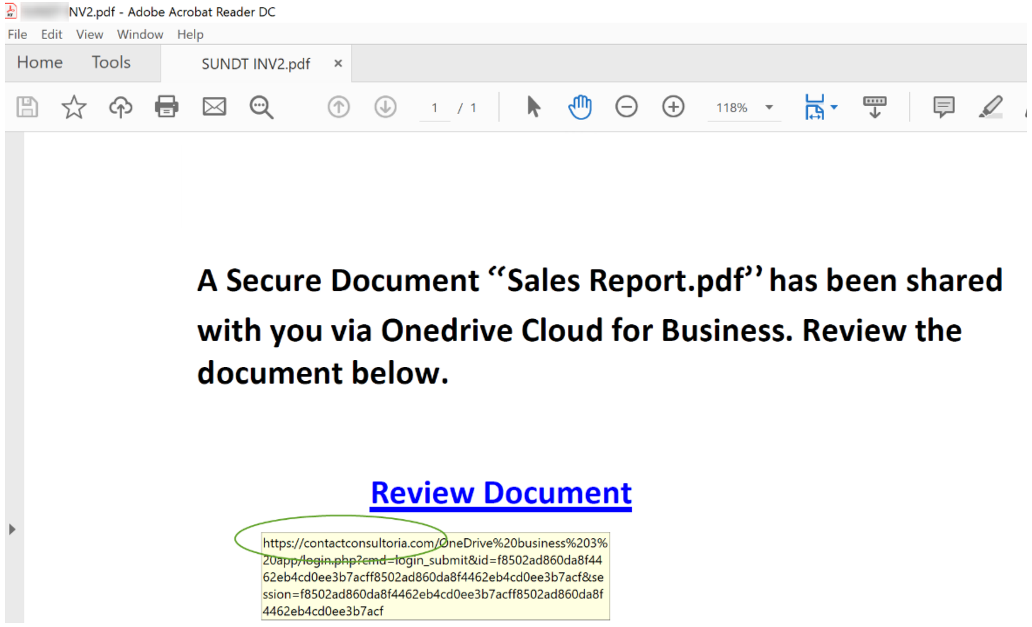
Better Together Signal Sharing

Microsoft 365 Defender



Defense in Depth

Problem Scenario: A PDF Attachment containing a hyperlink that points to a new URL designed for phishing.

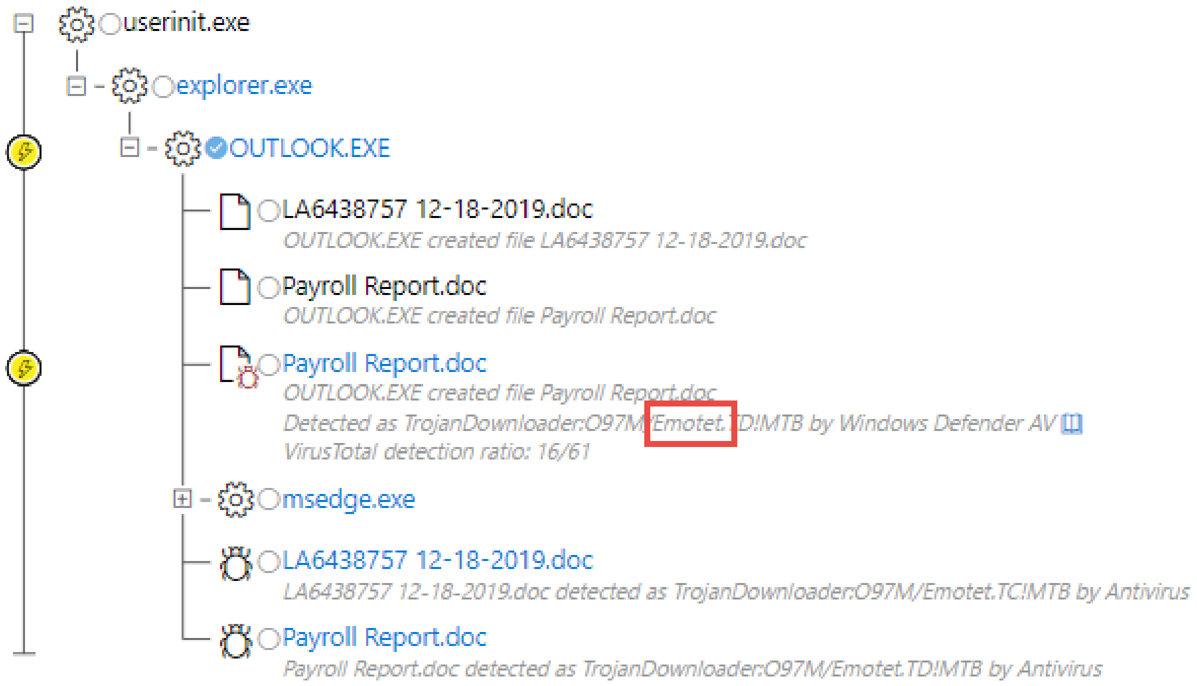

[redacted]NV2.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools SUNDT INV2.pdf ×
1 / 1
118%

A Secure Document "Sales Report.pdf" has been shared with you via Onedrive Cloud for Business. Review the document below.

Review Document

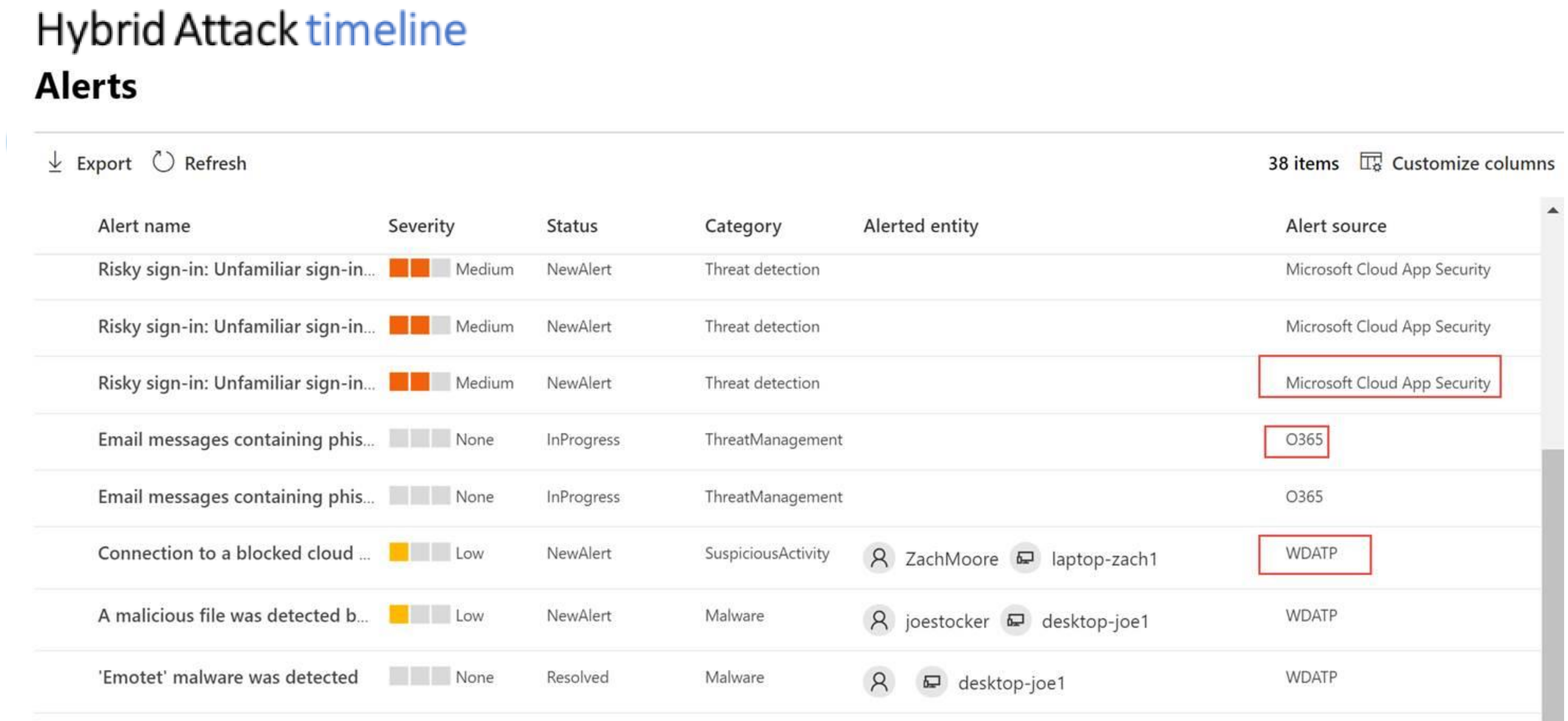
https://contactconsultoria.com/OneDrive%20business%203%20app/login.php?cmd=login_submit&id=f8502ad860da8f4462eb4cd0ee3b7acff8502ad860da8f4462eb4cd0ee3b7acf&session=f8502ad860da8f4462eb4cd0ee3b7acff8502ad860da8f4462eb4cd0ee3b7acf

Solution: Microsoft Defender ATP is the extra layer of defense



- userinit.exe
  - explorer.exe
    - OUTLOOK.EXE
      - LA6438757 12-18-2019.doc
        OUTLOOK.EXE created file LA6438757 12-18-2019.doc
      - Payroll Report.doc
        OUTLOOK.EXE created file Payroll Report.doc
      - Payroll Report.doc
        OUTLOOK.EXE created file Payroll Report.doc
        Detected as TrojanDownloader:O97M/Emotet.TD!MTB by Windows Defender AV
        VirusTotal detection ratio: 16/61
      - msedge.exe
      - LA6438757 12-18-2019.doc
        LA6438757 12-18-2019.doc detected as TrojanDownloader:O97M/Emotet.TC!MTB by Antivirus
      - Payroll Report.doc
        Payroll Report.doc detected as TrojanDownloader:O97M/Emotet.TD!MTB by Antivirus

Microsoft 365 Defender Portal provides correlates signals



Hybrid Attack timeline

Alerts

Alert name	Severity	Status	Category	Alerted entity	Alert source
Risky sign-in: Unfamiliar sign-in...	🟧🟧⬜ Medium	NewAlert	Threat detection		Microsoft Cloud App Security
Risky sign-in: Unfamiliar sign-in...	🟧🟧⬜ Medium	NewAlert	Threat detection		Microsoft Cloud App Security
Risky sign-in: Unfamiliar sign-in...	🟧🟧⬜ Medium	NewAlert	Threat detection		Microsoft Cloud App Security
Email messages containing phis...	⬜⬜⬜ None	InProgress	ThreatManagement		O365
Email messages containing phis...	⬜⬜⬜ None	InProgress	ThreatManagement		O365
Connection to a blocked cloud ...	🟨⬜⬜ Low	NewAlert	SuspiciousActivity	ZachMoore laptop-zach1	WDATP
A malicious file was detected b...	🟨⬜⬜ Low	NewAlert	Malware	joestocker desktop-joe1	WDATP
'Emotet' malware was detected	⬜⬜⬜ None	Resolved	Malware	desktop-joe1	WDATP

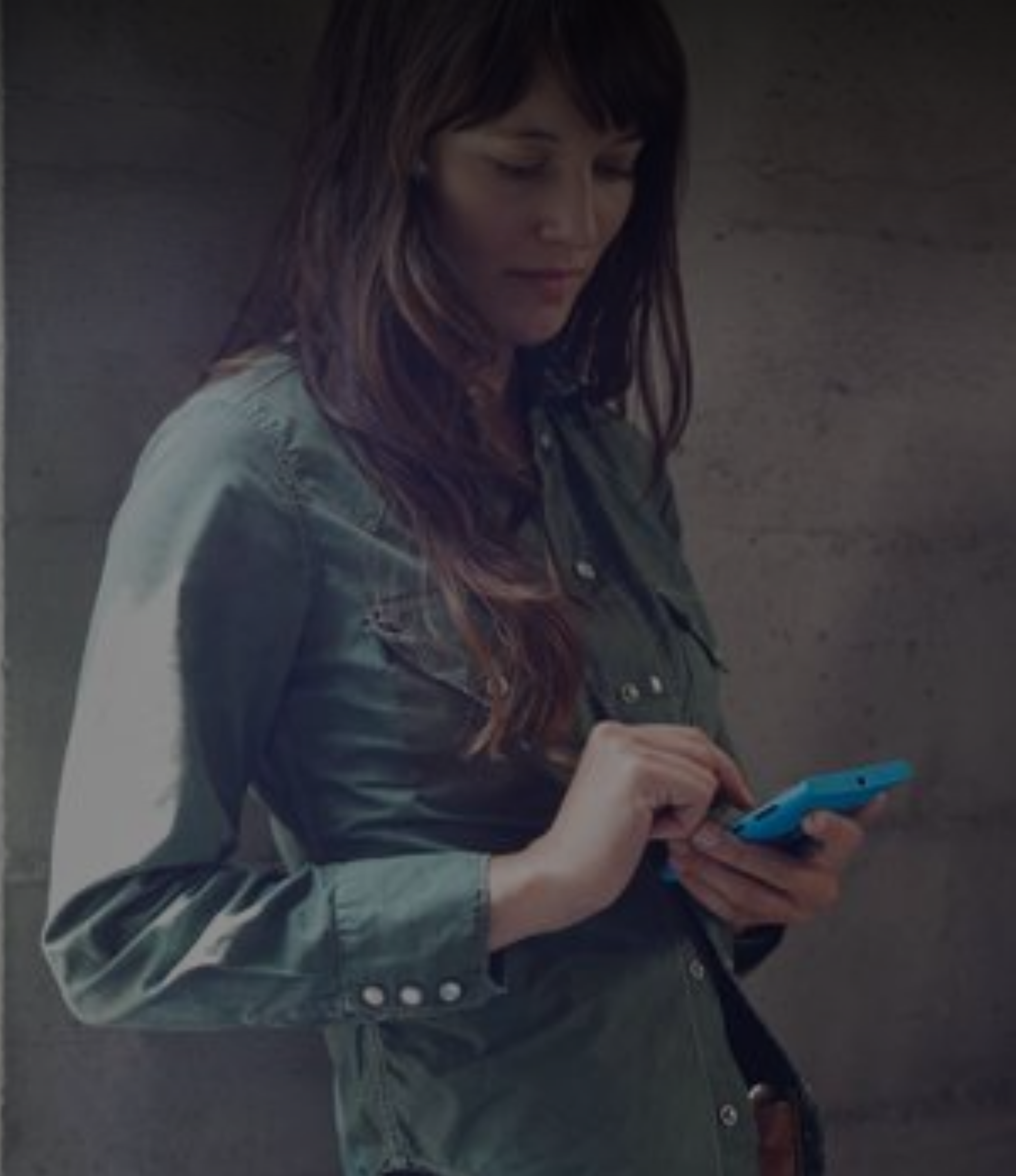
Security Issue #10

O365 Governance

Did you know the default values in Office 365 can lead to a data breach?

The default security score is 35 out of 700

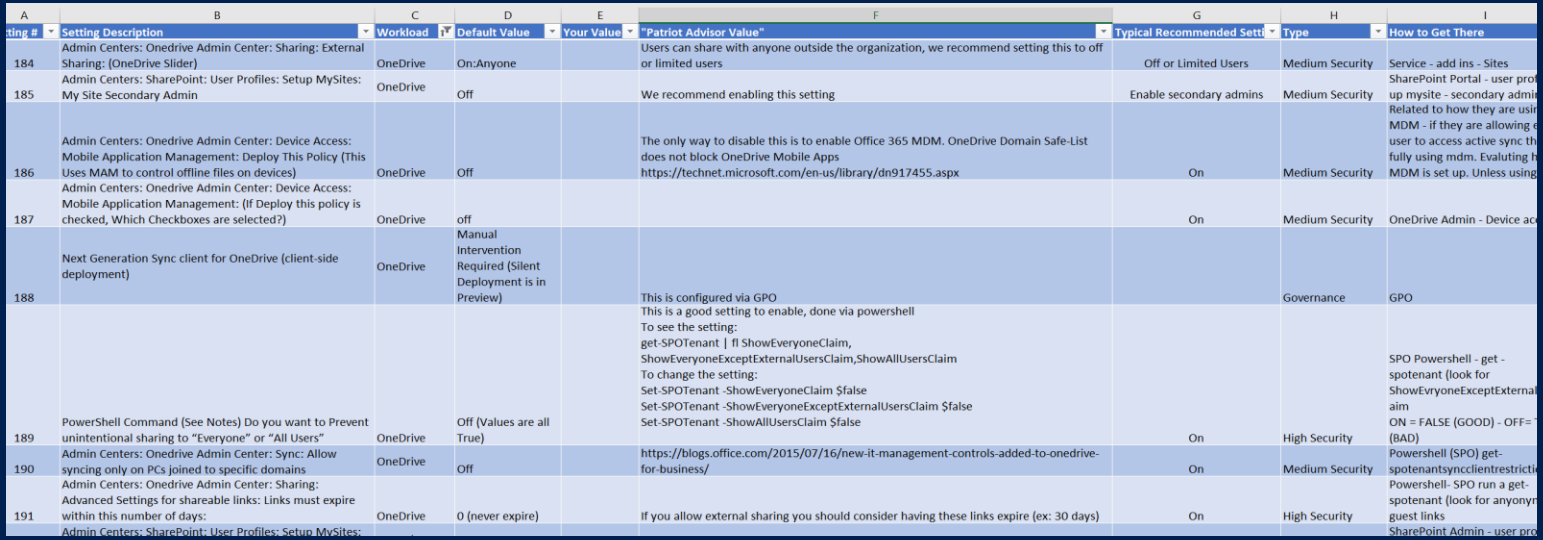
Microsoft adds 120 new settings every year to M365



CLOUD-POWERED PROTECTION

SecureAudit 365

- Audit of 600+ settings in Microsoft 365
- Delivery of a "Governance and Hardening" Audit Report with all your tenant's security settings documented
- Remediation and hardening recommendations along with guidance to implement recommendations
- Audit report is updated quarterly with new settings
- Includes a monthly report of new settings that we can help implement for you

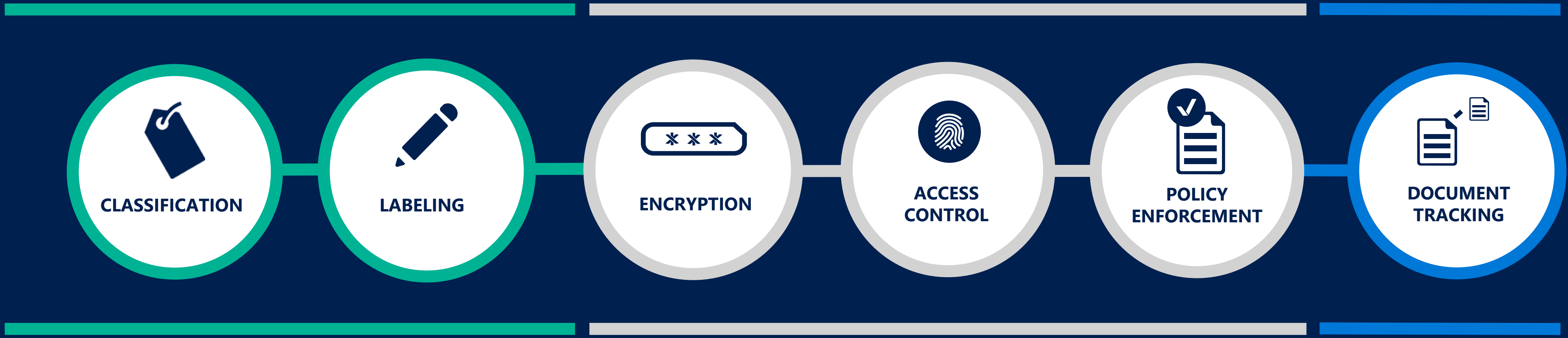


A	B	C	D	E	F	G	H	I
tting #	Setting Description	Workload	Default Value	Your Value	"Patriot Advisor Value"	Typical Recommended Setti	Type	How to Get There
184	Admin Centers: Onedrive Admin Center: Sharing: External Sharing: (OneDrive Slider)	OneDrive	On:Anyone		Users can share with anyone outside the organization, we recommend setting this to off or limited users	Off or Limited Users	Medium Security	Service - add ins - Sites
185	Admin Centers: SharePoint: User Profiles: Setup MySites: My Site Secondary Admin	OneDrive	Off		We recommend enabling this setting	Enable secondary admins	Medium Security	SharePoint Portal - user prof up mysite - secondary admi
186	Admin Centers: Onedrive Admin Center: Device Access: Mobile Application Management: Deploy This Policy (This Uses MAM to control offline files on devices)	OneDrive	Off		The only way to disable this is to enable Office 365 MDM. OneDrive Domain Safe-List does not block OneDrive Mobile Apps https://technet.microsoft.com/en-us/library/dn917455.aspx	On	Medium Security	Related to how they are usi MDM - if they are allowing user to access active sync th fully using mdm. Evaluting h MDM is set up. Unless using
187	Admin Centers: Onedrive Admin Center: Device Access: Mobile Application Management: (If Deploy this policy is checked, Which Checkboxes are selected?)	OneDrive	off			On	Medium Security	OneDrive Admin - Device ac
188	Next Generation Sync client for OneDrive (client-side deployment)	OneDrive	Manual Intervention Required (Silent Deployment is in Preview)		This is configured via GPO		Governance	GPO
189	PowerShell Command (See Notes) Do you want to Prevent unintentional sharing to "Everyone" or "All Users"	OneDrive	Off (Values are all True)		This is a good setting to enable, done via powershell To see the setting: get-SPOTenant | fl ShowEveryoneClaim, ShowEveryoneExceptExternalUsersClaim,ShowAllUsersClaim To change the setting: Set-SPOTenant -ShowEveryoneClaim $false Set-SPOTenant -ShowEveryoneExceptExternalUsersClaim $false Set-SPOTenant -ShowAllUsersClaim $false	On	High Security	SPO Powershell - get - spotenant (look for ShowEvryoneExceptExterna aim ON = FALSE (GOOD) - OFF= (BAD)
190	Admin Centers: Onedrive Admin Center: Sync: Allow syncing only on PCs joined to specific domains	OneDrive	Off		https://blogs.office.com/2015/07/16/new-it-management-controls-added-to-onedrive-for-business/	On	Medium Security	Powershell (SPO) get-spotenantsyncclientrestricti
191	Admin Centers: Onedrive Admin Center: Sharing: Advanced Settings for shareable links: Links must expire within this number of days:	OneDrive	0 (never expire)		If you allow external sharing you should consider having these links expire (ex: 30 days)	On	High Security	Powershell- SPO run a get-spotenant (look for anyony guest links
	Admin Centers: SharePoint: User Profiles: Setup MySites:							SharePoint Admin - user pro

Security Issue #11

Sensitive files being leaked

Solution #1 – Microsoft Information Protection



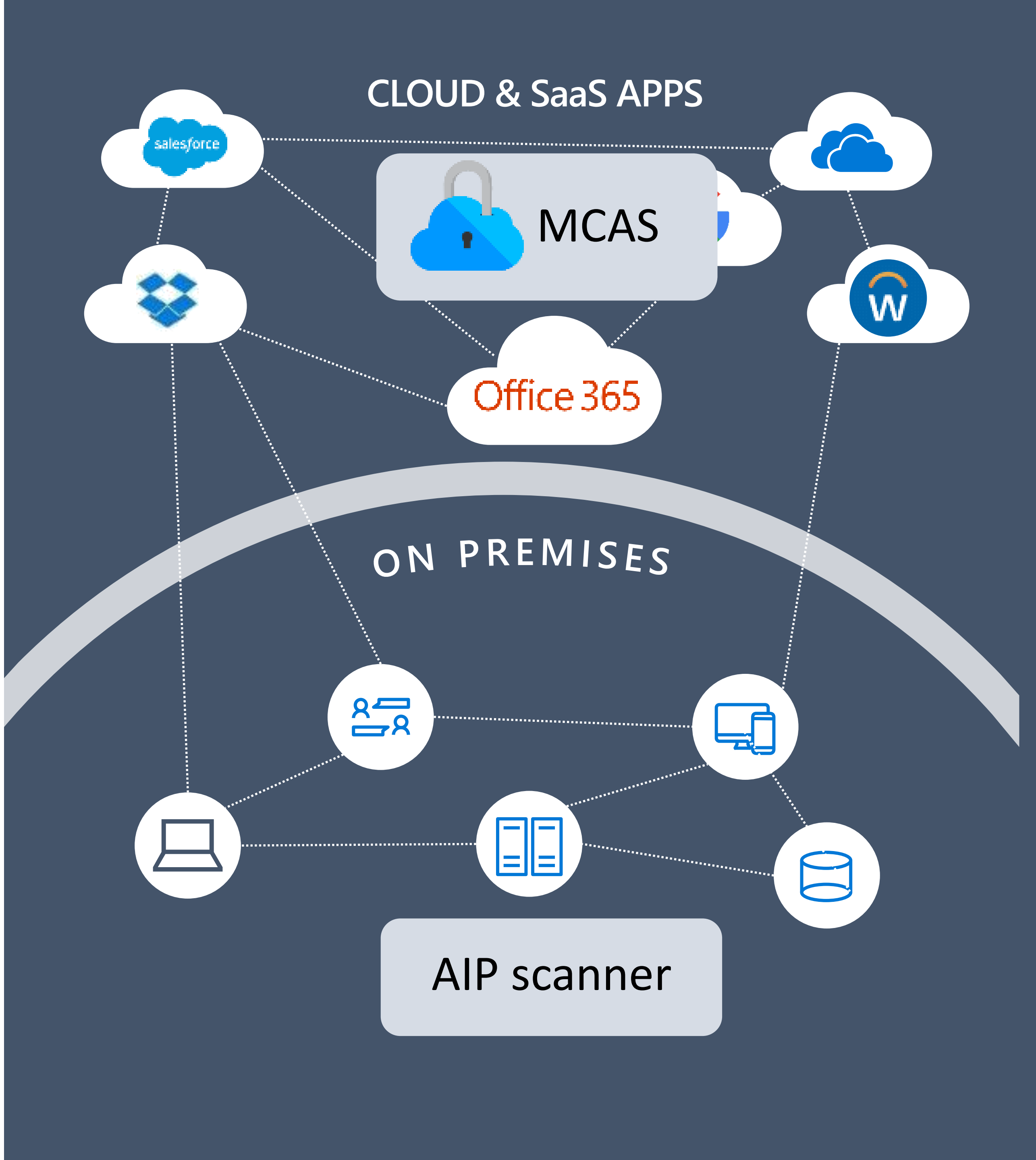
Classification & labeling

Protect

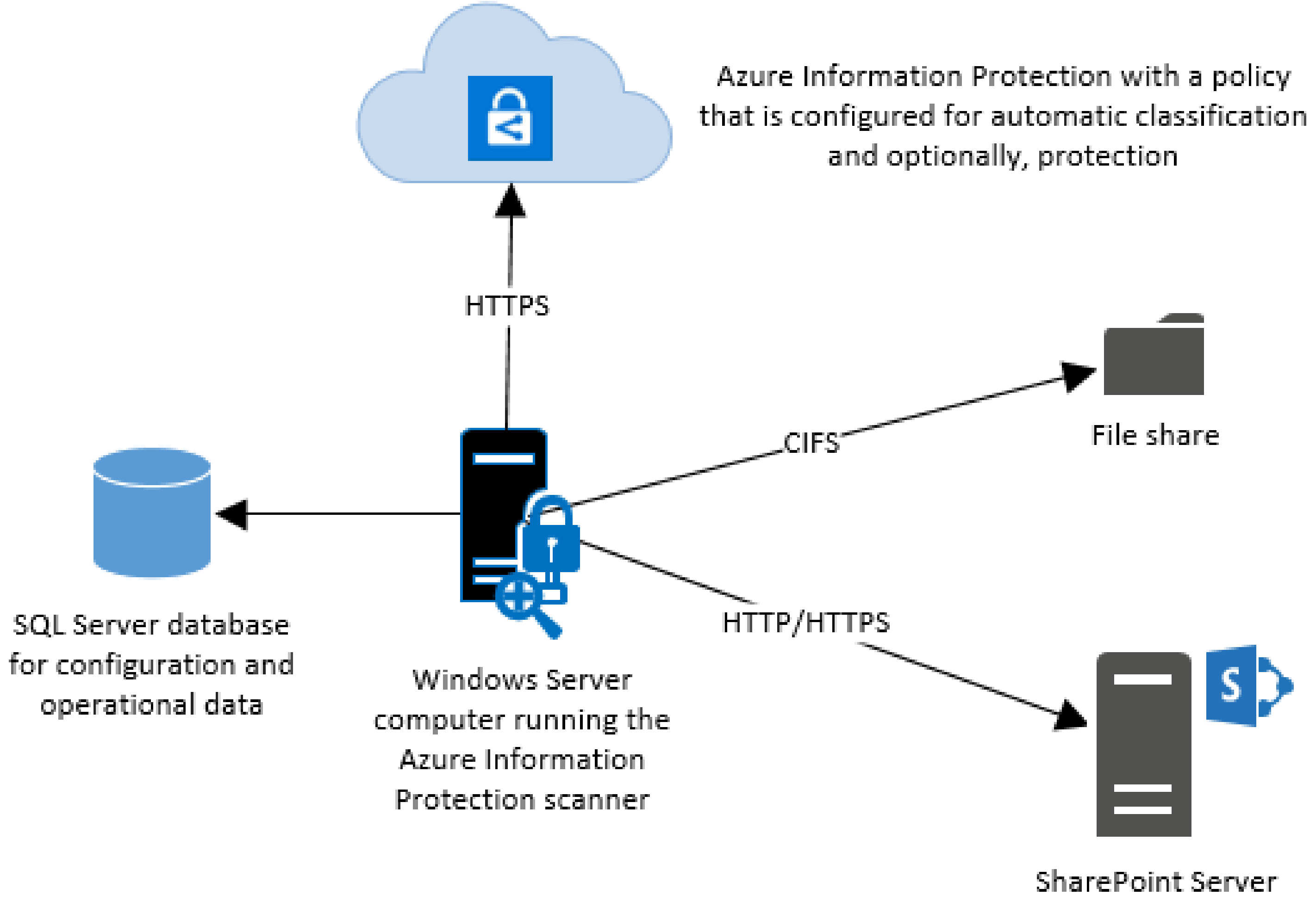
Monitor

EMS E3 = Manual Classification
EMS E5 = Automatic Classification

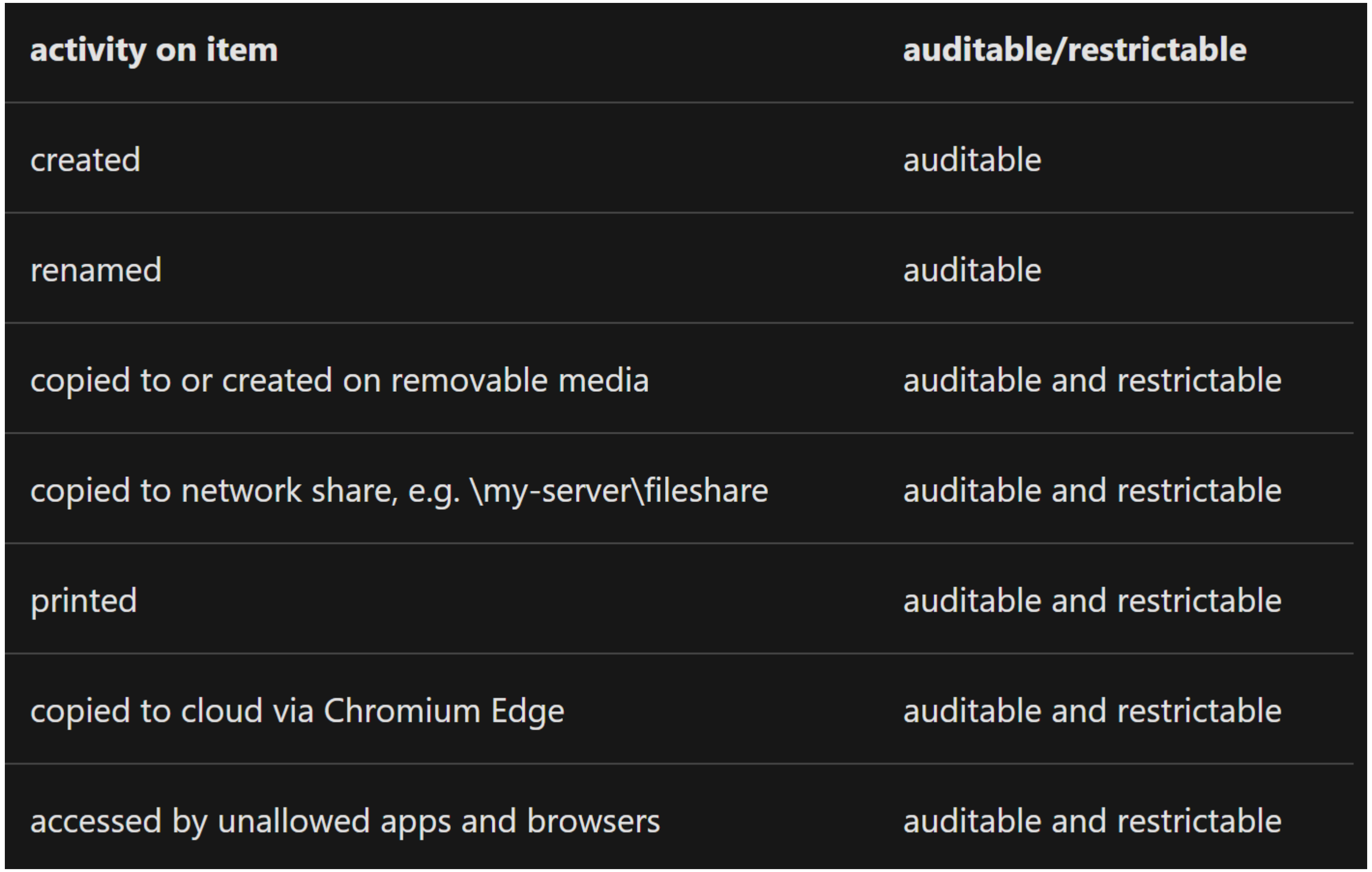
DETECT SENSITIVE INFORMATION
ON-PREMISES =AIP SCANNER
CLOUD =MCAS



AIP Scanner


Azure Information Protection with a policy that is configured for automatic classification and optionally, protection
HTTPS
CIFS
File share
HTTP/HTTPS
SQL Server database for configuration and operational data
Windows Server computer running the Azure Information Protection scanner
SharePoint Server

Endpoint DLP



activity on item	auditable/restrictable
created	auditable
renamed	auditable
copied to or created on removable media	auditable and restrictable
copied to network share, e.g. \my-server\fileshare	auditable and restrictable
printed	auditable and restrictable
copied to cloud via Chromium Edge	auditable and restrictable
accessed by unallowed apps and browsers	auditable and restrictable

System Requirements

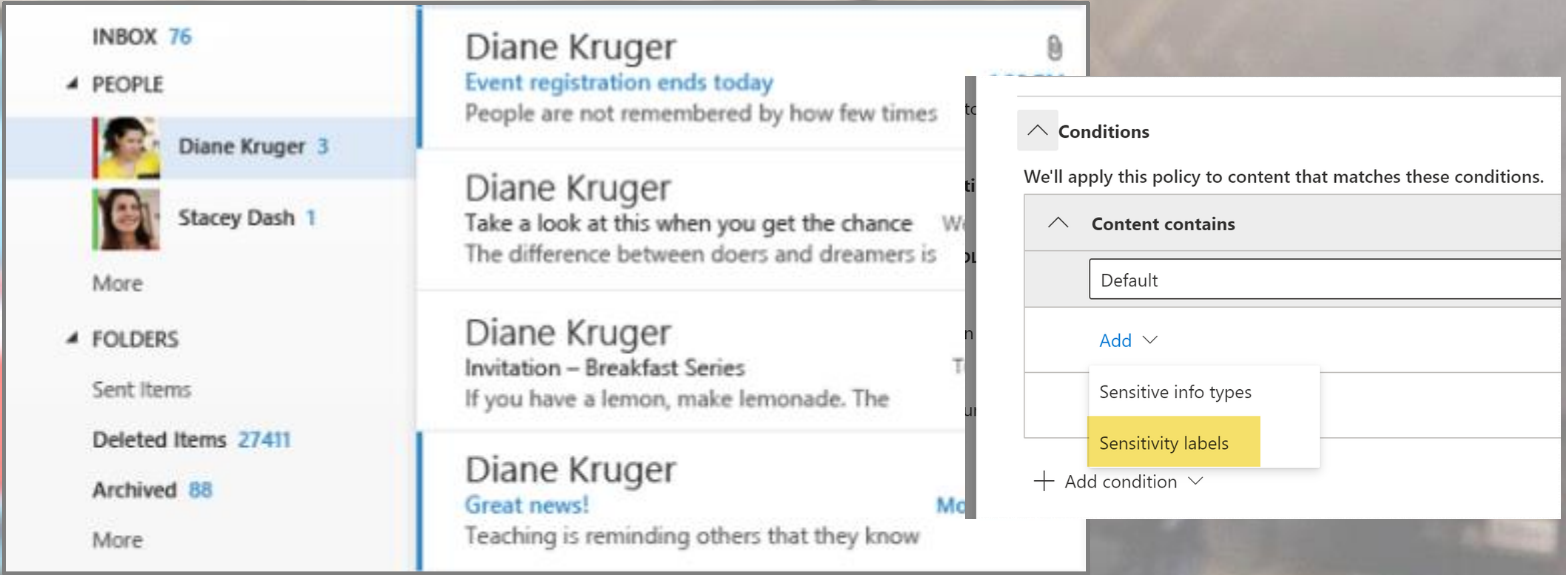
- Windows 10 1809+ (Win7 and Mac OSX are not supported)
- Hybrid domain joined
- MDATP *OR* DLP Enrollment Script
- Defender must be the Active AV
- Microsoft Chromium Edge browser

Exact Data Matching

- More Accurate than Regular Expressions
- Even more accurate when adding *Corresponding Key Words*
- Your sensitive data from SQL/Oracle Database extracted and hashed then used to scan content in
  - Email
  - OneDrive for Business
  - Microsoft Teams
  - SaaS apps

DLP Actions:

1. Audit Only
2. Policy Tip
3. Encrypt
4. Block
5. NEW: Apply AIP Label



INBOX 76

PEOPLE

Diane Kruger 3

Stacey Dash 1

More

FOLDERS

Sent Items

Deleted Items 27411

Archived 88

More

Diane Kruger
Event registration ends today
People are not remembered by how few times

Diane Kruger
Take a look at this when you get the chance
The difference between doers and dreamers is

Diane Kruger
Invitation – Breakfast Series
If you have a lemon, make lemonade. The

Diane Kruger
Great news!
Teaching is reminding others that they know

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

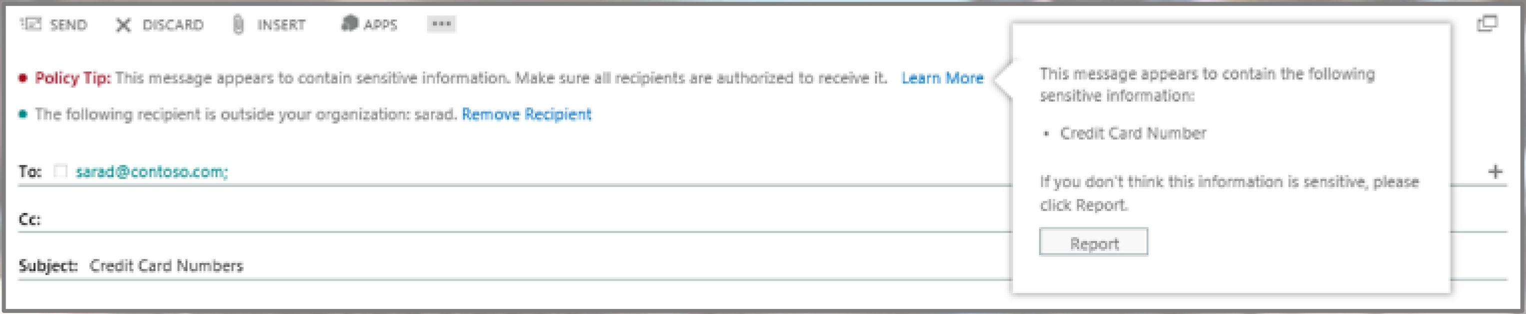
Default

Add

Sensitive info types

Sensitivity labels

Add condition



Policy Tip: This message appears to contain sensitive information. Make sure all recipients are authorized to receive it. Learn More

The following recipient is outside your organization: sarad. Remove Recipient

To: sarad@contoso.com;

Cc:

Subject: Credit Card Numbers

This message appears to contain the following sensitive information:

- Credit Card Number

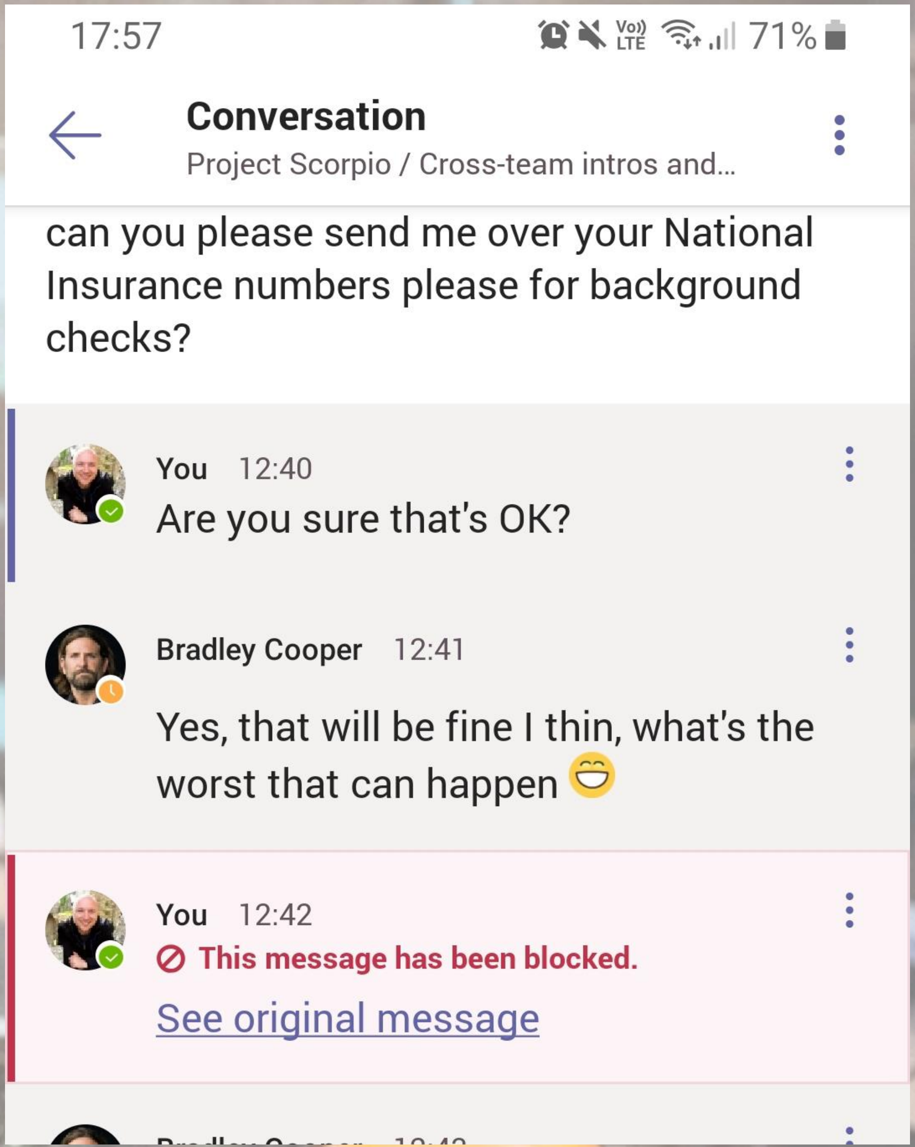
If you don't think this information is sensitive, please click Report.

Report

Block the transmission of your organization's sensitive information.

Data Loss Prevention for EXO/SPO/OneDrive

Office 365 E3



17:57 71%

Conversation

Project Scorpio / Cross-team intros and...

can you please send me over your National Insurance numbers please for background checks?

You 12:40

Are you sure that's OK?

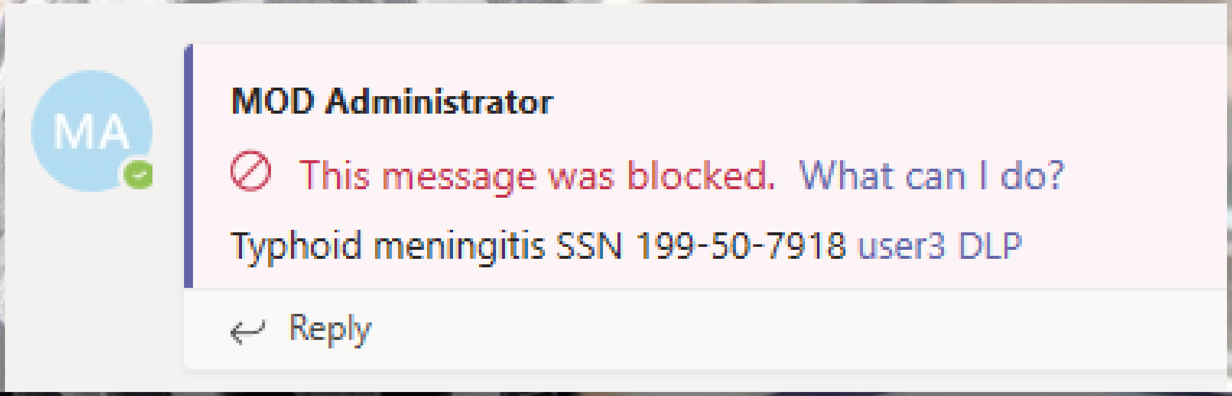
Bradley Cooper 12:41

Yes, that will be fine I thin, what's the worst that can happen 😁

You 12:42

⊘ **This message has been blocked.**

See original message



MOD Administrator

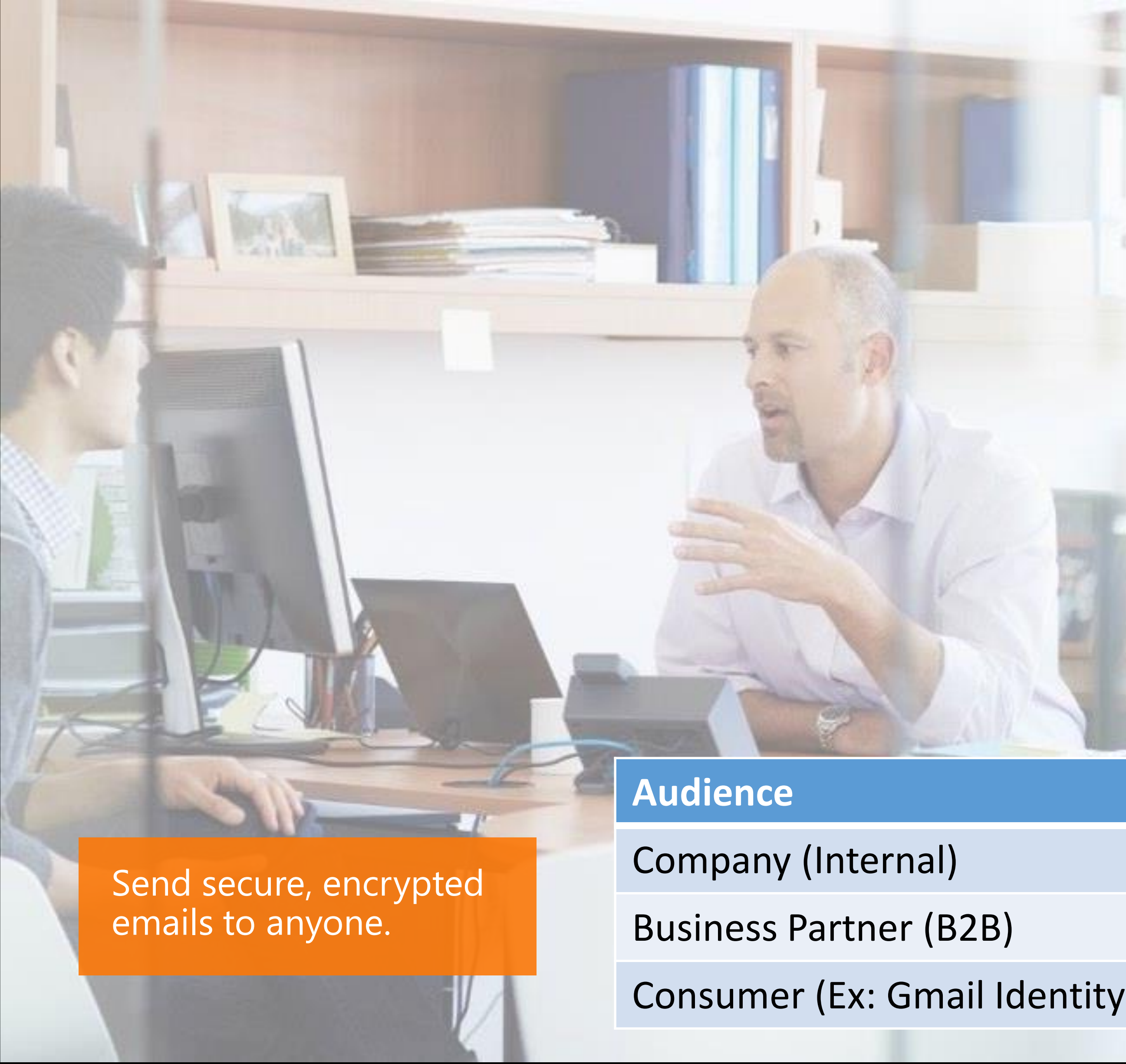
⊘ This message was blocked. What can I do?

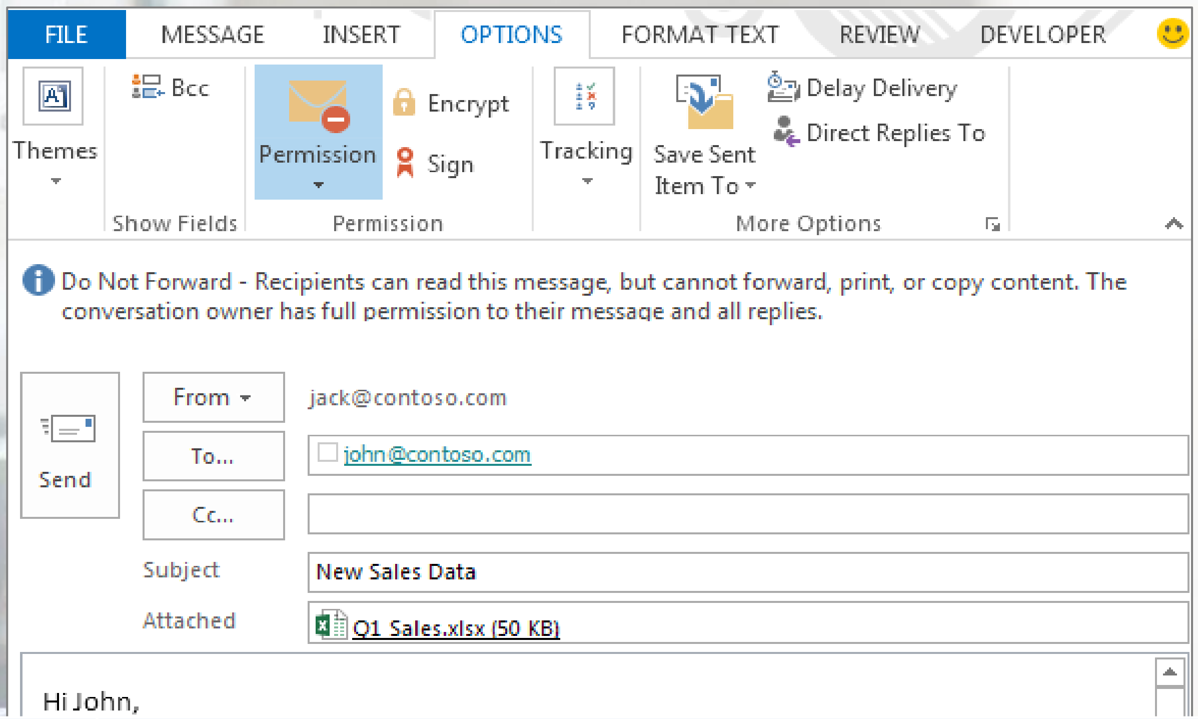
Typhoid meningitis SSN 199-50-7918 user3 DLP

↩ Reply

Data Loss Prevention for Teams

Office 365 E5





Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.

From: jack@contoso.com

To...: john@contoso.com

Cc...:

Subject: New Sales Data

Attached: Q1 Sales.xlsx (50 KB)

Hi John,

Send secure, encrypted emails to anyone.

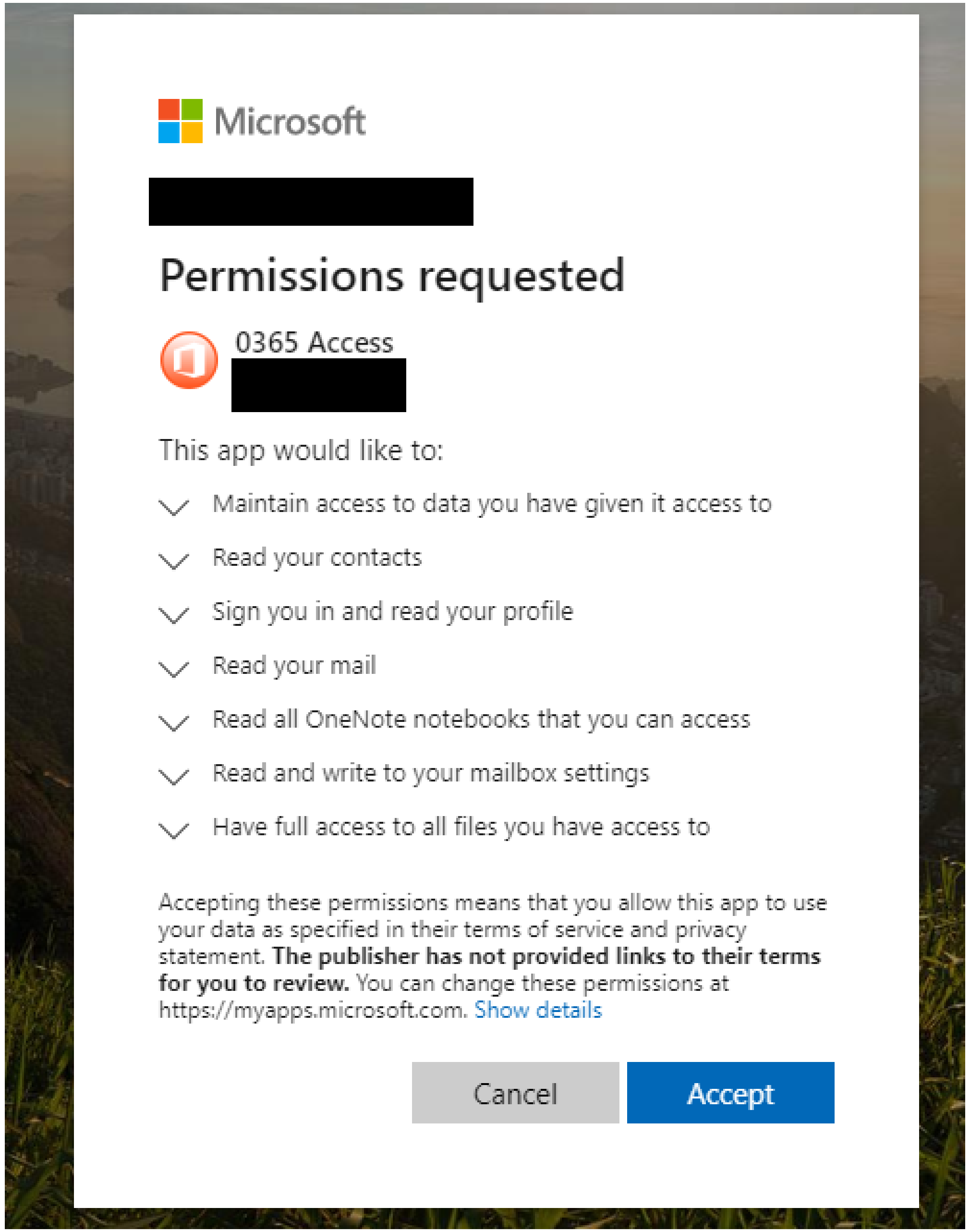
Audience	Solution
Company (Internal)	Azure Information Protection (AIP)
Business Partner (B2B)	TLS, AIP, S/Mime, or Office Message Encryption (OME)
Consumer (Ex: Gmail Identity)	Office Message Encryption (OME) v1 Web Portal and v2

Email Encryption

O365 E3 Office 365

Security Issue #12

Prevent oAuth Attacks



Microsoft

[redacted]

Permissions requested

0365 Access

[redacted]

This app would like to:

- Maintain access to data you have given it access to
- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

oAuth Attacks are stealthy

…attacker maintains persistent access

Even if you reset the user's password
Even if you enable MFA

attacker still dwells in the account.

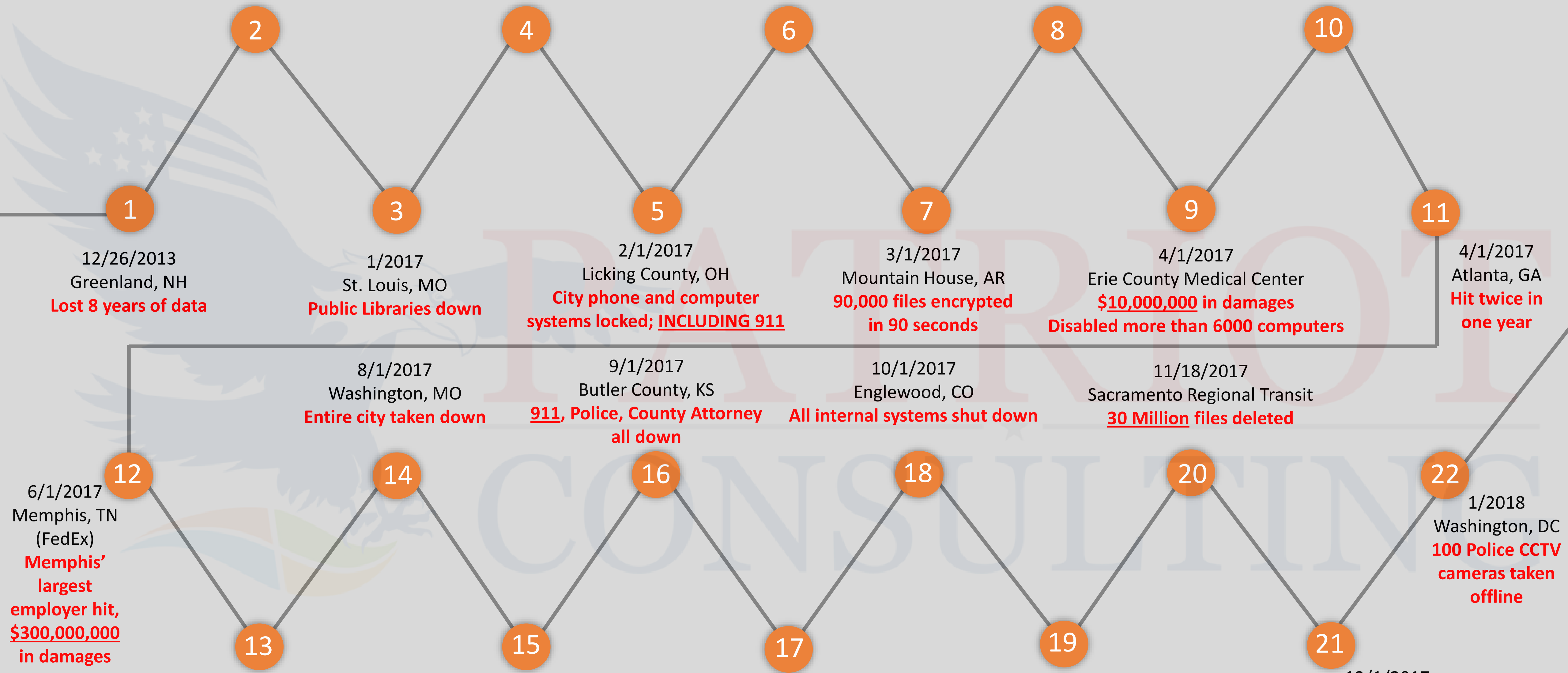
Solution 1 – Disable End User Consent

Solution 2 – Monitor for illicit apps with MCAS

Solution 3 – Route user consent to an Admin

Ransomware

How can Microsoft help Block Ransomware?



1 12/26/2013 Greenland, NH **Lost 8 years of data**

2 11/25/2016 San Francisco Railway **Internal communications halted; including email**

3 1/2017 St. Louis, MO **Public Libraries down**

4 1/2017 Bigfork, MT **Public School systems brought down**

5 2/1/2017 Licking County, OH **City phone and computer systems locked; INCLUDING 911**

6 2/15/2017 Bingham County, ID **Over $100,000 in damages**

7 3/1/2017 Mountain House, AR **90,000 files encrypted in 90 seconds**

8 3/1/2017 Pennsylvania Senate **16 Senators affected; Email, file and web servers**

9 4/1/2017 Erie County Medical Center **$10,000,000 in damages Disabled more than 6000 computers**

10 4/1/2017 Newark, NJ **City Hall hacked; files locked**

11 4/1/2017 Atlanta, GA **Hit twice in one year**

12 6/1/2017 Memphis, TN (FedEx) **Memphis' largest employer hit, $300,000,000 in damages**

13 7/1/2017 Mufreesboro, TN **Police and Fire Depts. hit**

14 8/1/2017 Washington, MO **Entire city taken down**

15 9/1/2017 Montgomery County, AL **City services halted**

16 9/1/2017 Butler County, KS **911, Police, County Attorney all down**

17 10/1/2017 Issaquah, WA **City offline for four days**

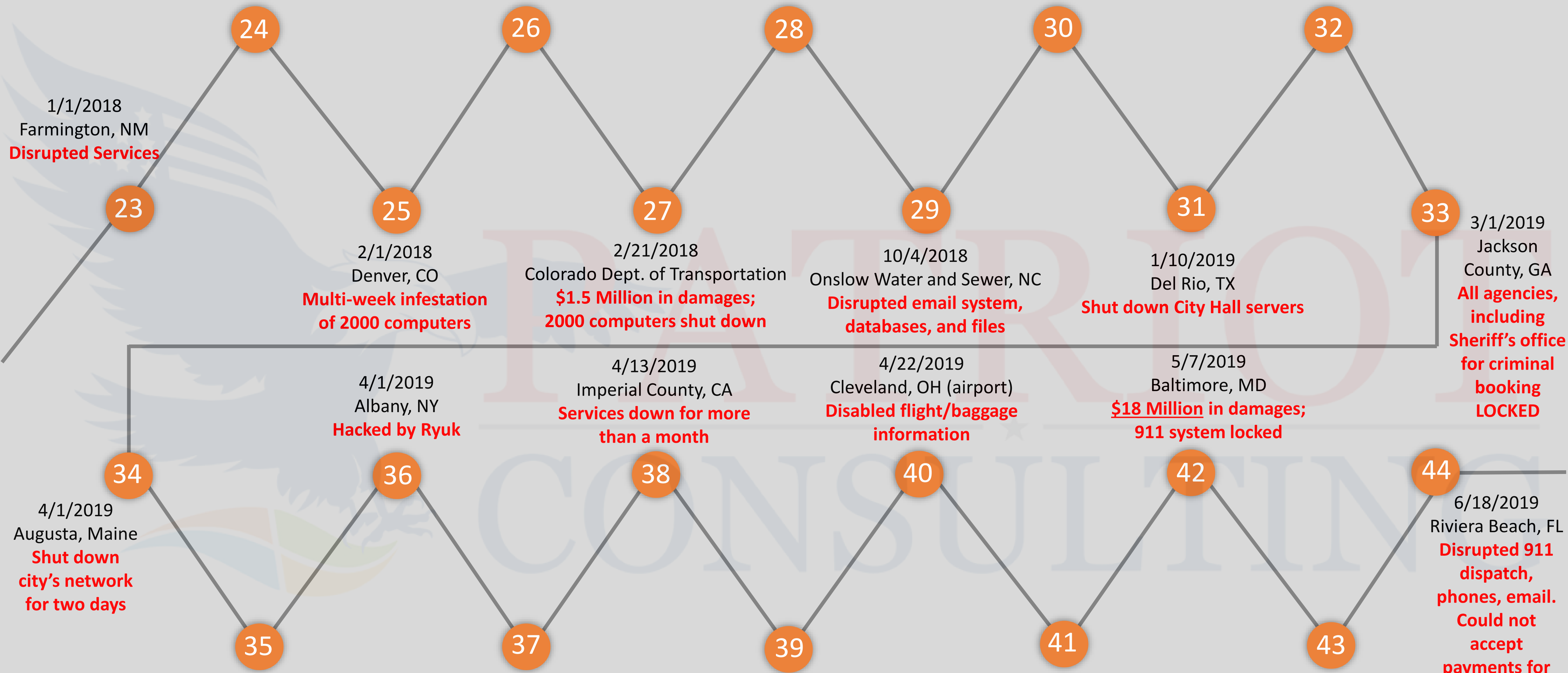
18 10/1/2017 Englewood, CO **All internal systems shut down**

19 11/2/2017 Spring Hill, TN **Halted credit/debit payments**

20 11/18/2017 Sacramento Regional Transit **30 Million files deleted**

21 12/1/2017 Mecklenburg, NC **Employee payroll; Soc. Services Depts. down**

22 1/2018 Washington, DC **100 Police CCTV cameras taken offline**



23
1/1/2018
Farmington, NM
Disrupted Services

24
1/1/2018
Cockrell Hill, TX
Lost seven years of data, including video evidence

25
2/1/2018
Denver, CO
Multi-week infestation of 2000 computers

26
2/5/2018
Dallas, TX
Tornado Alarm system down

27
2/21/2018
Colorado Dept. of Transportation
$1.5 Million in damages; 2000 computers shut down

28
3/1/2018
Atlanta, GA
$17,000,000 in damages

29
10/4/2018
Onslow Water and Sewer, NC
Disrupted email system, databases, and files

30
1/1/2019
Sammamish, WA
Unable to process passports, permits, and map services

31
1/10/2019
Del Rio, TX
Shut down City Hall servers

32
1/22/2019
Akron, OH
City services, including 311 and credit card payments down

33
3/1/2019
Jackson County, GA
All agencies, including Sheriff's office for criminal booking LOCKED

34
4/1/2019
Augusta, Maine
Shut down city's network for two days

35
4/1/2019
Lynn, Massachusetts
Online parking ticket payment system down

36
4/1/2019
Albany, NY
Hacked by Ryuk

37
4/10/2019
Greenville, NC
Computers down; only cash transactions

38
4/13/2019
Imperial County, CA
Services down for more than a month

39
4/13/2019
Stuart, Florida
$2,000,000 to rebuild network

40
4/22/2019
Cleveland, OH (airport)
Disabled flight/baggage information

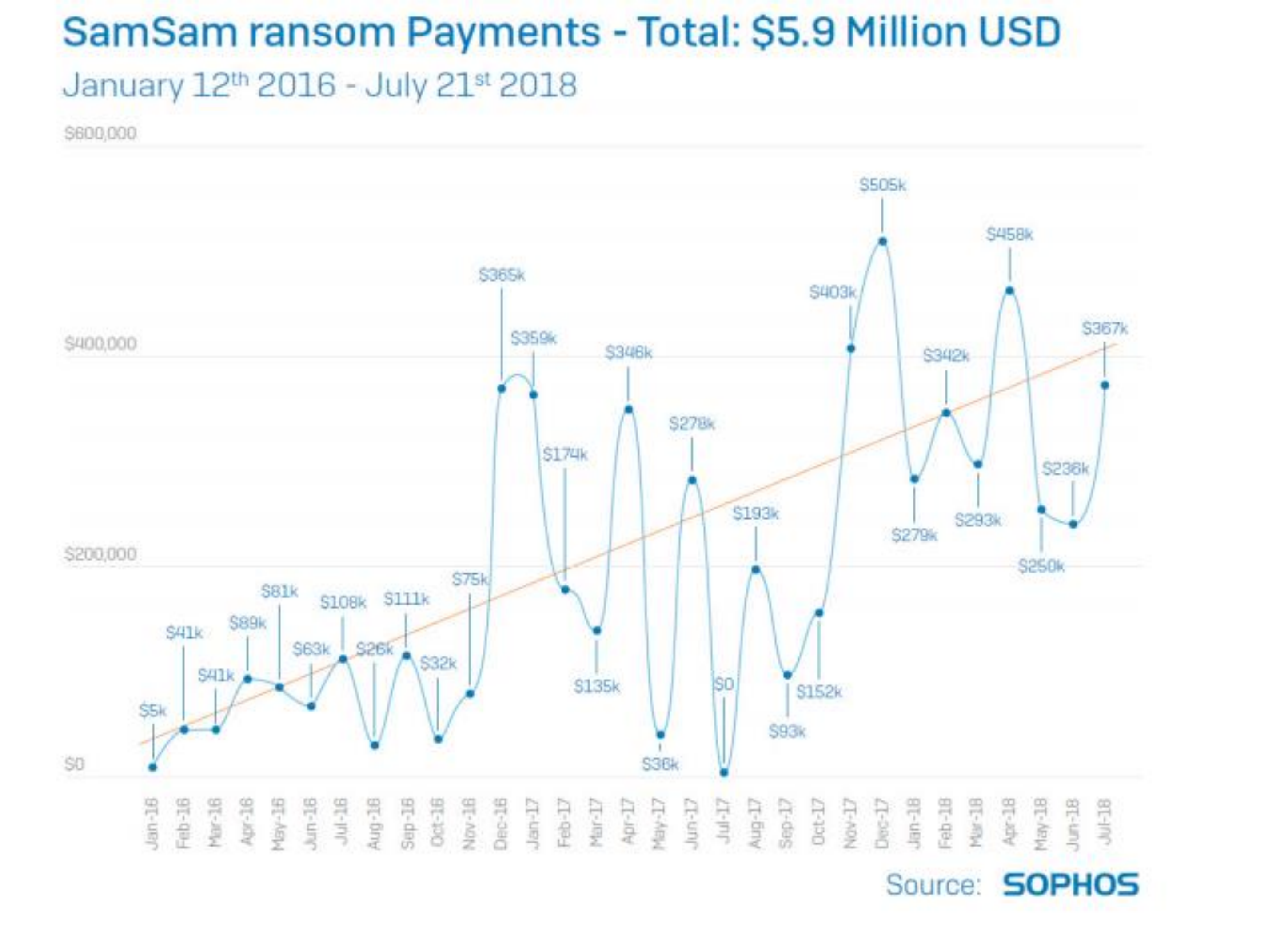
41
5/4/2019
Cartersville, GA
Online payments systems down for more than a week

42
5/7/2019
Baltimore, MD
$18 Million in damages; 911 system locked

43
6/10/2019
Lake City, FL
Hit by a "Triple Threat" Brought down email

44
6/18/2019
Riviera Beach, FL
Disrupted 911 dispatch, phones, email. Could not accept payments for city utilities.

Ransomware will continue because… its profitable $$$



SamSam ransom Payments - Total: $5.9 Million USD

January 12th 2016 - July 21st 2018

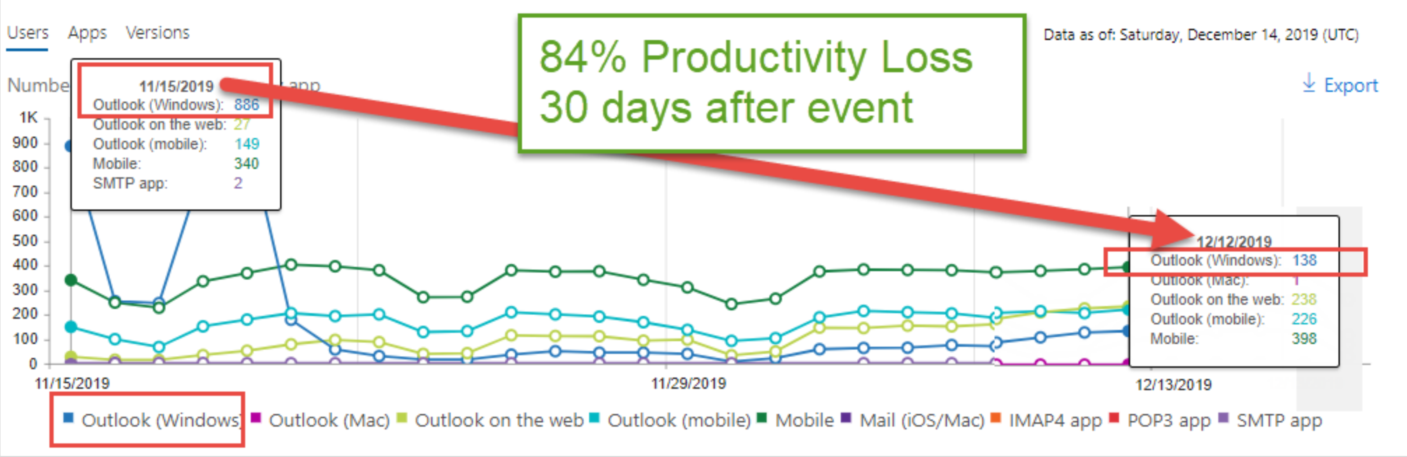
Source: SOPHOS

GrandCrab Ransomware earned its authors $2 billion in ransom payments, with average weekly payments of $2.5 million dollars.
Source: Bleeping Computer

*30% of CISO's for local governments stated that they are using **outdated technology**, making them vulnerable to cyber attacks, and fewer than half have purchased cybersecurity insurance*

Summary of Ransomware Damages

- ***Years*** of data permanently lost
- Personal information leaked to the internet (Increased Liability)
- Internal communications disrupted
- Critical systems taken offline (Payroll, Invoicing, etc)
- Employee down time, lost wages
- Expenses incurred for overtime pay for IT staff
- Disruption in services provided to customers
- Public Relations nightmare / damaged reputation and trust
- **<u>Ransomware infects one target every 40 seconds</u>**



Data as of: Saturday, December 14, 2019 (UTC)

84% Productivity Loss
30 days after event

11/15/2019	
Outlook (Windows):	886
Outlook on the web:	27
Outlook (mobile):	149
Mobile:	340
SMTP app:	2

12/12/2019	
Outlook (Windows):	138
Outlook (Mac):	1
Outlook on the web:	238
Outlook (mobile):	226
Mobile:	398

Ransomware Lessons

- If you pay the ransom - 30% of the time they will *not* give you the decryption key. Therefore, your backup system is absolutely mission critical to the mission of the IT Department. Data loss is unacceptable.
- Sometimes decryption keys are available for free at NoMoreRansome.org (newer ransomware is often not there)
- Sometimes Ransomware is meant to distract from the larger goals of the hacker (Data Exfiltration of Intellectual Property). This happened with Hermes Malware against the Bank of Taiwan and Bank of Bangladesh
- Lesson Learned: If you backup offsite (Cloud) – the internet download speed can hinder your recovery times. How long does it take to download multiple terabytes on your 100 Megabit Internet connection?
- Ransomware authors are well paid – some earn millions per week. They will outspend your defensive spending.
- Ransomware often uses zero day exploits to spread such as NSA's leaked Eternalblue vulnerability
- Ransomware authors can be state sponsored. According to the United Nations, North Korea uses ransomware to collect money against US-based companies to evade US Sanctions. They have earned 2 billion in ransom thus far.
- Sometimes these State-backed ransomware spills over into Civilian targets. Russia developed NotPetya to target Ukraine but it ended up spilling over and hitting Maersk (costing them 2 week outage and $300 million in losses)

Ransomware Lessons

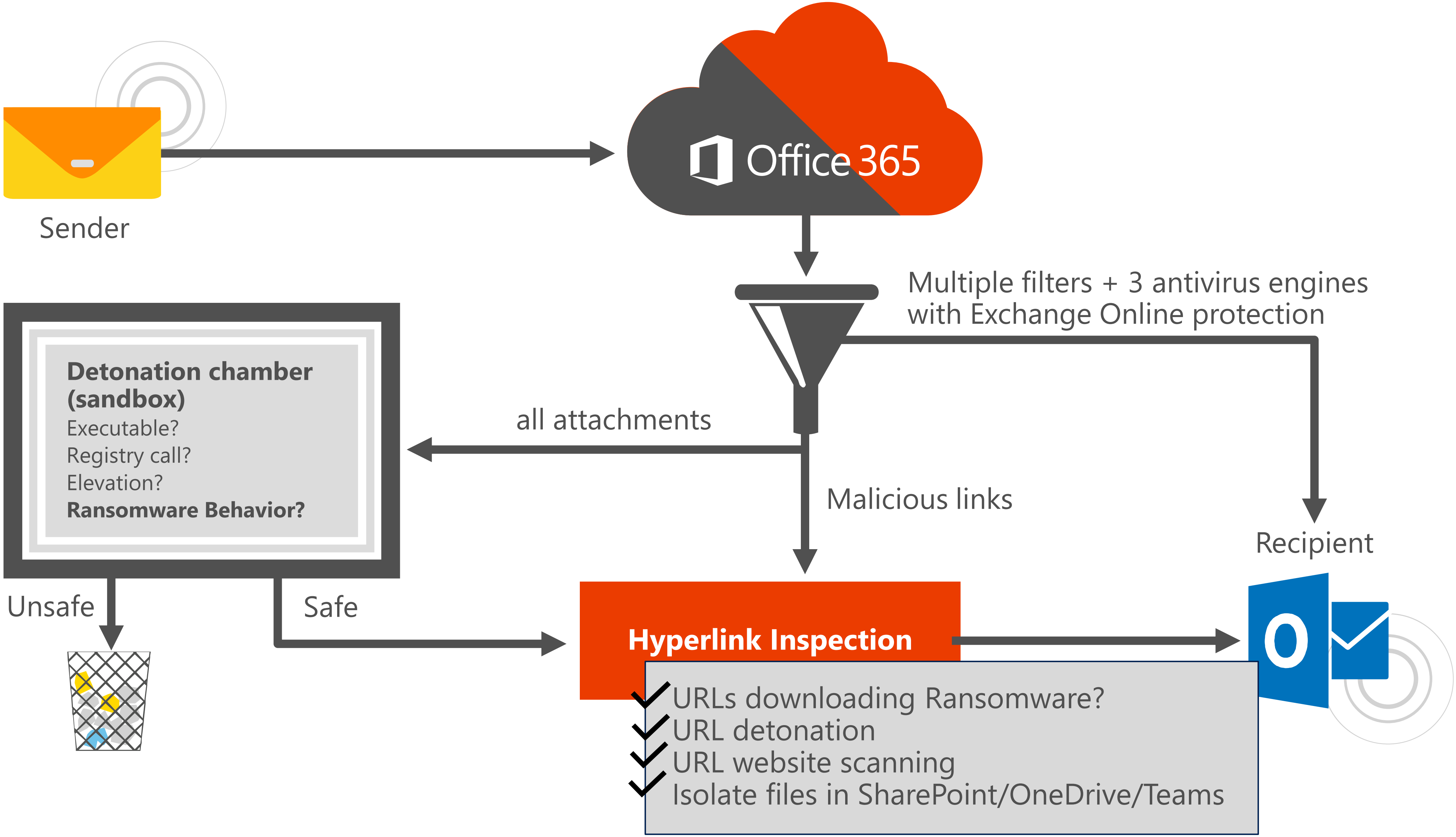
- Average Ransom Payment for a single computer is $1,000 (Paid in Bitcoin)
- Average Ransom Payment for an organization is $700,000 (Paid in Bitcoin)

How Ransomware Spreads:

- 80% to 90% of Ransomware spreads via Email Attachments
- Crysis Ransomware spreads via RDP
- Cerber/Cryptxxx spreads via Web downloads
- SAMSAM spreads via RedHat JBOSS
- WannaCry & NotPetya spread through SMB 1.0 vulnerabilities
- Mobile Ransomware on Android has increased 33% year over year
- Generally, iOS is more resistant to ransomware however there is a black market of iOS Vulnerabilities that are made by organizations such as the NSO Group that sell for $1 million. Examples include Pegasus Spyware that targeted the Trident Vulnerabilities

Ransomware Solutions

Defender for Office 365 blocks email ransomware



Sender
Office 365
Multiple filters + 3 antivirus engines with Exchange Online protection
all attachments
Malicious links
Recipient
Unsafe
Safe

Detonation chamber (sandbox)
Executable?
Registry call?
Elevation?
Ransomware Behavior?

Hyperlink Inspection

- ✓ URLs downloading Ransomware?
- ✓ URL detonation
- ✓ URL website scanning
- ✓ Isolate files in SharePoint/OneDrive/Teams

Win10 Attack Surface Reduction Rules (ASR)

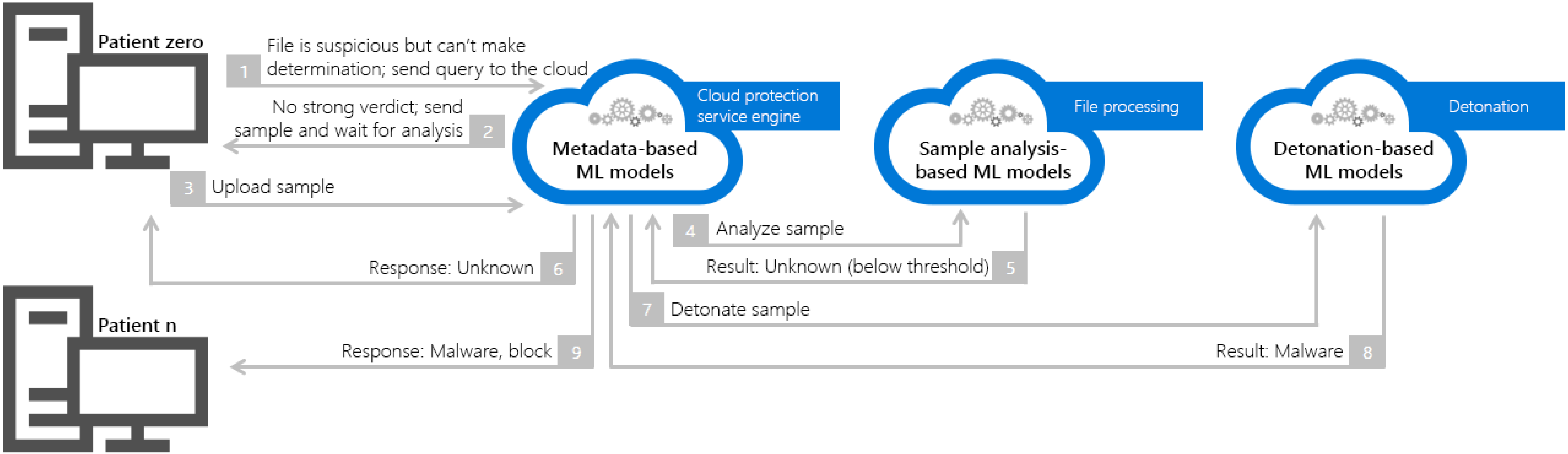
Win10 E3 ASR Rules

- **Advanced protection against ransomware**
  - This rule provides an extra layer of protection against ransomware. Executable files that enter the system will be scanned to determine whether they are trustworthy. If the files exhibit characteristics that closely resemble ransomware, they are blocked from being run or launched, provided they are not already in the trusted list or exception list.
- Block Office apps from creating executable content
- Block Office apps from launching child process
- Block Office apps from injecting into process
- Block Win32 imports from macro code in Office
- Block obfuscated macro code
- Block process creations originating from PSExec and WMI commands (do not enable if you have SCCM)
- Block untrusted and unsigned processes that run from USB
- Block executable content from email client and webmail
- Block JavaScript or VBScript from launching downloaded executable content
- Block execution of potentially obfuscated scripts
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)

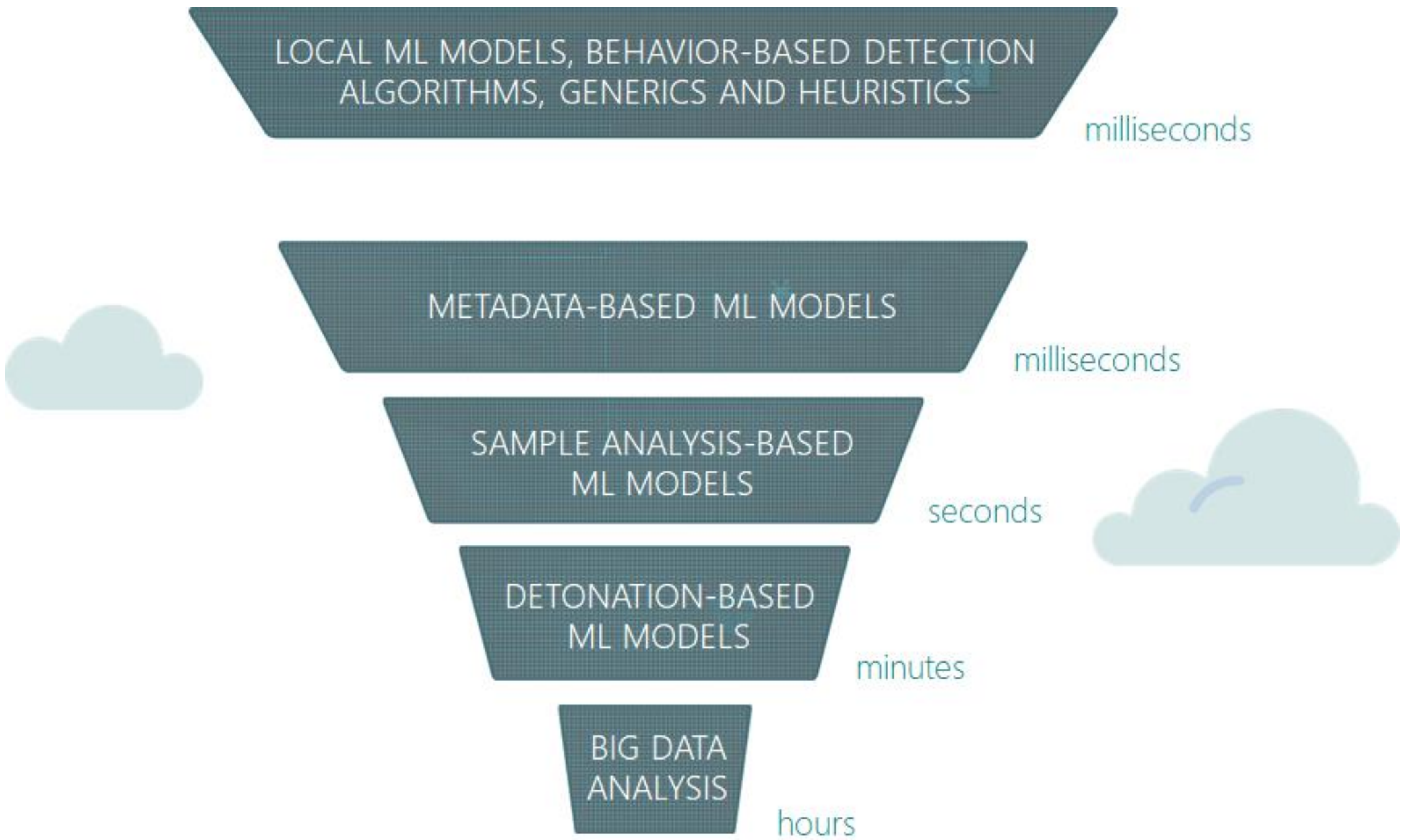
Win10 E5 ASR Rules

- Block Adobe Reader from creating child processes
- Block executable files from running unless they meet a prevalence, age, or trusted list criteria

Defender for Endpoint “Block at First Sight”


Patient zero
1 File is suspicious but can’t make determination; send query to the cloud
No strong verdict; send sample and wait for analysis 2
3 Upload sample
Cloud protection service engine
Metadata-based ML models
File processing
Sample analysis-based ML models
Detonation
Detonation-based ML models
4 Analyze sample
Result: Unknown (below threshold) 5
Response: Unknown 6
7 Detonate sample
Result: Malware 8
Response: Malware, block 9
Patient n

Microsoft Defender Multi-Layered Machine Learning



LOCAL ML MODELS, BEHAVIOR-BASED DETECTION ALGORITHMS, GENERICS AND HEURISTICS

milliseconds

METADATA-BASED ML MODELS

milliseconds

SAMPLE ANALYSIS-BASED ML MODELS

seconds

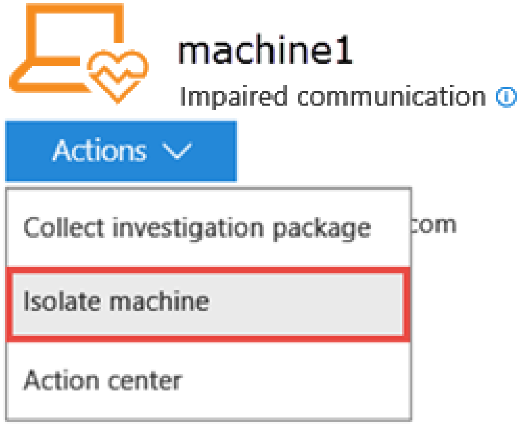
DETONATION-BASED ML MODELS

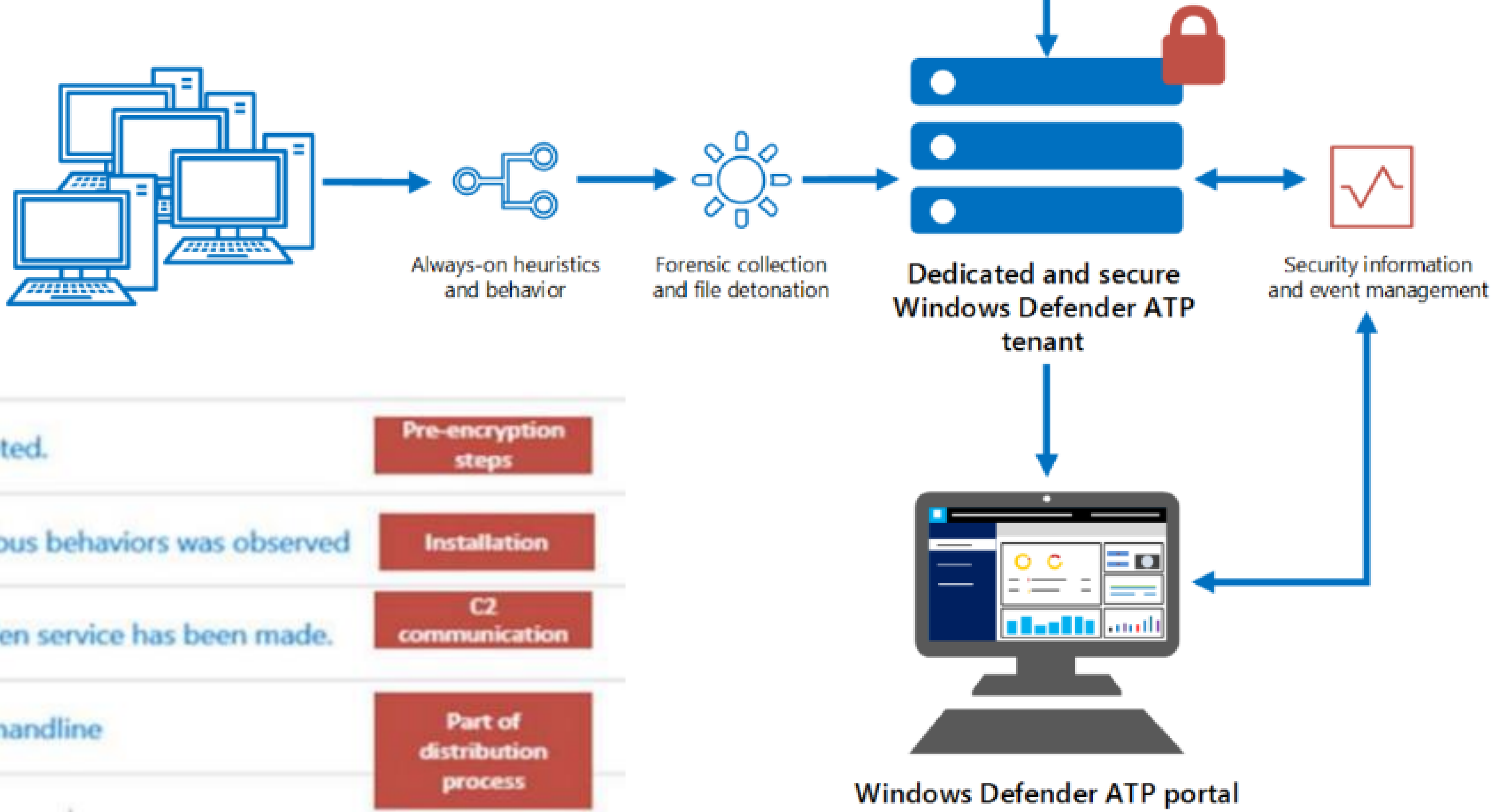
minutes

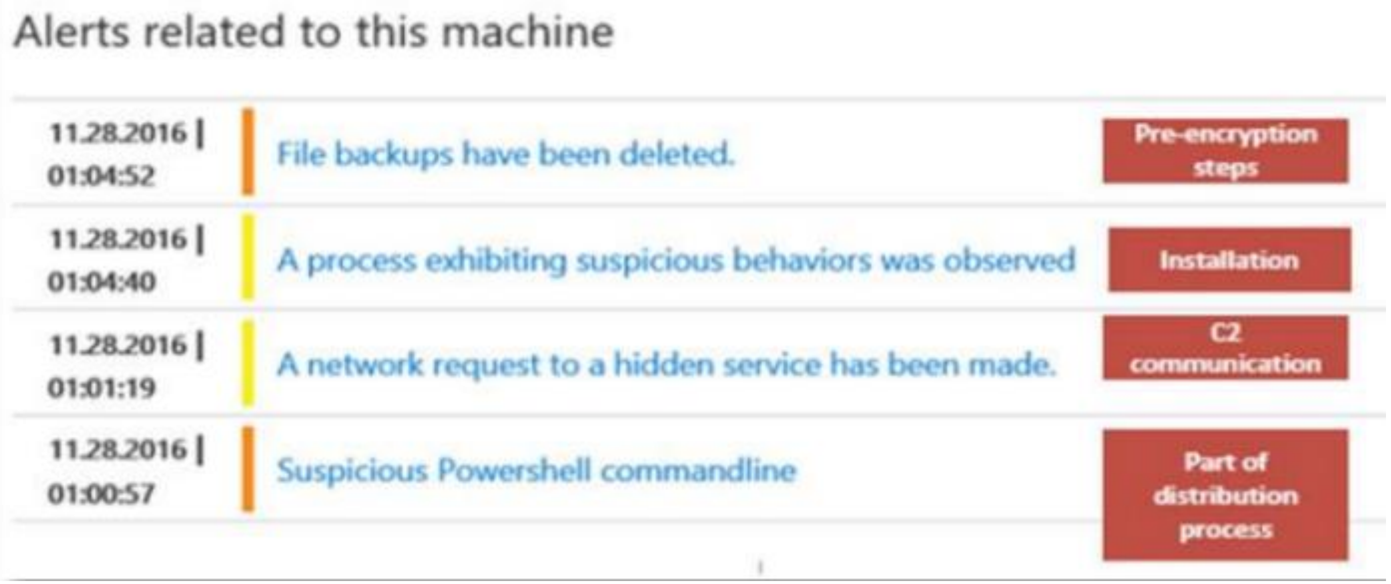
BIG DATA ANALYSIS

hours

Defender for Endpoint



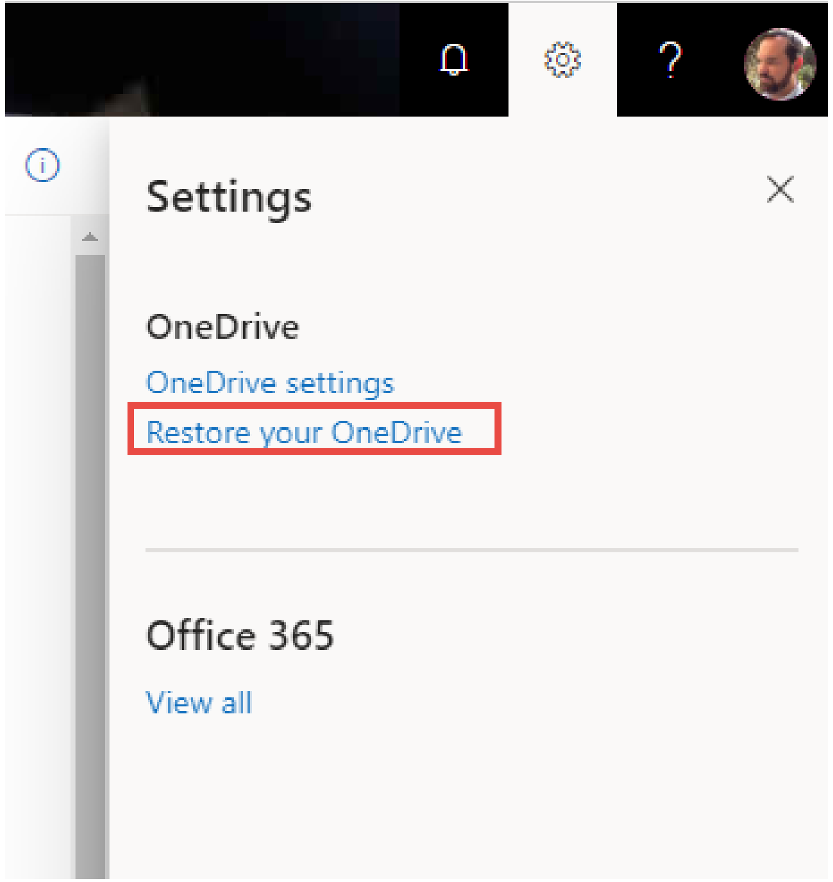

Cloud monitoring and reporting
Windows APT hunters
Industry collaborators
Microsoft AM researchers
Microsoft threat intelligence
Always-on heuristics and behavior
Forensic collection and file detonation
Dedicated and secure Windows Defender ATP tenant
Security information and event management
Windows Defender ATP portal



Alerts related to this machine

11.28.2016 | 01:04:52	File backups have been deleted.	Pre-encryption steps
11.28.2016 | 01:04:40	A process exhibiting suspicious behaviors was observed	Installation
11.28.2016 | 01:01:19	A network request to a hidden service has been made.	C2 communication
11.28.2016 | 01:00:57	Suspicious Powershell commandline	Part of distribution process

Self Service Ransomware Rollback in OneDrive



Settings

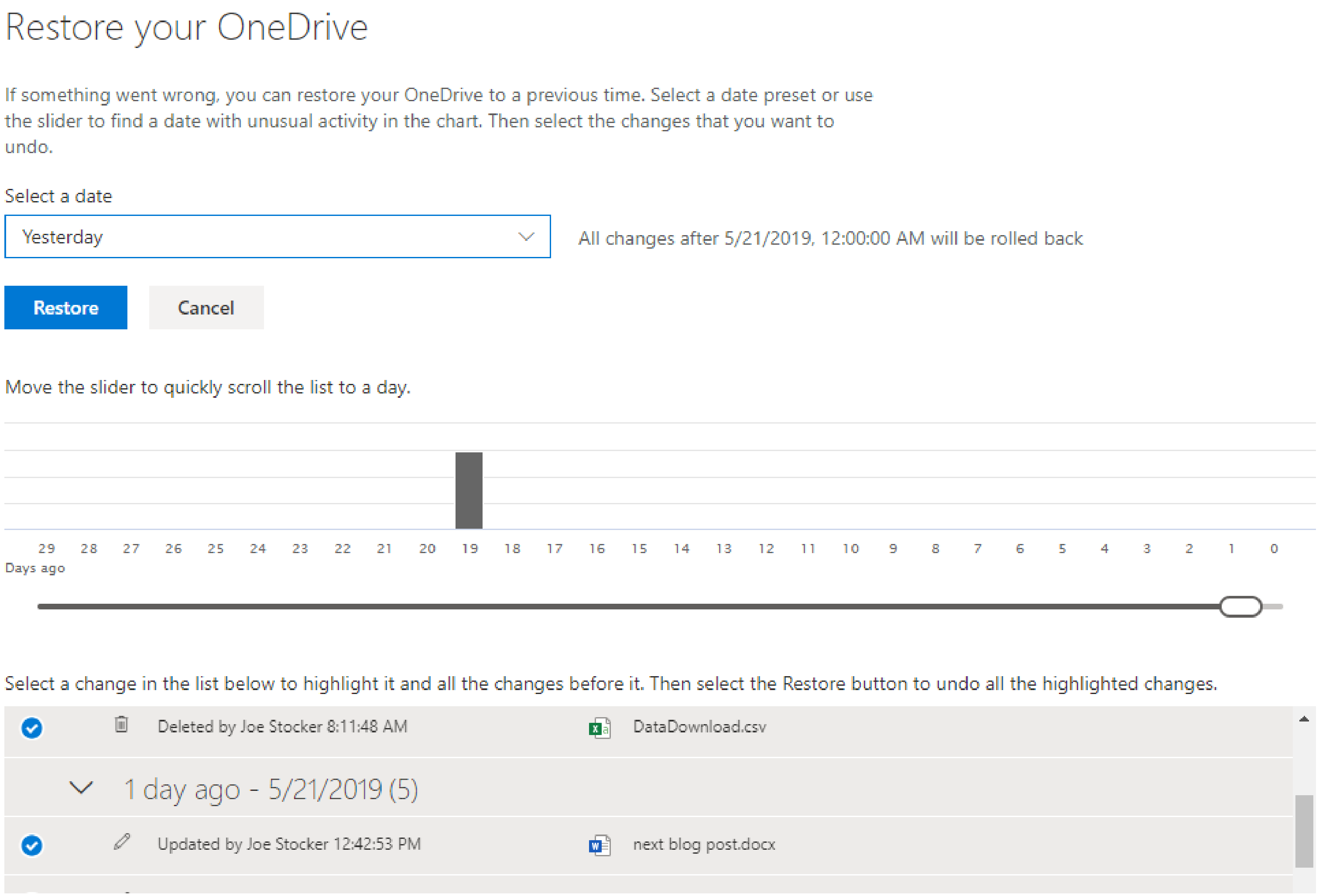
OneDrive

OneDrive settings

Restore your OneDrive

Office 365

View all



Restore your OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find a date with unusual activity in the chart. Then select the changes that you want to undo.

Select a date

Yesterday

All changes after 5/21/2019, 12:00:00 AM will be rolled back

Move the slider to quickly scroll the list to a day.

Select a change in the list below to highlight it and all the changes before it. Then select the Restore button to undo all the highlighted changes.

✓	Deleted by Joe Stocker 8:11:48 AM	DataDownload.csv
	1 day ago - 5/21/2019 (5)	
✓	Updated by Joe Stocker 12:42:53 PM	next blog post.docx

Win10 Controlled Folder Access

- Controlled folder access helps you protect valuable data from malicious apps and threats, such as ransomware.

- All apps (any executable file, including .exe, .scr, .dll files and others) are assessed by Windows Defender Antivirus, which then determines if the app is malicious or safe. If the app is determined to be malicious or suspicious, then it will not be allowed to make changes to any files in any protected folder.

- This is especially useful in helping to protect your documents and information from ransomware that can attempt to encrypt your files and hold them hostage.

- Requirements
  - Windows 10 and Windows Server 2019
  - Windows Defender Antivirus

Ransomware Recommendations

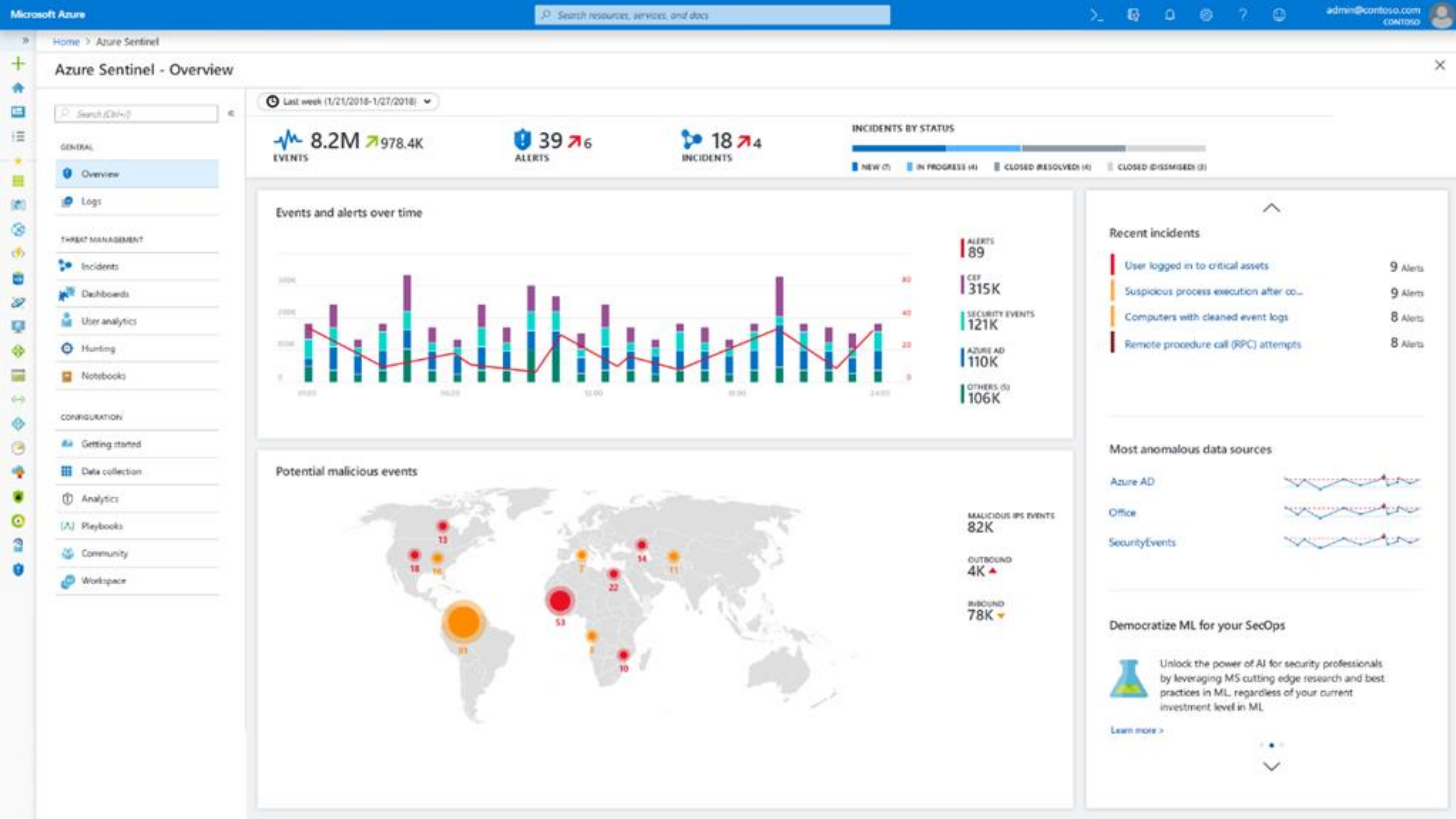
- Test backups as frequently as you are willing to accept data loss (Assume attackers will tamper/disrupt Backups)
    - Recovery Point Objective (RPO) = The amount of acceptable Data Loss. 1 Day? 1 Week? Test backups that often
- **Purchase Cybersecurity Insurance and Cybersecurity Public Relations**
- Have an Incident Response Plan ready (NIST 800-184, NIST 1800-11, and http://aka.ms/IRRG)
- Have a communications plan on how you will communicate with your employees (automated SMS Text solution)
- Microsoft Solutions for Ransomware:
    - Enable Office ATP to scan email for Ransomware
    - Enable Windows 10 Attack Surface Reduction rules to block ransomware
    - Enable Microsoft Defender ATP's EDR to detect ransomware activity (backup deletions)
    - Enable Microsoft Defender ATP "Block at First Site" and learn how to use Machine Isolation
    - Microsoft Cloud App Security can detect Ransomware Uploads (based on file extensions)
    - Backup all laptop data to OneDrive. OneDrive keeps versions of files, so you can restore to previous backup.
    - Backup Server data to Azure which provides versioned restore capabilities
    - Long Term: Consider Windows 10 Controlled Folder Access. It's a white-list to prevent changes to your documents.

Security Issue #9

Too Many Logs

Is your Security Operations Center drowning in log data to find meaningful alerts?

Introducing Azure Sentinel
Microsoft has entered the SIEM Market on 2/28/2019



Azure Sentinel - Overview

8.2M ↗978.4K EVENTS

39 ↗6 ALERTS

18 ↗4 INCIDENTS

INCIDENTS BY STATUS

NEW (7) | IN PROGRESS (4) | CLOSED (RESOLVED) (4) | CLOSED (DISMISSED) (3)

ALERTS 89

CEF 315K

SECURITY EVENTS 121K

AZURE AD 110K

OTHERS (5) 106K

User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

MALICIOUS IPS EVENTS 82K

OUTBOUND 4K ▲

INBOUND 78K ▼

Azure AD

Office

SecurityEvents

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML

Licensing

New Security and Compliance Bundles

"M365 E5 Security" ($12/user/month)

AND/OR

"M365 E5 Compliance" ($10/user/month) (new pricing as of April 1, 2020)

Microsoft Threat Protection

Defender for Identity
Identify suspicious activities & advanced attacks **on premises**.

Defender for Office 365
Zero-day threat and malware protection

Defender for Endpoint
Behavior-based, attack detection
Built-in threat intelligence
Forensic investigation and mitigation

Built into Windows

Threat Intelligence
Attack Simulator, Threat dashboard, Threat Explorer, and Incidents.

Microsoft Cloud App Security
Bring enterprise-grade visibility, control, and protection to your cloud applications.

Azure Active Directory (P2)

Single sign-on to cloud and on-premises applications.
Powerful conditional access
MFA for VPN/RDP
Advanced risk based identity protection with alerts, analysis, & remediation.

New Capabilities
Insider Risk Management
Advanced Auditing
Classification using Machine Learning
Endpoint DLP (uses WIP)
Cloud DLP

O365 Advanced Compliance
Advanced eDiscovery, Information Governance, Customer Lockbox, Customer Key, Privileged Access Management, Records Management, Communication Compliance, Information barriers, DLP for Teams, Advanced Message Encryption

Azure Information Protection (P2)
Automatic Classification and labelling
Encryption for all files and storage locations. Cloud based file tracking and revocation

Key License Dependency
Both these SKUs depend upon M365 E3

Microsoft 365 E5 Compliance offers effective April 1, 2020

Microsoft 365 E5 Compliance $12/u/m NEW PRICE

Pre-req: M365 E3 or Office 365 E3 + EMS E3[1]

NEW OFFER

M365 E5 Info Protection & Governance $7/u/m

- Cloud DLP (MCAS + new value[2])
- Communication DLP (Teams chat)
- Information Governance advanced features (incl. Records Management[2])
- Machine Learning-based auto classification[2]
- Rules-based auto classification
- Customer Key
- Advanced Message Encryption

Pre-req: Any EXO/SPO/ODfB + AIP P1[3,4]

NEW OFFER

M365 E5 Insider Risk Management $6/u/m

- Insider Risk Management[5]
- Communication Compliance[5]
- Information Barriers
- Customer Lockbox
- Privileged Access Management

Pre-req: Any EXO/SPO/ODfB[3]

NEW OFFER

M365 E5 eDiscovery and Audit $6/u/m

- Advanced Audit[5]
- Advanced eDiscovery

Pre-req: Any EXO/SPO/ODfB[3]

Office 365 Enterprise capabilities

APPS

Cloud Productivity & Mobility

Office Pro Plus:

Office apps on up to 5 PCs & Macs

Mobile Office Apps:

Office Apps for Tablet & Smartphones

SERVICES

Rich Communication and Collaboration

Exchange :
Business-class email & Calendar

OneDrive:
Cloud Storage and file sharing

SharePoint:
Team sites & internal portals

Skype for Business:
Online Meetings, IM, video chat

Yammer:
Private social networking

Teams:
Chat Based Workspace

Security and Compliance
DLP, EOP, MFA, OME

SECURITY

Advanced Enterprise Protection

Advanced Threat Protection:
Zero-day threat and malware protection

Office 365 Cloud App Security
Enhanced visibility and control

Customer Lockbox:
Enhanced customer data access controls

Advanced eDiscovery:
Identifying the relevant data quickly

Threat Intelligence + Attack Simulator (New)

Advanced Data Governance

ANALYTICS

Insights for Everyone

Power BI Pro:
Live business analytics and visualization

My Analytics:
Individual and team effectiveness

Workplace Analytics (Add-On)
For organizations 10,000+ Users

VOICE

Complete Cloud Communication

Audio Conferencing:
Worldwide dial-in for your online meetings

Phone System
Business phone system in the cloud

Calling Plan (add-on)
Cost effective cloud based dial tone

Office 365 **E3** ←→ (Apps, Services)

Office 365 **E5** ←→ (all)

Enterprise Mobility & Security capabilities

EMS **E3**

EMS **E5**

Identity and access management	Identity Driven Security	Managed Mobile Productivity	Information Protection
Azure Active Directory Premium P1 Single sign-on to cloud and on-premises applications. Powerful conditional access MFA for On-Premises VPN/RDP Lots more (see other slide)	**Microsoft Advanced Threat Analytics** Identify suspicious activities & advanced attacks **on premises**. Note: This product is now end-of-life and is in a 5-year extended support lifecycle (no new features)	**Microsoft Intune** Mobile device and app management to protect corporate apps and data on any device.	**Azure Information Protection Premium P1** Manual classification and labelling Encryption for all files and storage locations. Cloud based file tracking and revocation
Azure Active Directory Premium P2 Advanced risk based identity protection with alerts, analysis, & remediation.	**Microsoft Cloud App Security & Azure ATP** Bring enterprise-grade visibility, control, and protection to your cloud applications. Azure ATP is the ATA product from E3 but with a cloud back-end		**Azure Information Protection Premium P2** Automated & Intelligent classification, labelling, & encryption for files shared inside & outside your organization

Windows 10 Enterprise capabilities

Windows 10 Enterprise **E5**

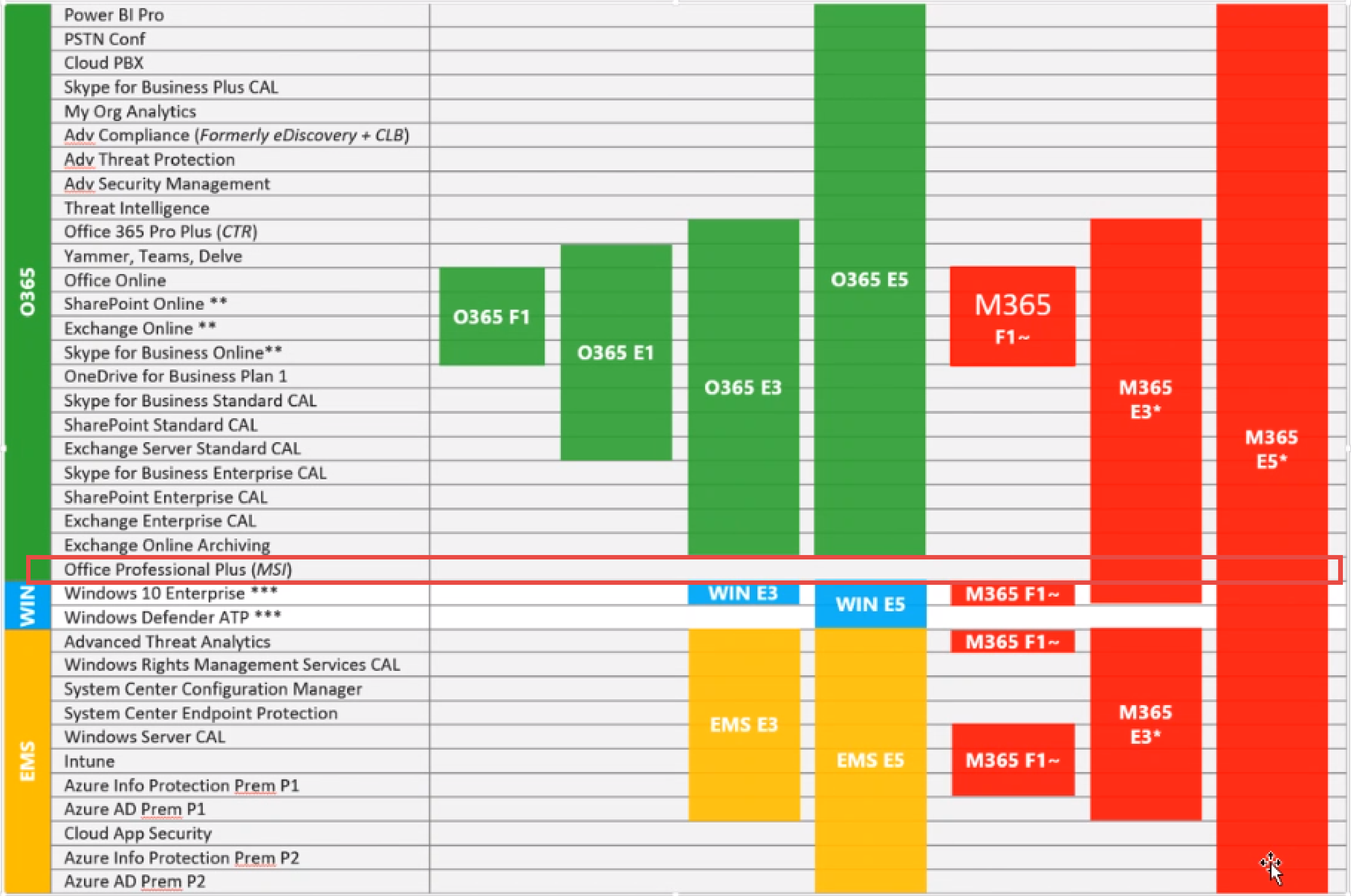
Windows 10 Enterprise **E3**

The most trusted platform	More productive	More personal	The most versatile devices
Windows Information Protection Prevent accidental leaks by separating personal and business data	**Azure Active Directory Join** Streamline IT process by harnessing the power of the cloud	**User Experience Virtualization** (UX-V) OS and app settings synchronized across Windows instances	**Windows 10 for Industry Devices** Turn any inexpensive, off-the-shelf device, into an embedded, handheld, or kiosk experience
Windows Hello for Business Enterprise grade biometric and companion device login	**MDM enablement** Manage all of your devices with the simplicity of MDM	**Granular UX Control** Enterprise control over user experience	
Credential Guard Protects user access tokens in a hardware-isolated container	**Windows Store for Business, Private Catalog** Create a curated store experience for employee self-service		
AppLocker Block unwanted and inappropriate apps from running	**Application Virtualization** (App-V) Simplify app delivery and management		
Device Guard Device locked down to only run fully trusted apps	**Cortana Management** Create, personalize, and manage Cortana profiles through Azure Active Directory		

Advanced Threat Protection
Behavior-based, attack detection
Built-in threat intelligence
Forensic investigation and mitigation
Built into Windows

MDATP for servers as a stand-alone license launches April 1st, 2020 (previously only available through Azure Security Center)

Bundle: MS 365



O365	Power BI Pro				O365 E5			M365 E5*
	PSTN Conf							
	Cloud PBX							
	Skype for Business Plus CAL							
	My Org Analytics							
	Adv Compliance (*Formerly eDiscovery + CLB*)							
	Adv Threat Protection							
	Adv Security Management							
	Threat Intelligence							
	Office 365 Pro Plus (*CTR*)			O365 E3			M365 E3*	
	Yammer, Teams, Delve		O365 E1					
	Office Online	O365 F1				M365 F1~		
	SharePoint Online **							
	Exchange Online **							
	Skype for Business Online**							
	OneDrive for Business Plan 1							
	Skype for Business Standard CAL							
	SharePoint Standard CAL							
	Exchange Server Standard CAL							
	Skype for Business Enterprise CAL							
	SharePoint Enterprise CAL							
	Exchange Enterprise CAL							
	Exchange Online Archiving							
	Office Professional Plus (*MSI*)							
WIN	Windows 10 Enterprise ***			WIN E3	WIN E5	M365 F1~		
	Windows Defender ATP ***							
EMS	Advanced Threat Analytics			EMS E3	EMS E5	M365 F1~	M365 E3*	
	Windows Rights Management Services CAL							
	System Center Configuration Manager							
	System Center Endpoint Protection							
	Windows Server CAL					M365 F1~		
	Intune							
	Azure Info Protection Prem P1							
	Azure AD Prem P1							
	Cloud App Security							
	Azure Info Protection Prem P2							
	Azure AD Prem P2							

M365
Quick Reference

* M365 E3 and M365 E5 include On-Prem Productivity Server Rights, some conditions apply.

** O365 F1 includes K1 and SfB Plan 1.
O365 E1 includes Plan 1.
O365 E3/E5 and M365 E3/E5 include Plan 2.

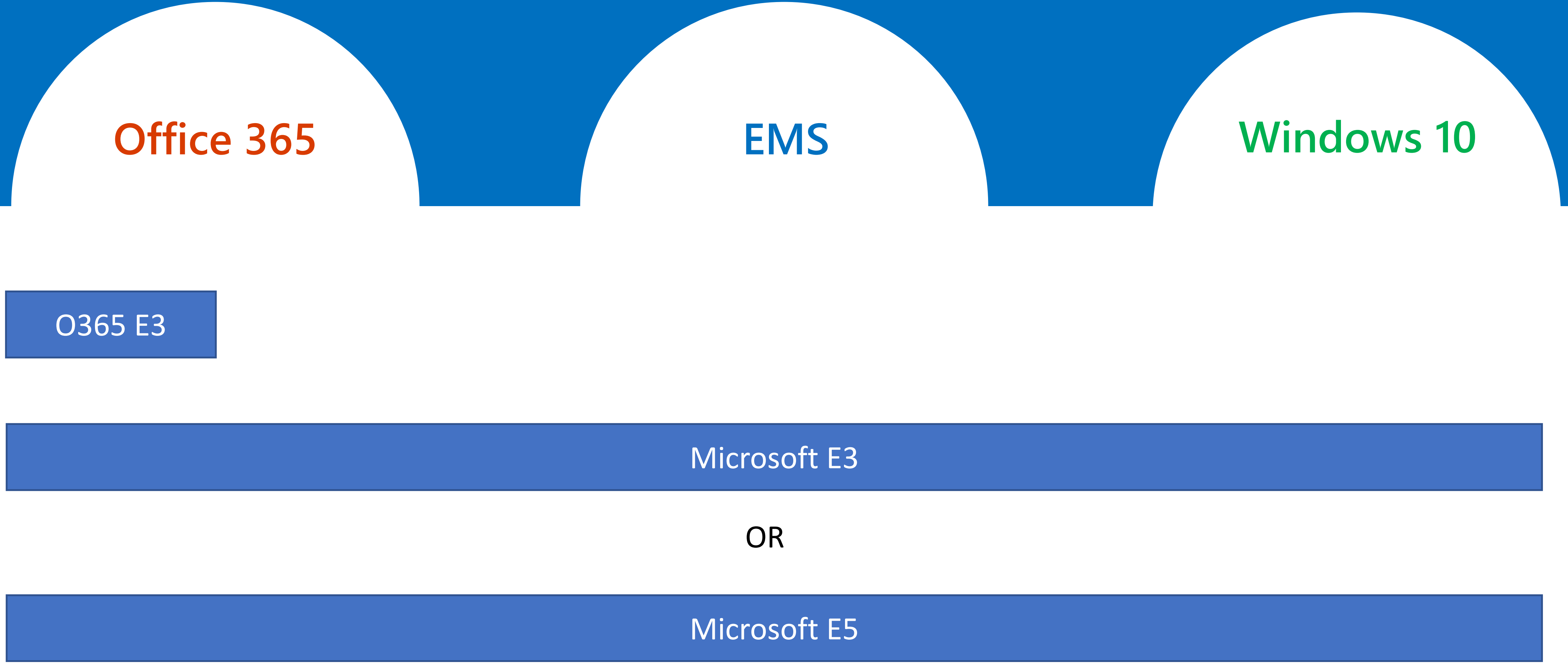
*** Windows 10 Enterprise licenses are upgrade licenses and require a qualifying OS.

~ M365 F1 includes AAD Premium P1, Intune, ATA, and Windows Server CAL (does not include AIP and SCCM ML)

~ M365 F1 is the full Windows 10 Enterprise E3 without reimaging rights, downgrade rights, Enterprise LTSB rights, virtualization rights & customer must use Azure AD-based activation

See Product Terms for details.

“Microsoft 365”
One License that includes all three product families



Office 365

EMS

Windows 10

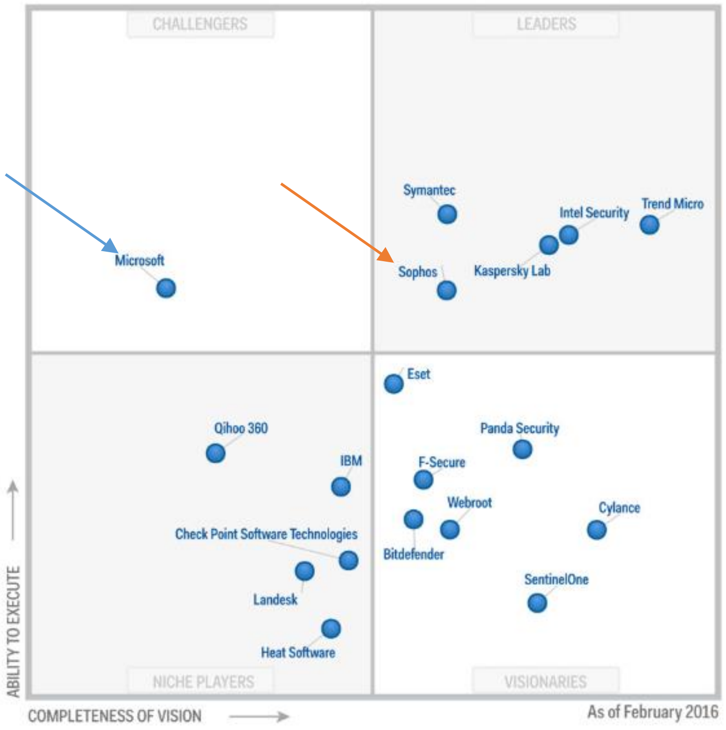
O365 E3

Microsoft E3

OR

Microsoft E5

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (February 2016)

Gartner MQ EPP progression

Figure 1. Magic Quadrant for Endpoint Protection Platforms

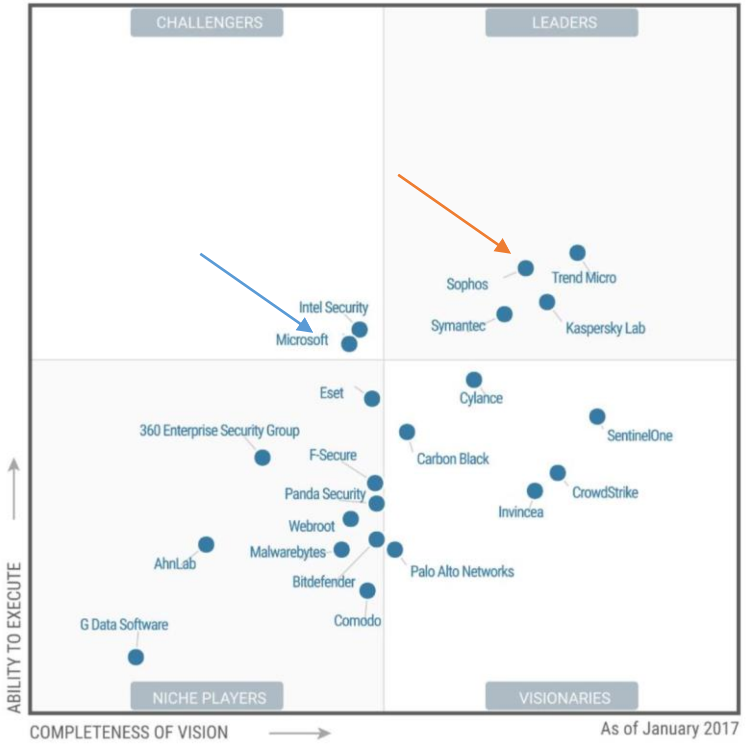
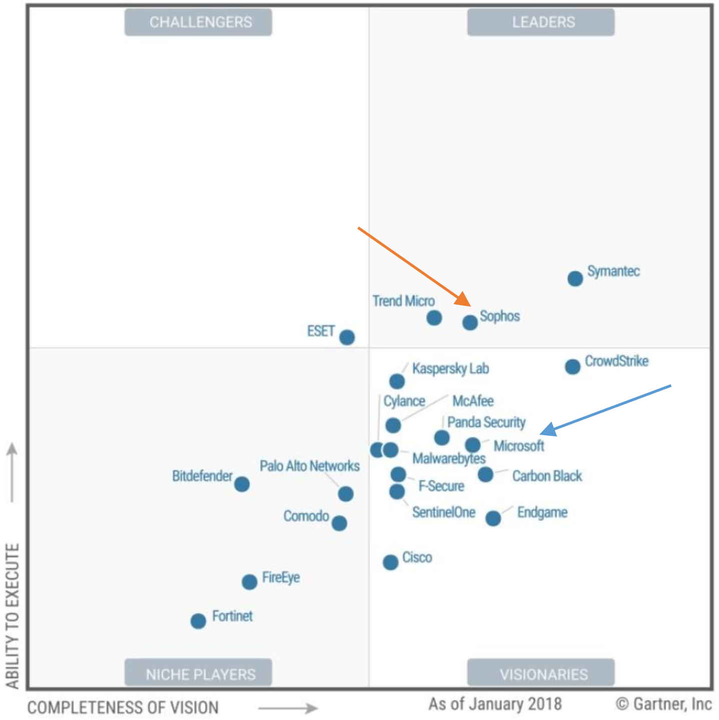
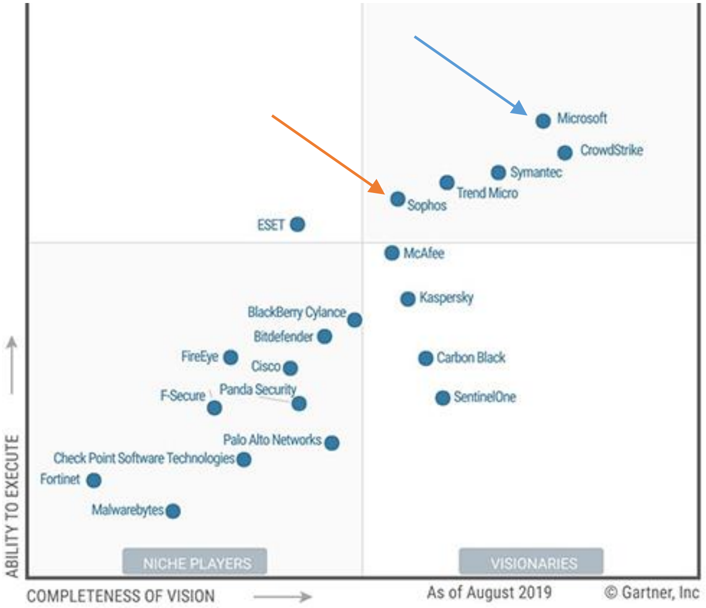
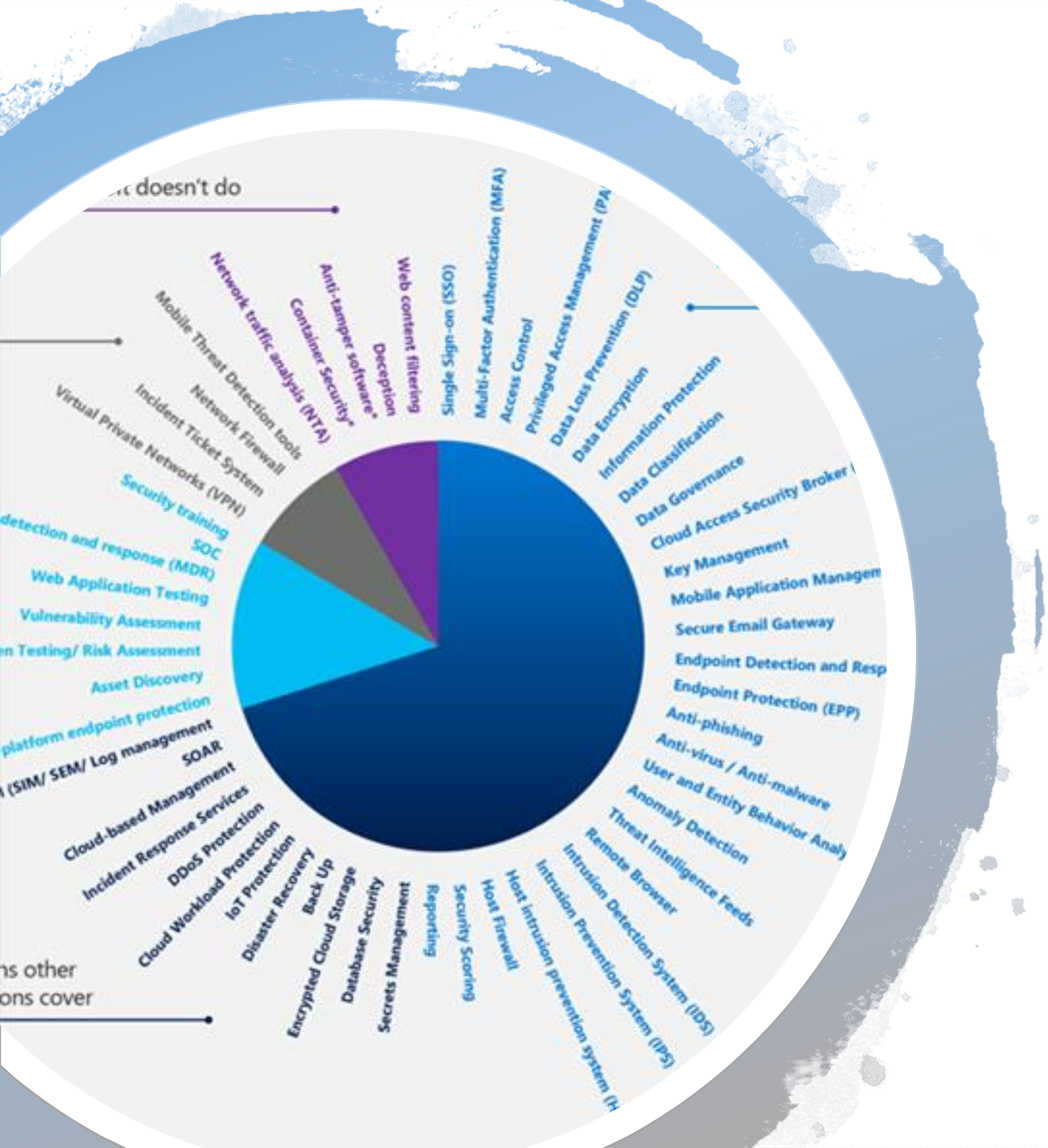


Figure 1. Magic Quadrant for Endpoint Protection Platforms





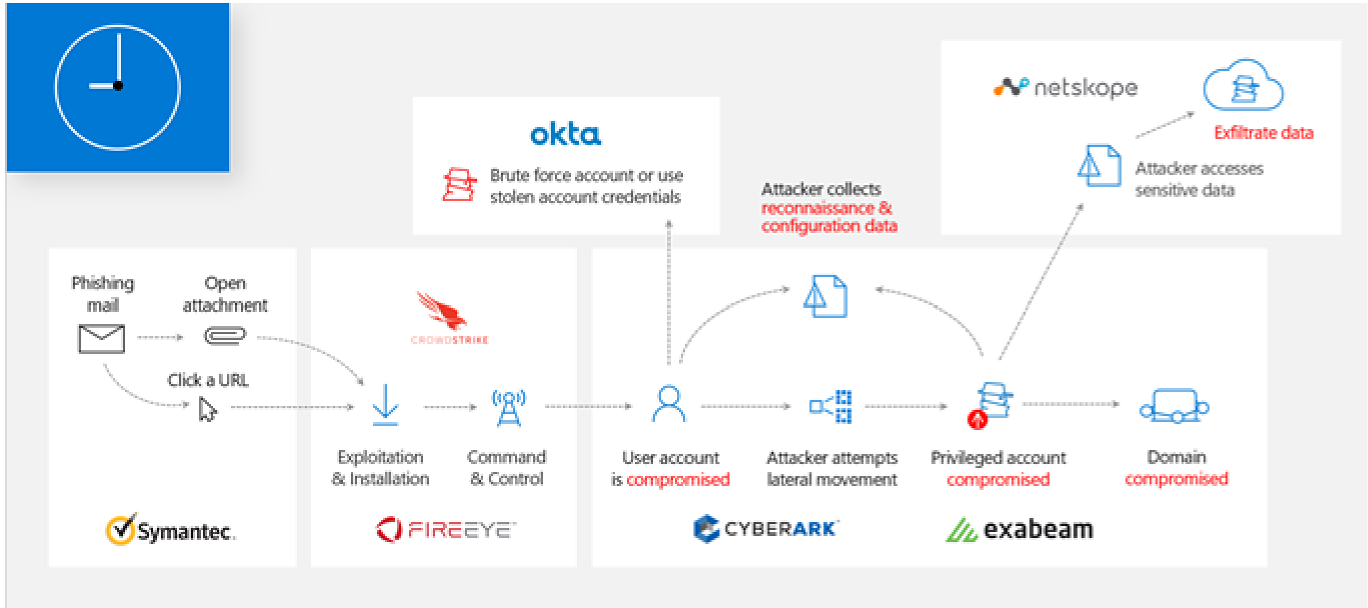


Microsoft 365 E5 Security can replace up to 26 other security vendors

Microsoft Leads in 5 of the Gartner Magic Quadrants

So you no longer need to compromise when consolidating

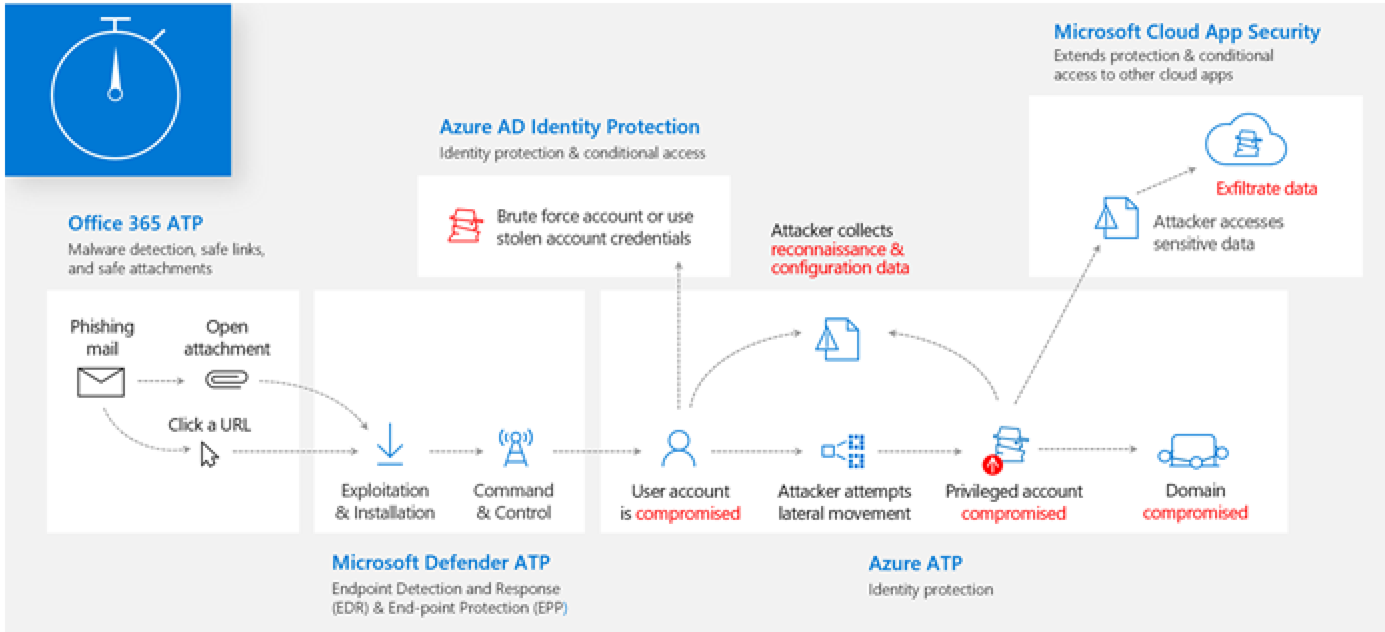
Best of breed vs Vendor Consolidation



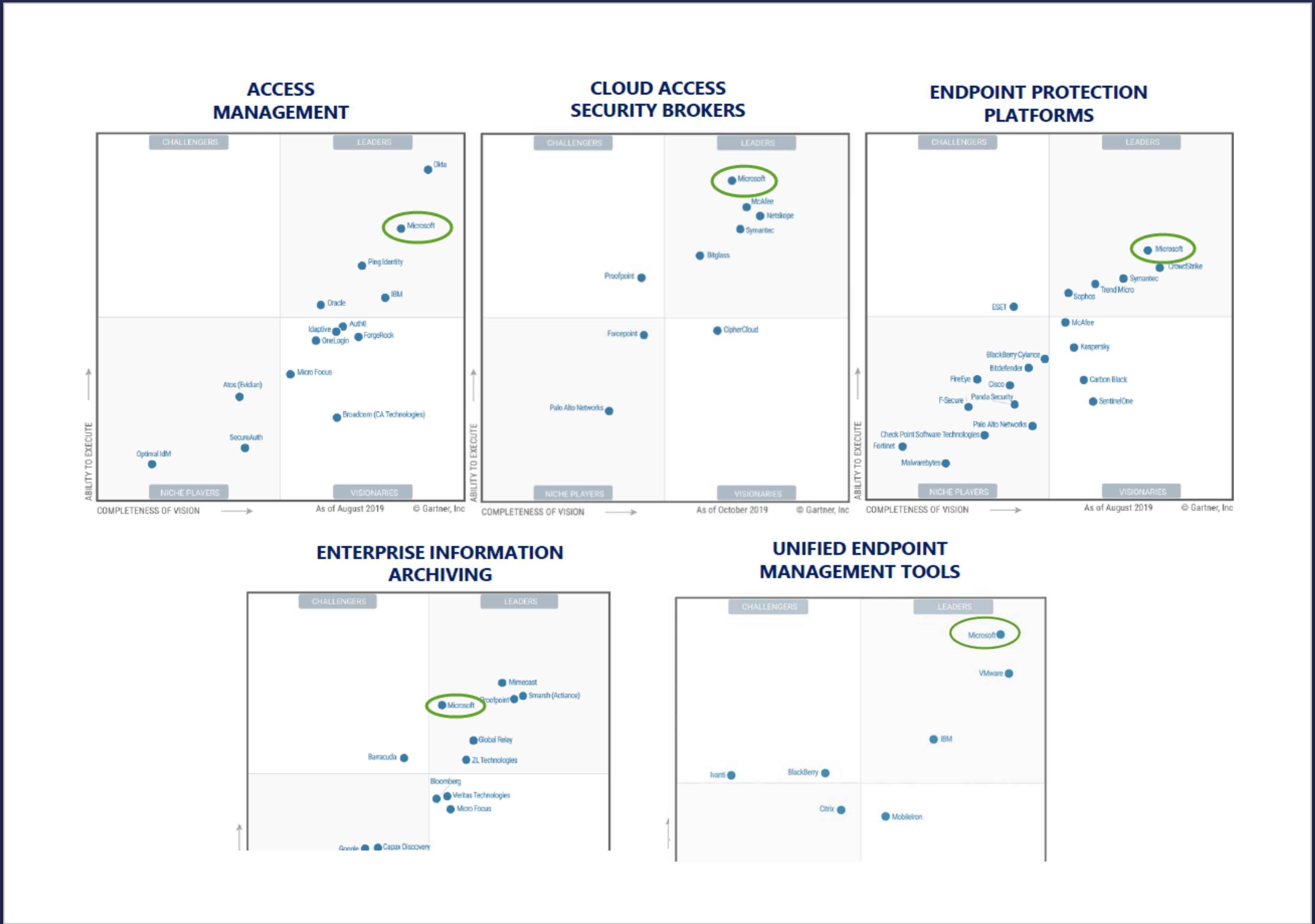
okta
Brute force account or use stolen account credentials
Attacker collects reconnaissance & configuration data
netskope
Exfiltrate data
Attacker accesses sensitive data
Phishing mail
Open attachment
Click a URL
CROWDSTRIKE
Exploitation & Installation
Command & Control
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised
Symantec.
FIREEYE
CYBERARK
exabeam

- Multiple contract renewals to negotiate
- Multiple vendor relationships to manage
- Multiple skill sets to train IT
- Loss of fidelity during integration
- Lack of holistic strategy
- More expensive
- Longer Median Time to Respond (IR) Investigations

- One Contract
- More common skill set to find for staffing (MS-500 Certification)
- Tight Integration and Signal Sharing
- Unified Administration
- Automation and Orchestration built-in
- Faster Investigations
- Better ROI and TCO



Microsoft Cloud App Security
Extends protection & conditional access to other cloud apps
Azure AD Identity Protection
Identity protection & conditional access
Brute force account or use stolen account credentials
Attacker collects reconnaissance & configuration data
Exfiltrate data
Attacker accesses sensitive data
Office 365 ATP
Malware detection, safe links, and safe attachments
Phishing mail
Open attachment
Click a URL
Exploitation & Installation
Command & Control
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised
Microsoft Defender ATP
Endpoint Detection and Response (EDR) & End-point Protection (EPP)
Azure ATP
Identity protection



Consolidating doesn’t mean compromising

Microsoft

Microsoft Ignite 2020 Recap

Subtitle or speaker name

Microsoft

Branding Changes

- **Microsoft Threat Protection has been rebranded as "Microsoft 365 Defender"**
  - **This name change reflects that Azure Security Center is now included in this new SKU for "Microsoft 365 Defender"**
- **Microsoft Defender Advanced Threat Protection has been rebranded as "Microsoft Defender for Endpoint"**

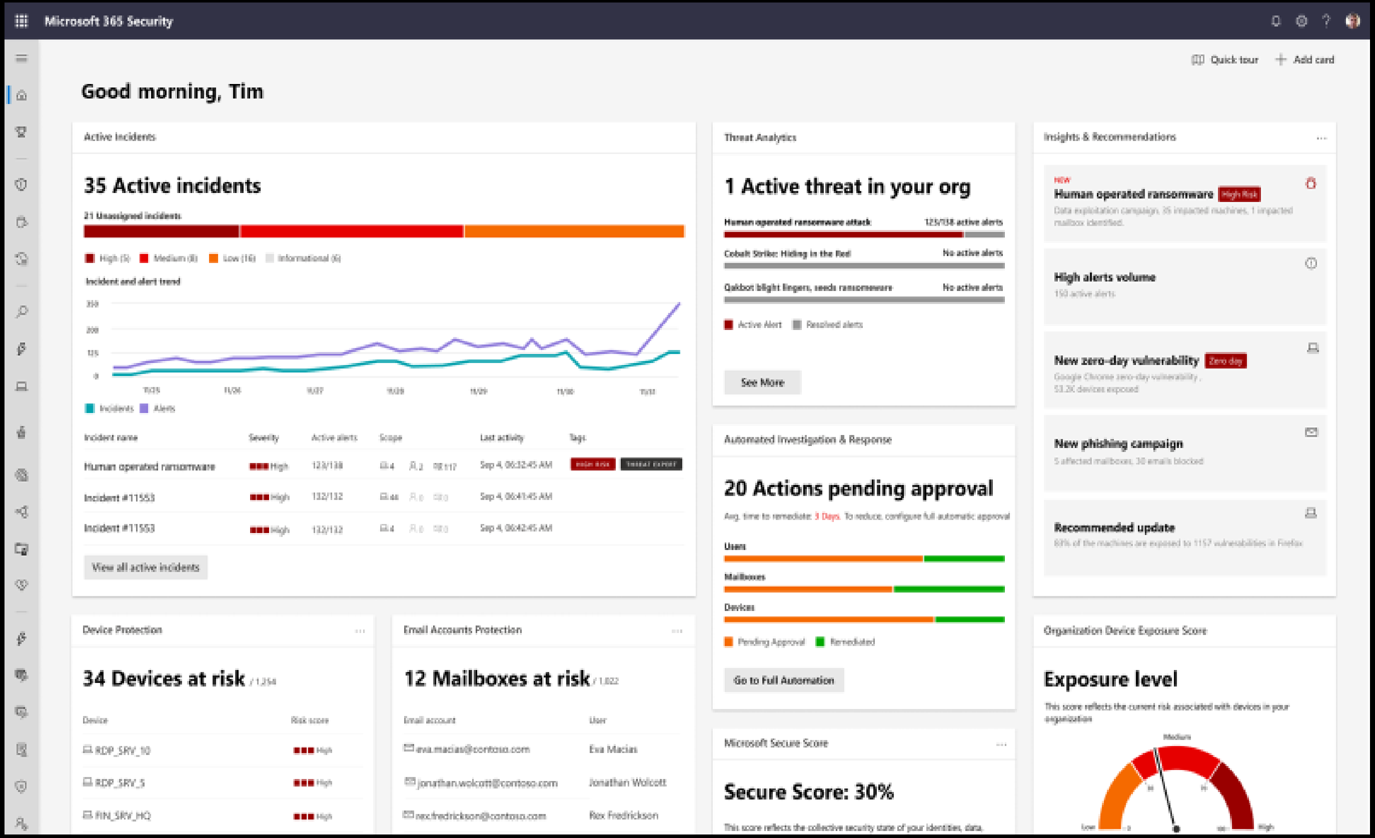
  This branding change reflects Microsoft's investments in Mobile protection:
  - **For Android, it provides protection against phishing, offers proactive scanning of malicious applications and files, blocks access to corporate resources to mitigate the impact of breaches, and gives security teams visibility into mobile threats and alerts via the security center.**
  - **For iOS, customers will also get phishing and web protection and the same unified SecOps experience.**
  - **Support for macOS has been expanded with the public preview of threat and vulnerability management.**
- Office 365 Advanced Threat Protection has been rebranded as "**Microsoft Defender for Office 365"**
- Azure Advanced Threat Protection has been rebranded as "**Microsoft Defender for Identity**"
- Azure Security Center is now "**Azure Defender"**
- **Azure Sentinel remains linked to "Microsoft 365 Defender" in the sense that any telemetry from O365 is free to ingest into Sentinel, but customers are still responsible for extra storage fees.**

Microsoft Defender XDR

XDR = “Extended Detection and Response”

This is not a SKU/License

This reflects the extended protection linking Azure and Office 365



Good morning, Tim

Active Incidents

35 Active incidents

21 Unassigned incidents

🟥 High (5) 🟥 Medium (8) 🟧 Low (16) ▨ Informational (6)

Incident name	Severity	Active alerts	Scope	Last activity	Tags
Human operated ransomware	High	123/138	4 2 117	Sep 4, 06:32:45 AM	HIGH RISK THREAT EXPERT
Incident #11553	High	132/132	44 0 0	Sep 4, 06:41:45 AM	
Incident #11553	High	132/132	4 0 0	Sep 4, 06:42:45 AM	

View all active incidents

Threat Analytics

1 Active threat in your org

Human operated ransomware attack 123/138 active alerts

Cobalt Strike: Hiding in the Red No active alerts

Qakbot blight lingers, seeds ransomeware No active alerts

See More

Insights & Recommendations

NEW

Human operated ransomware High Risk

Data exploitation campaign, 35 impacted machines, 1 impacted mailbox identified.

High alerts volume

150 active alerts

New zero-day vulnerability Zero day

Google Chrome zero-day vulnerability , 53.2K devices exposed

New phishing campaign

5 affected mailboxes, 30 emails blocked

Recommended update

83% of the machines are exposed to 1157 vulnerabilities in Firefox

Automated Investigation & Response

20 Actions pending approval

Avg. time to remediate: 3 Days. To reduce, configure full automatic approval

Users

Mailboxes

Devices

Go to Full Automation

Device Protection

34 Devices at risk / 1,254

Device	Risk score
RDP_SRV_10	High
RDP_SRV_5	High
FIN_SRV_HQ	High

Email Accounts Protection

12 Mailboxes at risk / 1,022

Email account	User
eva.macias@contoso.com	Eva Macias
jonathan.wolcott@contoso.com	Jonathan Wolcott
rex.fredrickson@contoso.com	Rex Fredrickson

Microsoft Secure Score

Secure Score: 30%

This score reflects the collective security state of your identities, data,

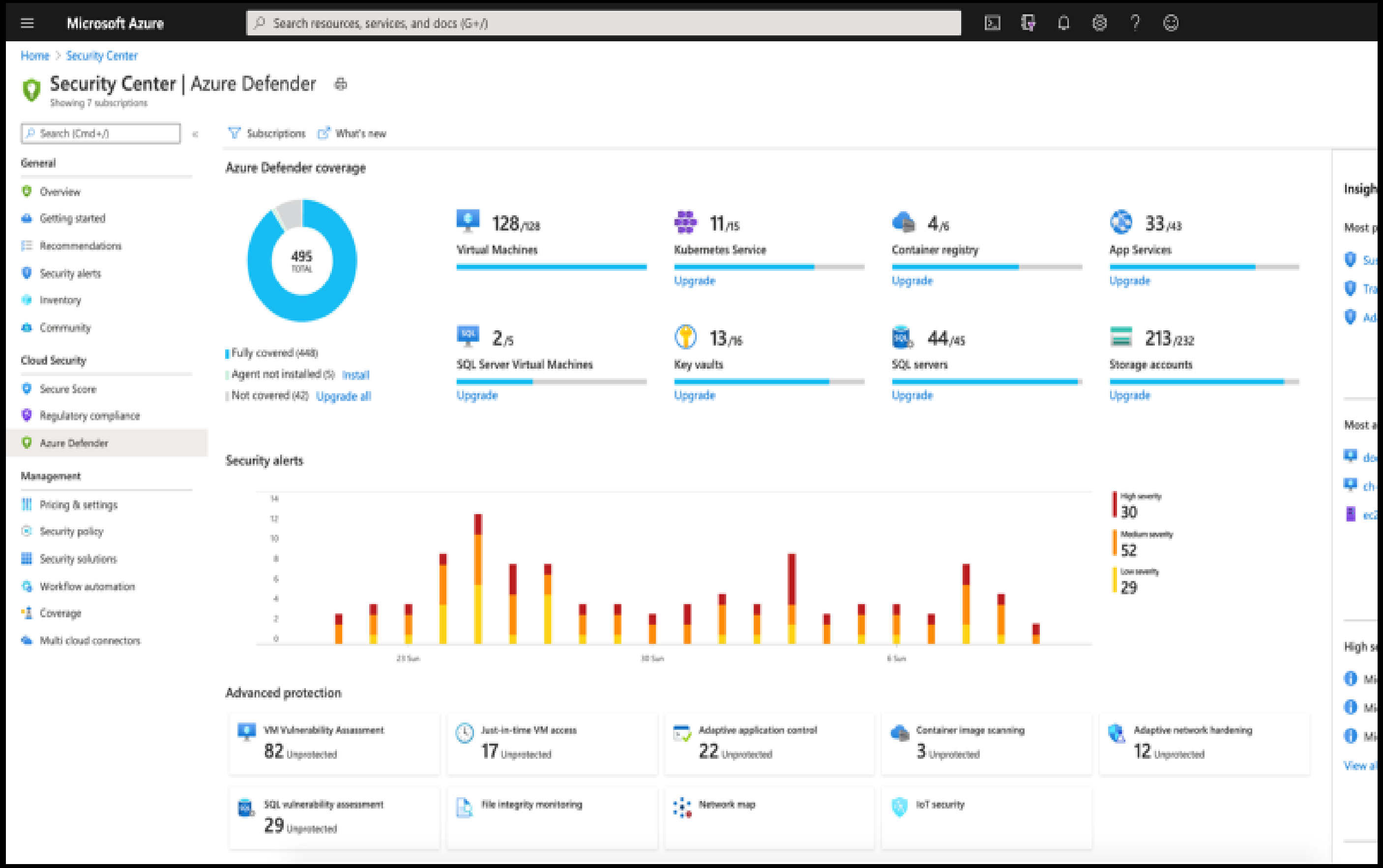
Organization Device Exposure Score

Exposure level

This score reflects the current risk associated with devices in your organization

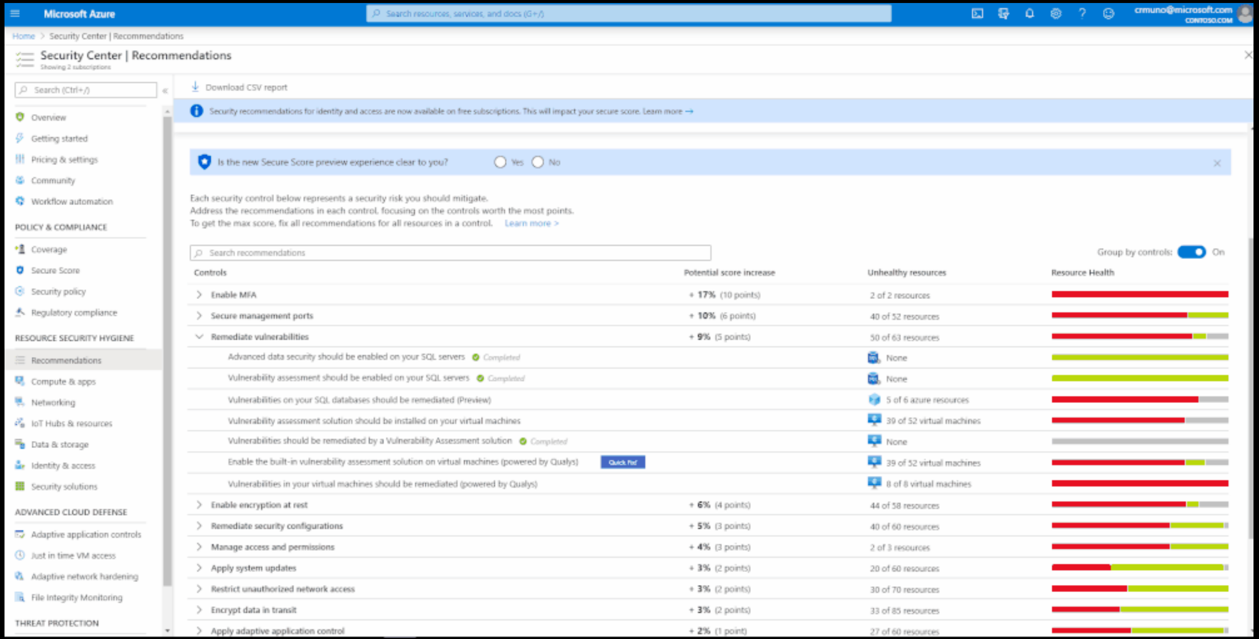
Azure Defender

(Formerly Azure Security Center)


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Security Center
Security Center | Azure Defender
Showing 7 subscriptions
Search (Cmd+/)
General
Overview
Getting started
Recommendations
Security alerts
Inventory
Community
Cloud Security
Secure Score
Regulatory compliance
Azure Defender
Management
Pricing & settings
Security policy
Security solutions
Workflow automation
Coverage
Multi cloud connectors
Subscriptions
What's new
Azure Defender coverage
495 TOTAL
Fully covered (448)
Agent not installed (5) Install
Not covered (42) Upgrade all
128/128 Virtual Machines
11/15 Kubernetes Service Upgrade
4/6 Container registry Upgrade
33/43 App Services Upgrade
2/5 SQL Server Virtual Machines Upgrade
13/16 Key vaults Upgrade
44/45 SQL servers Upgrade
213/232 Storage accounts Upgrade
Security alerts
High severity 30
Medium severity 52
Low severity 29
Advanced protection
VM Vulnerability Assessment 82 Unprotected
Just-in-time VM access 17 Unprotected
Adaptive application control 22 Unprotected
Container image scanning 3 Unprotected
Adaptive network hardening 12 Unprotected
SQL vulnerability assessment 29 Unprotected
File integrity monitoring
Network map
IoT security
Insigh
View a

Azure Defender (Continued)

(Formerly Azure Security Center) enhancements include multi-cloud posture management with Azure Arc, Azure Defender and Azure Security Center Inventory



Security Center | Recommendations
Showing 2 subscriptions

Security recommendations for identity and access are now available on free subscriptions. This will impact your secure score. Learn more →

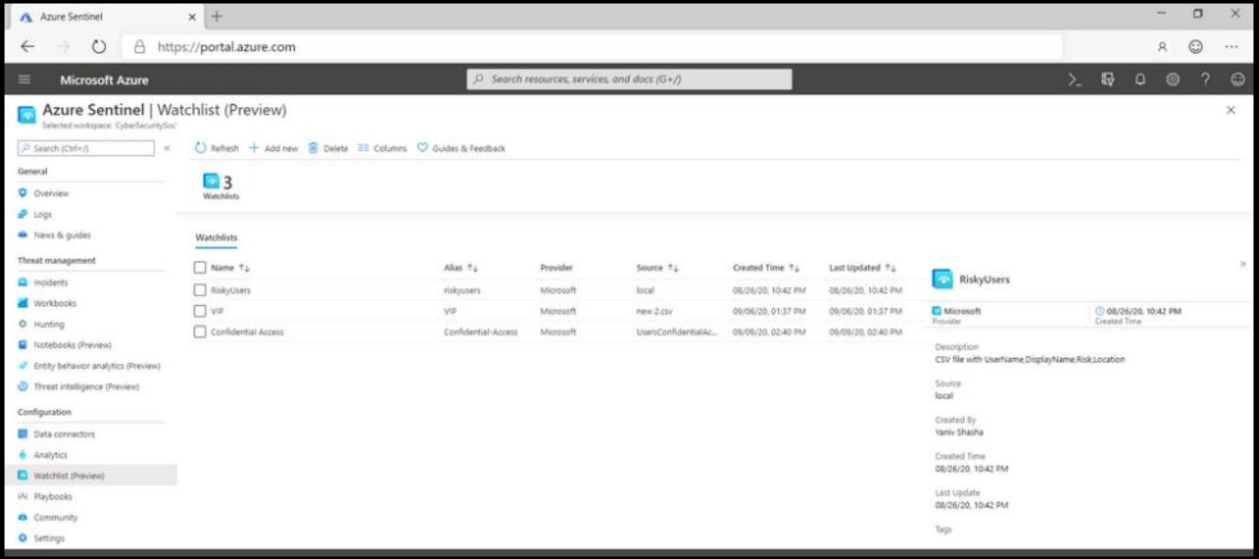
Is the new Secure Score preview experience clear to you? ○ Yes ○ No

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. Learn more >

Controls	Potential score increase	Unhealthy resources	Resource Health
Enable MFA	+ **17%** (10 points)	2 of 2 resources	
Secure management ports	+ **10%** (6 points)	40 of 52 resources	
Remediate vulnerabilities	+ **9%** (5 points)	50 of 63 resources	
Advanced data security should be enabled on your SQL servers ✓ Completed		None	
Vulnerability assessment should be enabled on your SQL servers ✓ Completed		None	
Vulnerabilities on your SQL databases should be remediated (Preview)		5 of 6 azure resources	
Vulnerability assessment solution should be installed on your virtual machines		39 of 52 virtual machines	
Vulnerabilities should be remediated by a Vulnerability Assessment solution ✓ Completed		None	
Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys)		39 of 52 virtual machines	
Vulnerabilities in your virtual machines should be remediated (powered by Qualys)		8 of 8 virtual machines	
Enable encryption at rest	+ **6%** (4 points)	44 of 58 resources	
Remediate security configurations	+ **5%** (3 points)	40 of 60 resources	
Manage access and permissions	+ **4%** (3 points)	2 of 3 resources	
Apply system updates	+ **3%** (2 points)	20 of 60 resources	
Restrict unauthorized network access	+ **3%** (2 points)	30 of 70 resources	
Encrypt data in transit	+ **3%** (2 points)	33 of 85 resources	
Apply adaptive application control	+ **2%** (1 point)	27 of 60 resources	

Azure Sentinel

Stay ahead of threats with new innovations from Azure Sentinel including User and Entity Behavior Analytics, Threat Intelligence enhancements



Azure Sentinel | Watchlist (Preview)

Selected workspace: 'CyberSecuritySoc'

3 Watchlists

Watchlists

Name	Alias	Provider	Source	Created Time	Last Updated
RiskyUsers	riskyusers	Microsoft	local	08/26/20, 10:42 PM	08/26/20, 10:42 PM
VIP	VIP	Microsoft	new 2.csv	09/06/20, 01:37 PM	09/06/20, 01:37 PM
Confidential Access	Confidential-Access	Microsoft	UsersConfidentialAc...	09/09/20, 02:40 PM	09/09/20, 02:40 PM

RiskyUsers

Microsoft
Provider

08/26/20, 10:42 PM
Created Time

Description
CSV file with UserName,DisplayName,Risk,Location

Source
local

Created By
Yaniv Shasha

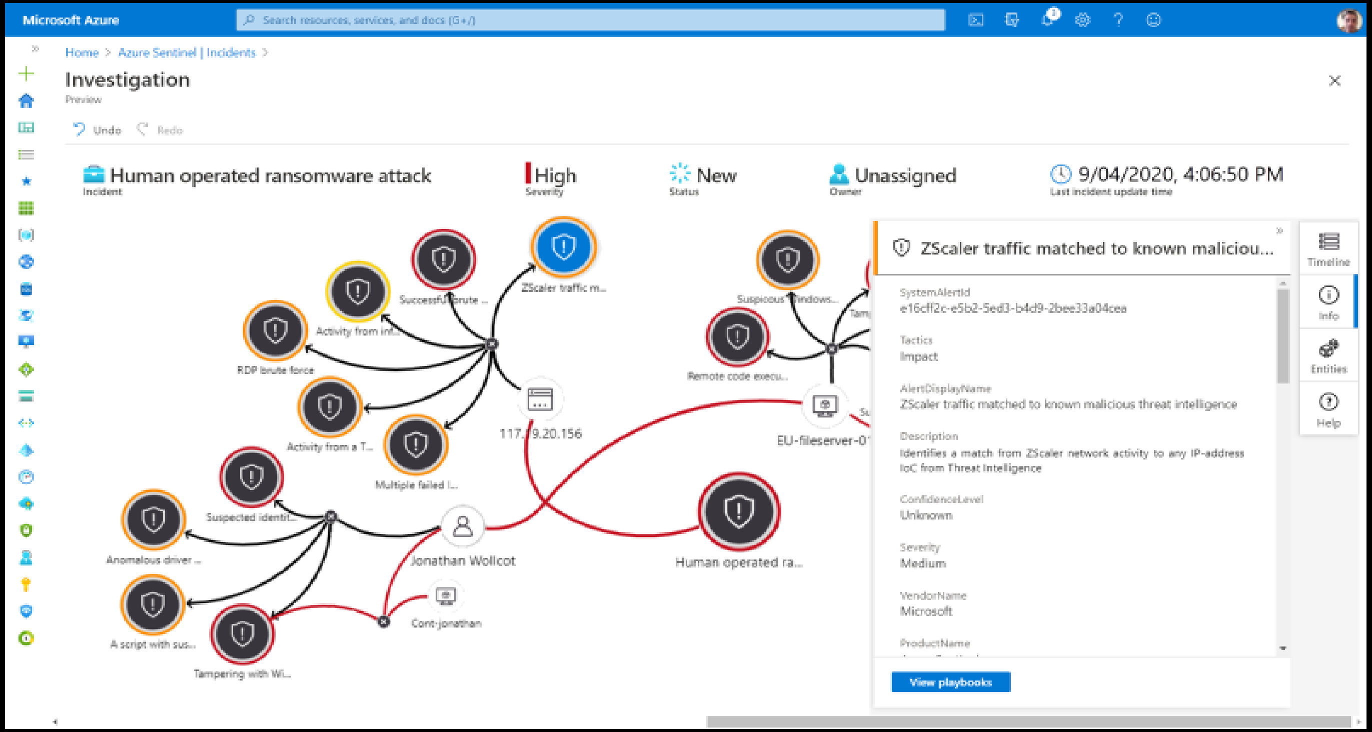
Created Time
08/26/20, 10:42 PM

Last Update
08/26/20, 10:42 PM

Tags

Azure Sentinel Integration

With Microsoft Defender XDR



Investigation
Preview

Human operated ransomware attack
Incident

High
Severity

New
Status

Unassigned
Owner

9/04/2020, 4:06:50 PM
Last incident update time

ZScaler traffic matched to known maliciou...

SystemAlertId
e16cff2c-e5b2-5ed3-b4d9-2bee33a04cea

Tactics
Impact

AlertDisplayName
ZScaler traffic matched to known malicious threat intelligence

Description
Identifies a match from ZScaler network activity to any IP-address IoC from Threat Intelligence

ConfidenceLevel
Unknown

Severity
Medium

VendorName
Microsoft

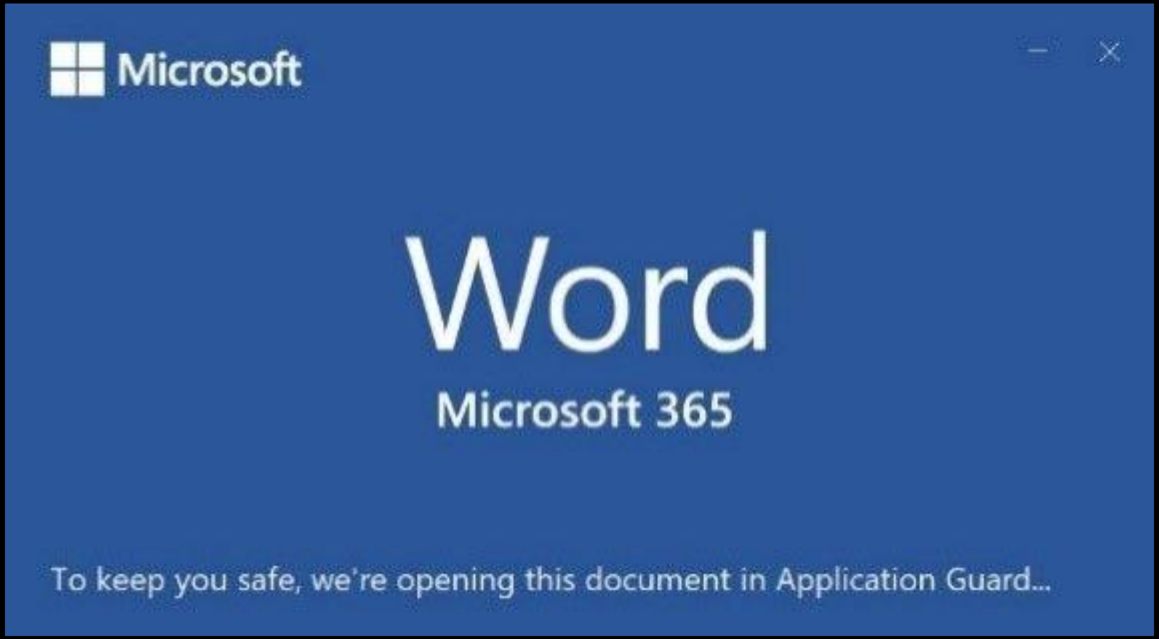
ProductName

Application Guard

Formerly "Safe Documents"

Opens Office Documents in Sandbox

Relies on Microsoft Defender for Endpoint

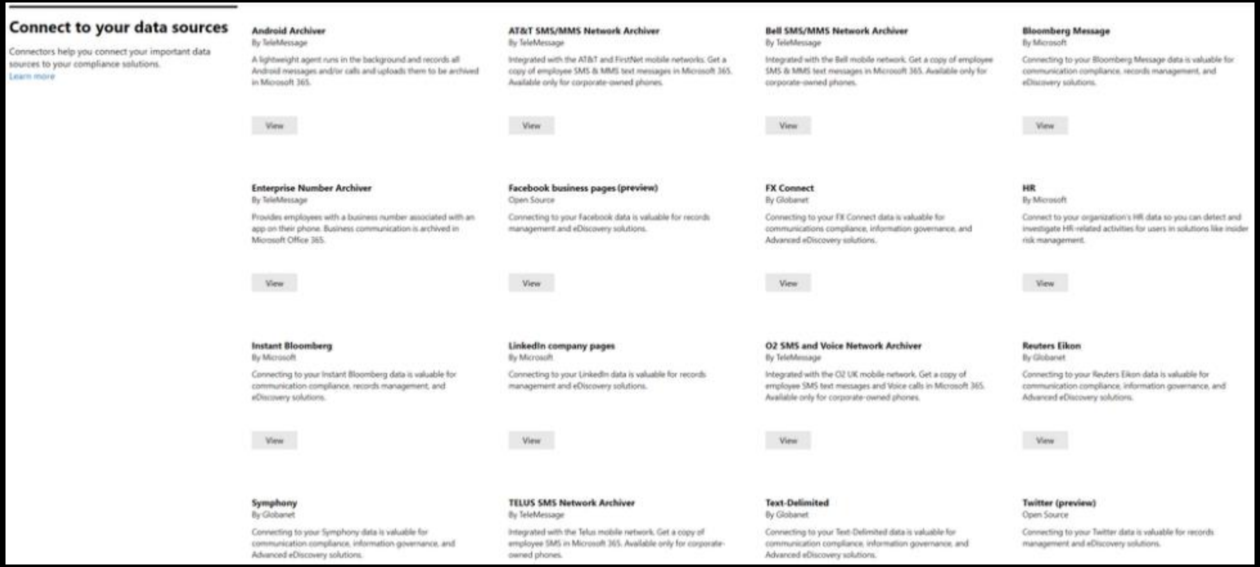


To keep you safe, we're opening this document in Application Guard...

Microsoft Cloud App Security

MCAS and Sentinel were the only two security products not rebranded

New Feature: Public preview of data loss prevention capabilities extended to Microsoft Cloud App Security (MCAS)



Connect to your data sources

Connectors help you connect your important data sources to your compliance solutions.
Learn more

Android Archiver
By TeleMessage
A lightweight agent runs in the background and records all Android messages and/or calls and uploads them to be archived in Microsoft 365.

AT&T SMS/MMS Network Archiver
By TeleMessage
Integrated with the AT&T and FirstNet mobile networks. Get a copy of employee SMS & MMS text messages in Microsoft 365. Available only for corporate-owned phones.

Bell SMS/MMS Network Archiver
By TeleMessage
Integrated with the Bell mobile network. Get a copy of employee SMS & MMS text messages in Microsoft 365. Available only for corporate-owned phones.

Bloomberg Message
By Microsoft
Connecting to your Bloomberg Message data is valuable for communication compliance, records management, and eDiscovery solutions.

Enterprise Number Archiver
By TeleMessage
Provides employees with a business number associated with an app on their phone. Business communication is archived in Microsoft Office 365.

Facebook business pages (preview)
Open Source
Connecting to your Facebook data is valuable for records management and eDiscovery solutions.

FX Connect
By Globanet
Connecting to your FX Connect data is valuable for communications compliance, information governance, and Advanced eDiscovery solutions.

HR
By Microsoft
Connect to your organization's HR data so you can detect and investigate HR-related activities for users in solutions like insider risk management.

Instant Bloomberg
By Microsoft
Connecting to your Instant Bloomberg data is valuable for communication compliance, records management, and eDiscovery solutions.

LinkedIn company pages
By Microsoft
Connecting to your LinkedIn data is valuable for records management and eDiscovery solutions.

O2 SMS and Voice Network Archiver
By TeleMessage
Integrated with the O2 UK mobile network. Get a copy of employee SMS text messages and Voice calls in Microsoft 365. Available only for corporate-owned phones.

Reuters Eikon
By Globanet
Connecting to your Reuters Eikon data is valuable for communication compliance, information governance, and Advanced eDiscovery solutions.

Symphony
By Globanet
Connecting to your Symphony data is valuable for communication compliance, information governance, and Advanced eDiscovery solutions.

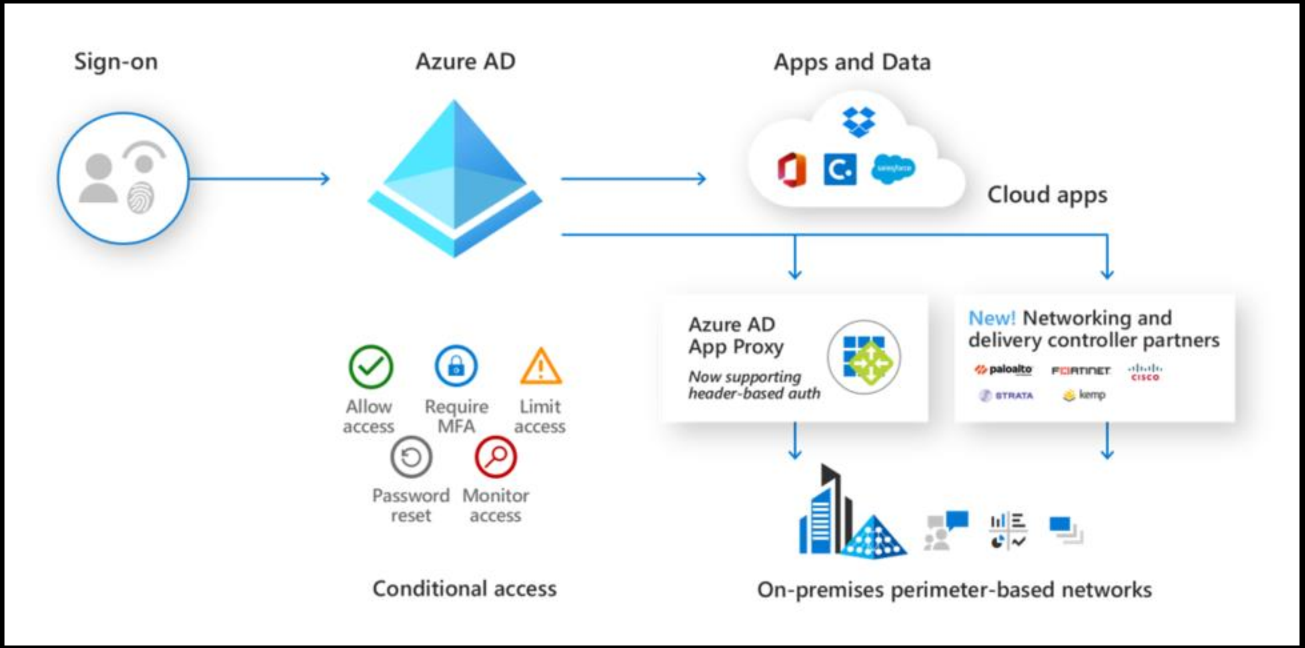
TELUS SMS Network Archiver
By TeleMessage
Integrated with the Telus mobile network. Get a copy of employee SMS in Microsoft 365. Available only for corporate-owned phones.

Text-Delimited
By Globanet
Connecting to your Text-Delimited data is valuable for communication compliance, information governance, and Advanced eDiscovery solutions.

Twitter (preview)
Open Source
Connecting to your Twitter data is valuable for records management and eDiscovery solutions.

Azure AD App Proxy

New Azure AD Application Proxy capabilities, partner* integrations extend secure, seamless access to virtually all legacy apps

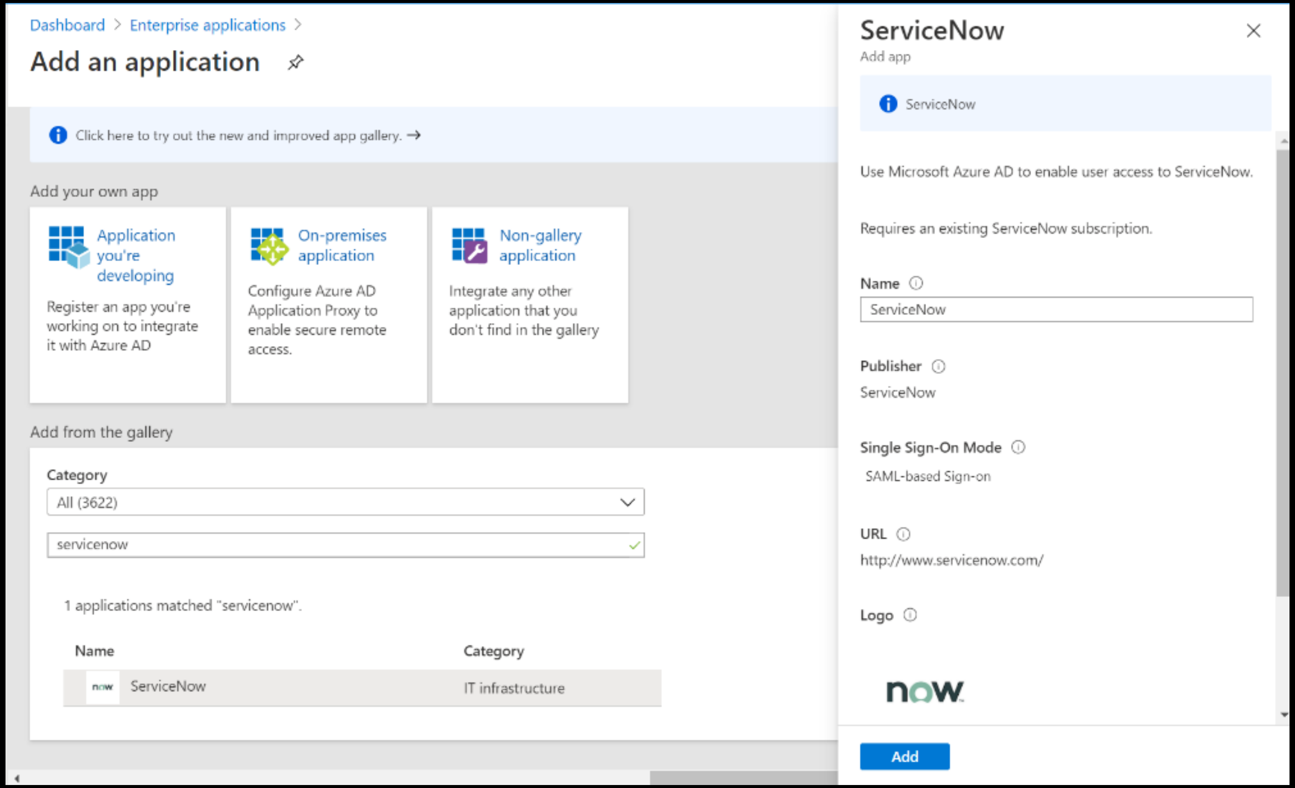


***F5, Citrix, Cisco AnyConnect, Fortinet, Kemp, Palo Alto Networks, and Strata.**

Azure AD Integrations

Better user lifecycle management with deep integrations between Azure AD and popular SaaS apps ServiceNow, Adobe

139 Apps now support automated provisioning



Dashboard > Enterprise applications >

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

Application you're developing

Register an app you're working on to integrate it with Azure AD

On-premises application

Configure Azure AD Application Proxy to enable secure remote access.

Non-gallery application

Integrate any other application that you don't find in the gallery

Add from the gallery

Category: All (3622)

servicenow

1 applications matched "servicenow".

Name	Category
ServiceNow	IT infrastructure

ServiceNow

Add app

ServiceNow

Use Microsoft Azure AD to enable user access to ServiceNow.

Requires an existing ServiceNow subscription.

Name: ServiceNow

Publisher: ServiceNow

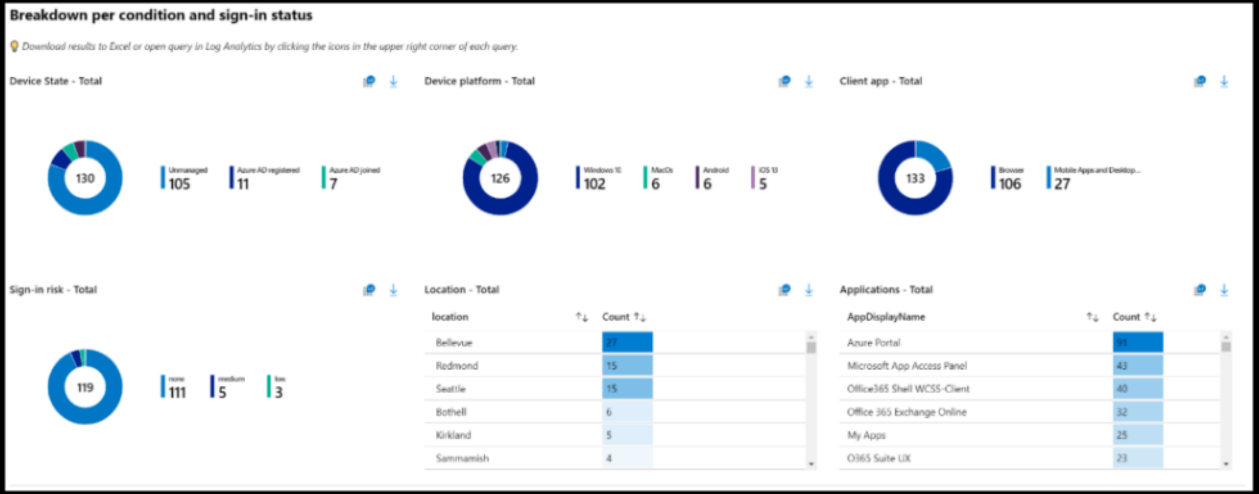
Single Sign-On Mode: SAML-based Sign-on

URL: http://www.servicenow.com/

Logo

Azure AD Conditional Access

Azure AD Conditional Access enhancements to manage policies at scale, improve security posture



Breakdown per condition and sign-in status

💡 *Download results to Excel or open query in Log Analytics by clicking the icons in the upper right corner of each query.*

Location - Total

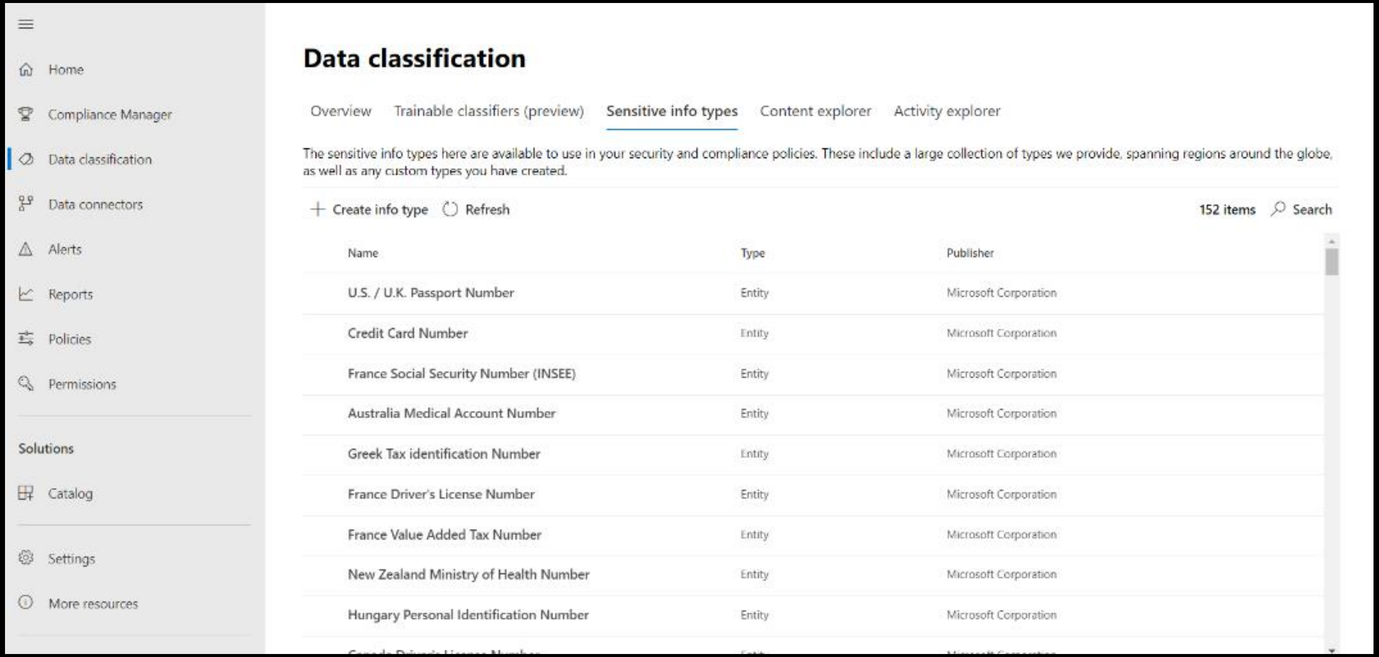
location ↑↓	Count ↑↓
Bellevue	27
Redmond	15
Seattle	15
Bothell	6
Kirkland	5
Sammamish	4

Applications - Total

AppDisplayName ↑↓	Count ↑↓
Azure Portal	91
Microsoft App Access Panel	43
Office365 Shell WCSS-Client	40
Office 365 Exchange Online	32
My Apps	25
O365 Suite UX	23

Microsoft Information Protection

Additional Sensitive Information Types



Data classification

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

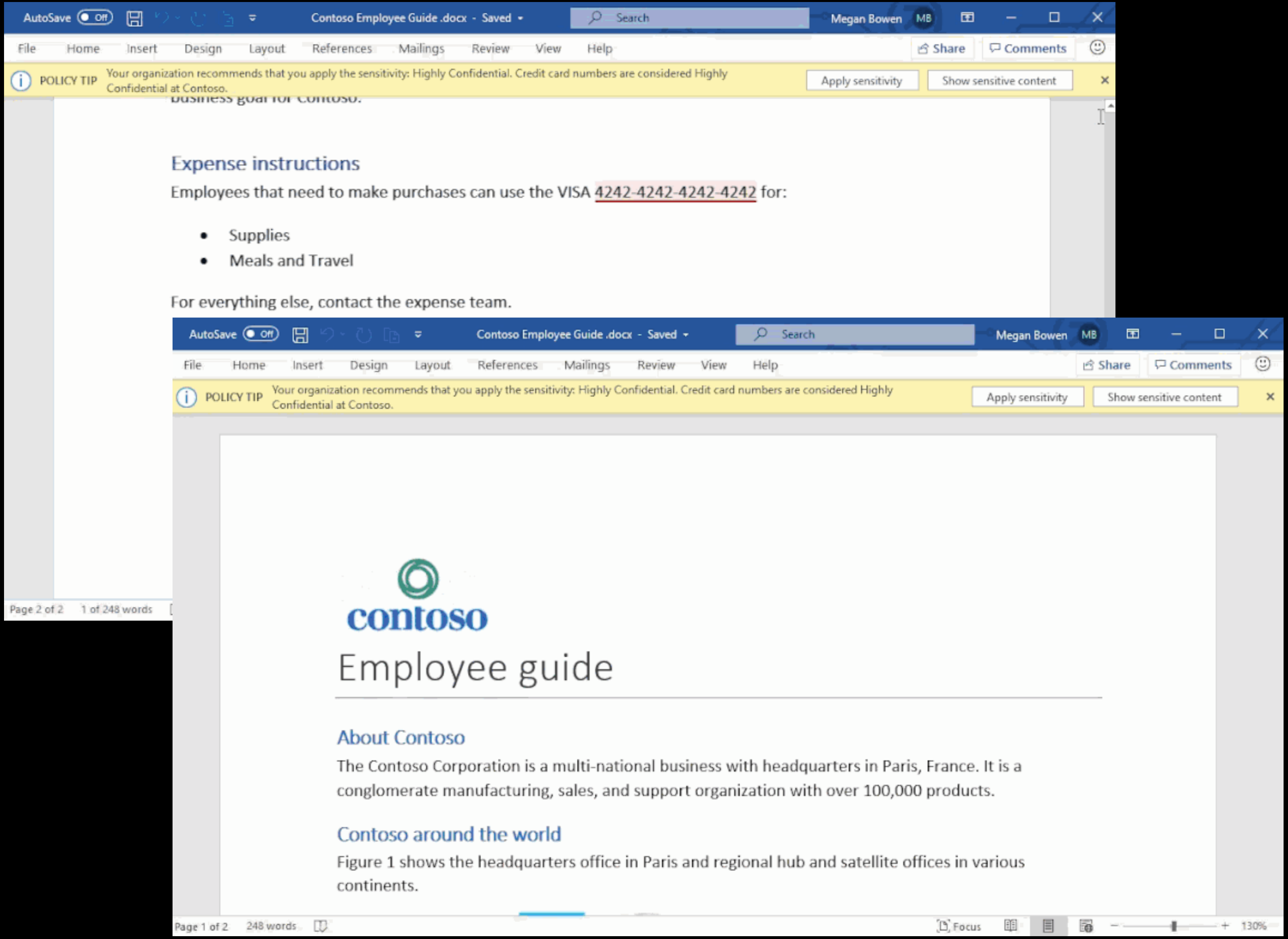
Name	Type	Publisher
U.S. / U.K. Passport Number	Entity	Microsoft Corporation
Credit Card Number	Entity	Microsoft Corporation
France Social Security Number (INSEE)	Entity	Microsoft Corporation
Australia Medical Account Number	Entity	Microsoft Corporation
Greek Tax identification Number	Entity	Microsoft Corporation
France Driver's License Number	Entity	Microsoft Corporation
France Value Added Tax Number	Entity	Microsoft Corporation
New Zealand Ministry of Health Number	Entity	Microsoft Corporation
Hungary Personal Identification Number	Entity	Microsoft Corporation

Microsoft Information Protection

Automated On-premises
Network Discovery

Microsoft Information Protection

Automatic Labelling



AutoSave Off
Contoso Employee Guide .docx - Saved
Search
Megan Bowen MB
File Home Insert Design Layout References Mailings Review View Help
Share Comments
Apply sensitivity
Show sensitive content
Page 2 of 2 1 of 248 words

POLICY TIP Your organization recommends that you apply the sensitivity: Highly Confidential. Credit card numbers are considered Highly Confidential at Contoso.

business goal for Contoso.

Expense instructions

Employees that need to make purchases can use the VISA 4242-4242-4242-4242 for:

- Supplies
- Meals and Travel

For everything else, contact the expense team.

POLICY TIP Your organization recommends that you apply the sensitivity: Highly Confidential. Credit card numbers are considered Highly Confidential at Contoso.

Employee guide

About Contoso

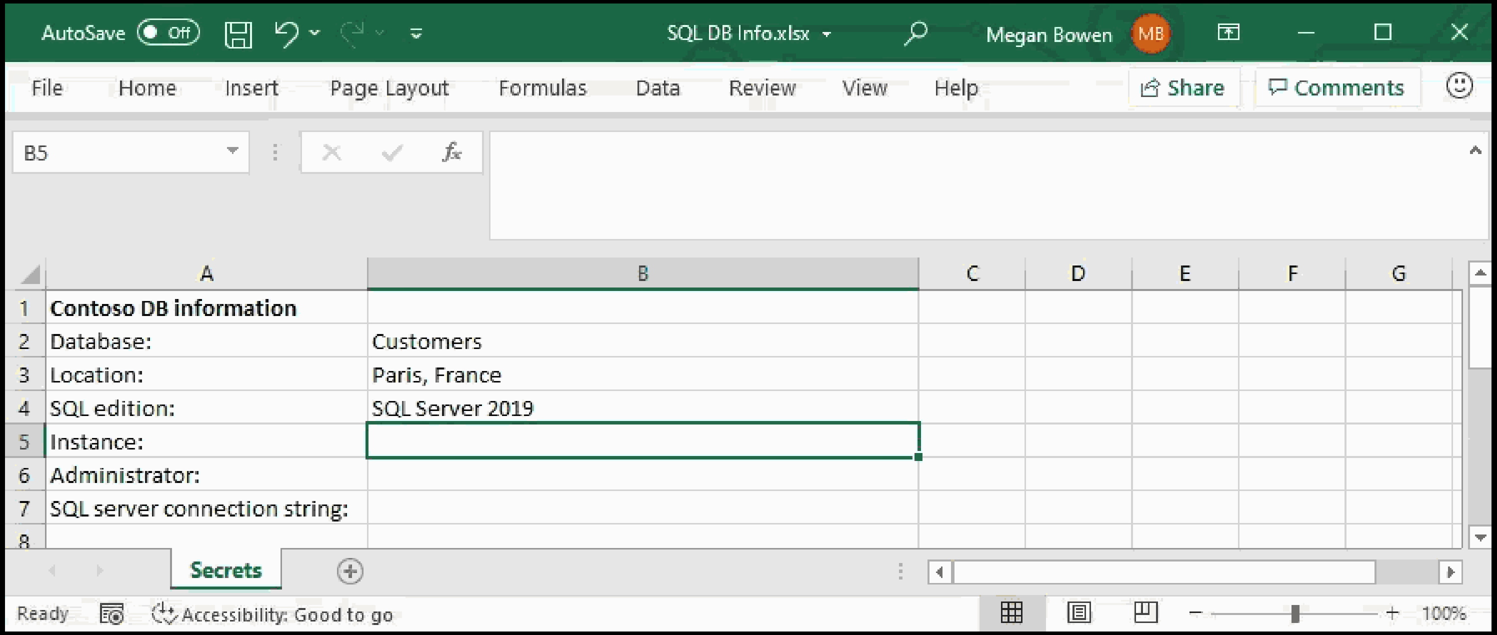
The Contoso Corporation is a multi-national business with headquarters in Paris, France. It is a conglomerate manufacturing, sales, and support organization with over 100,000 products.

Contoso around the world

Figure 1 shows the headquarters office in Paris and regional hub and satellite offices in various continents.

Microsoft Information Protection

Protecting in Office



	A	B	C	D	E	F	G
1	**Contoso DB information**						
2	Database:	Customers					
3	Location:	Paris, France					
4	SQL edition:	SQL Server 2019					
5	Instance:						
6	Administrator:						
7	SQL server connection string:						
8							