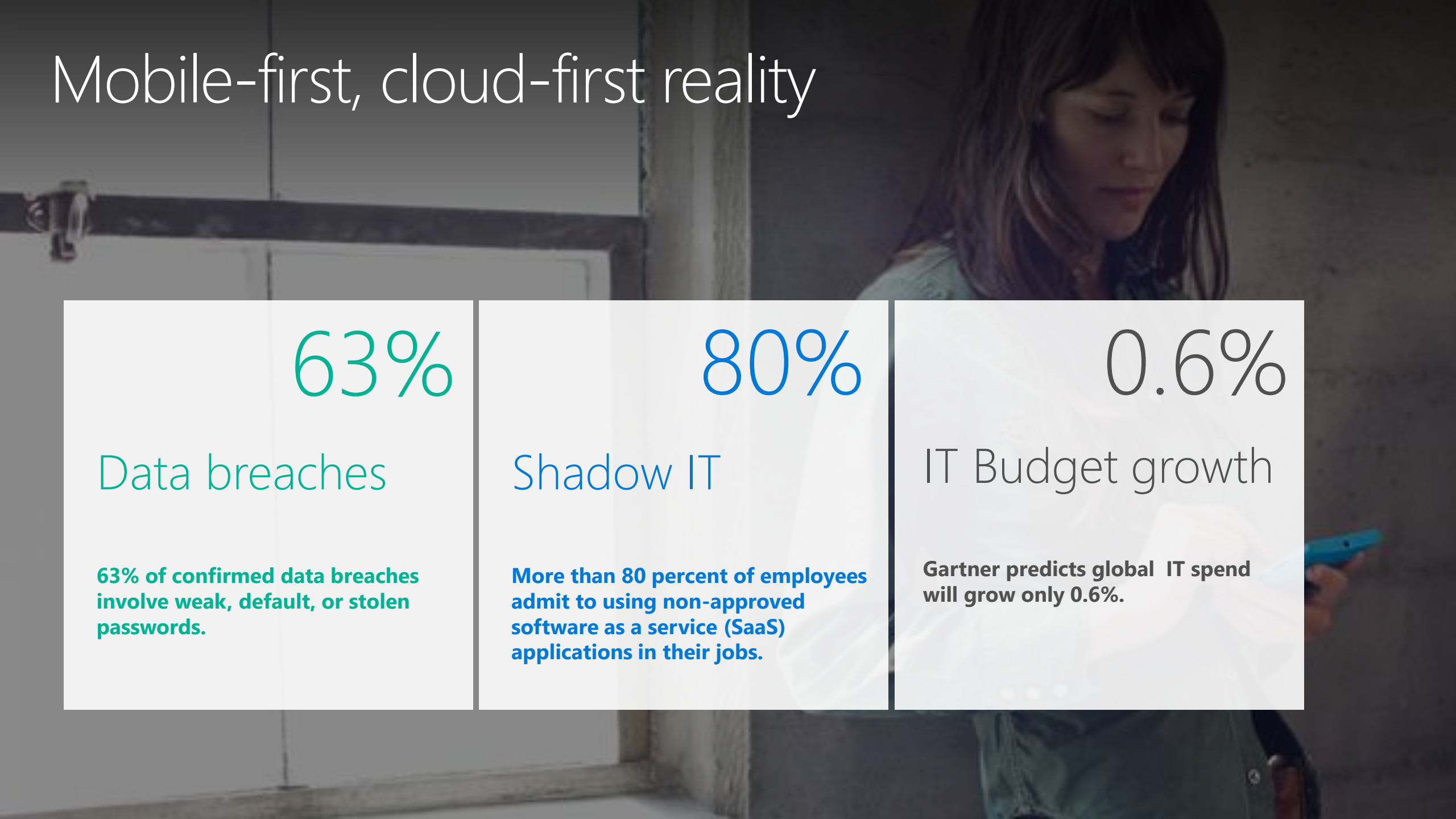
Microsoft

# Go mobile.
# Stay in control.

**Enterprise Mobility + Security**

Igor Shastitko, igorsh@outlook.com

# Mobile-first, cloud-first reality



## 63%

### Data breaches

**63% of confirmed data breaches involve weak, default, or stolen passwords.**

## 80%

### Shadow IT

**More than 80 percent of employees admit to using non-approved software as a service (SaaS) applications in their jobs.**

## 0.6%

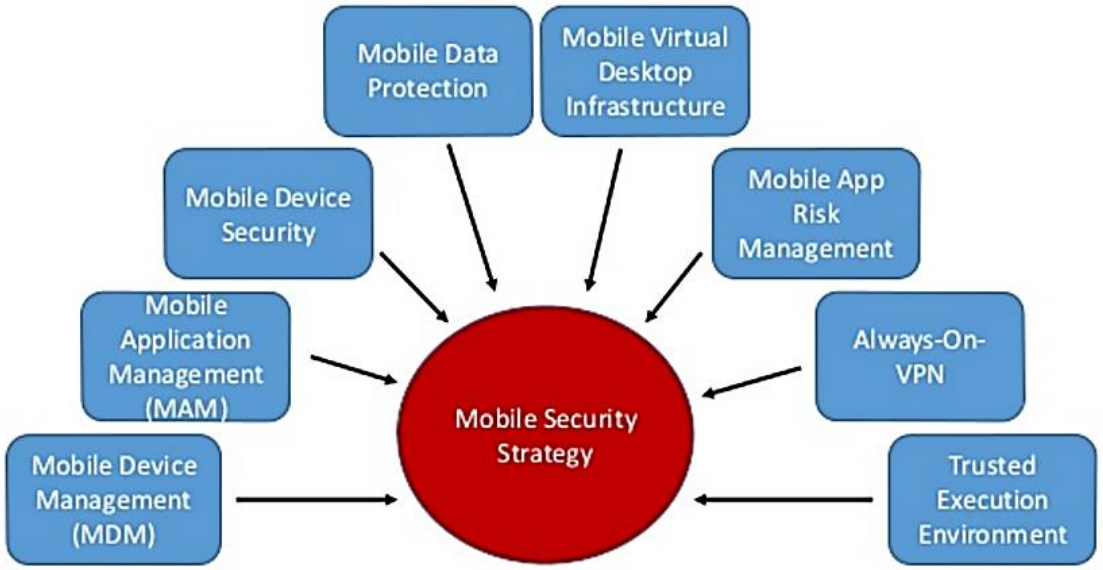
### IT Budget growth

**Gartner predicts global IT spend will grow only 0.6%.**

# Additional numbers: Lost/Stolen mobile devices statistic


- One laptop is **stolen** every **53 seconds**.
- **70 million** smartphones are **lost each year**, with only 7 percent recovered.
- **4.3 percent** of **company-issued** smartphones are **lost or stolen** every year.
- **80 percent** of the cost of a lost laptop is from **data breach**.
- **52 percent** of devices are **stolen** from the **office/workplace**, and **24 percent** from **conferences**.

# Additional numbers: Mobile data usage and breaches




- **49 percent** of people use their personal mobile devices for **both work and play**
- **36 percent** say their employer **has no policy** on using personal devices for work;
- **52 percent** of mobile users say they **store sensitive files** online or in mobile device;
- **One-quarter** of those who use online/mobile file storage **use the same account** for both work and personal files
- **30 percent** of parents **allow their children** to **use their work device** to play, shop and download.
- **21 percent share passwords** and logins with **families**, while **18 percent share** passwords and logins with **friends**.

# Microsoft Enterprise Mobility + Security

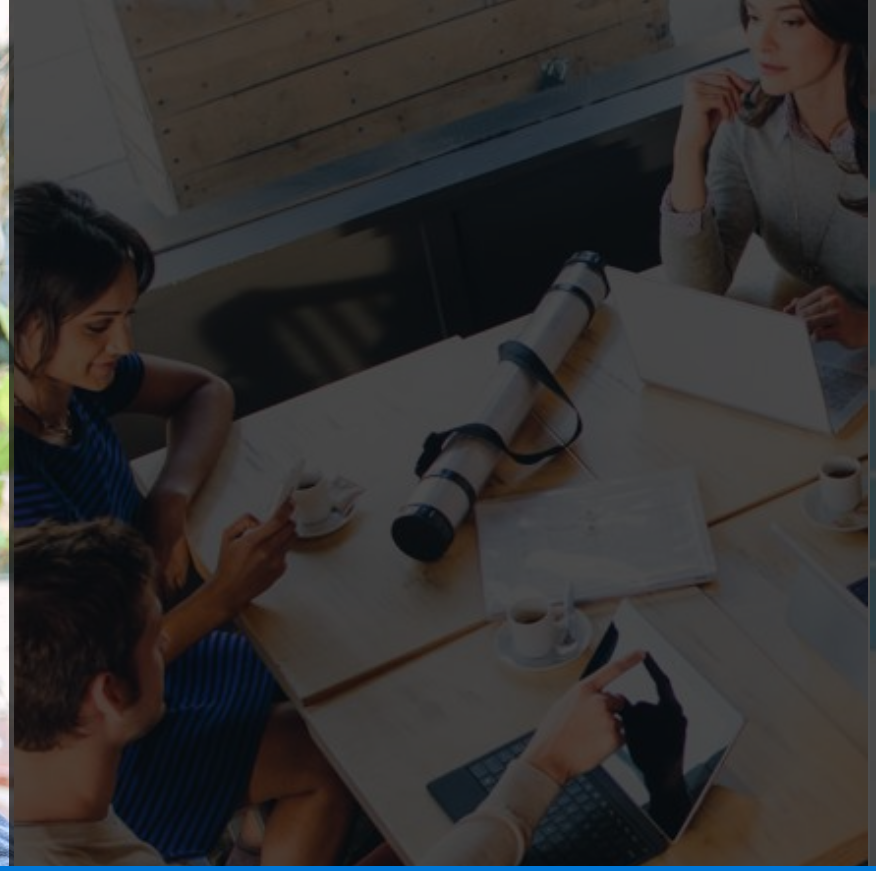
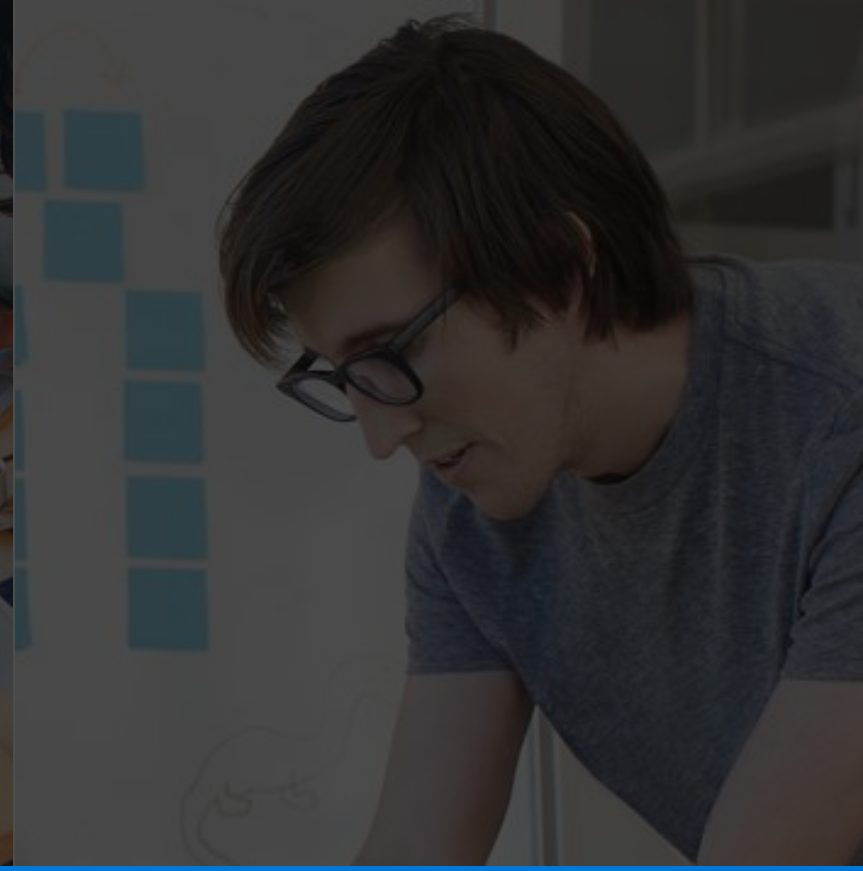
## Customers need

| Secure against new threats | User freedom | Do more with less |
| --- | --- | --- |
|  |  |  |

**ENTERPRISE MOBILITY + SECURITY**

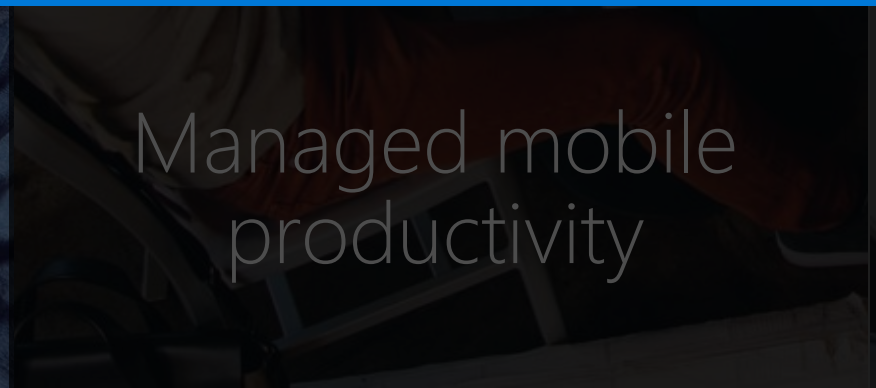
## Microsoft solution

| Identity-driven security | Managed mobile productivity | Comprehensive solution |
| --- | --- | --- |

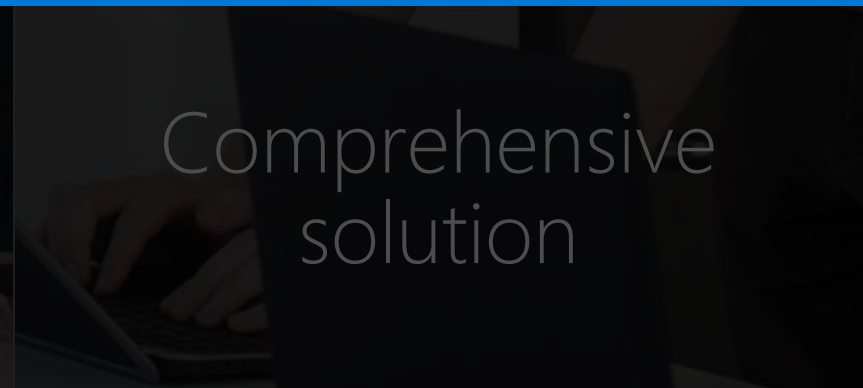




# ENTERPRISE MOBILITY + SECURITY

Identity-driven security

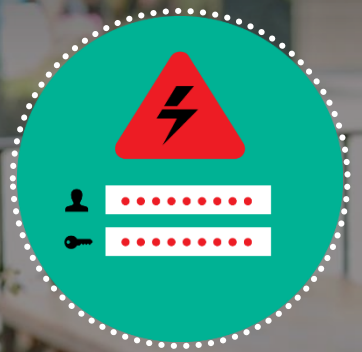


Managed mobile productivity



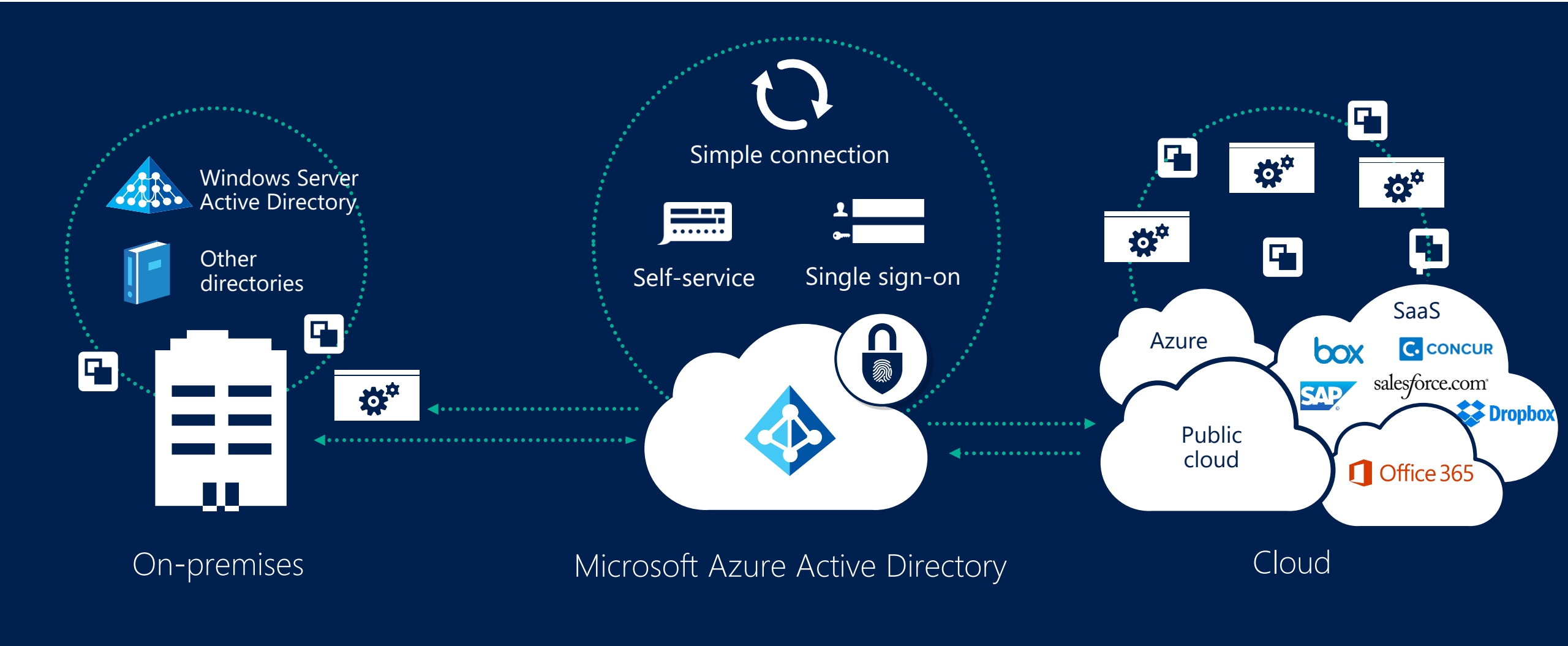
Comprehensive solution

# Identity-driven Security



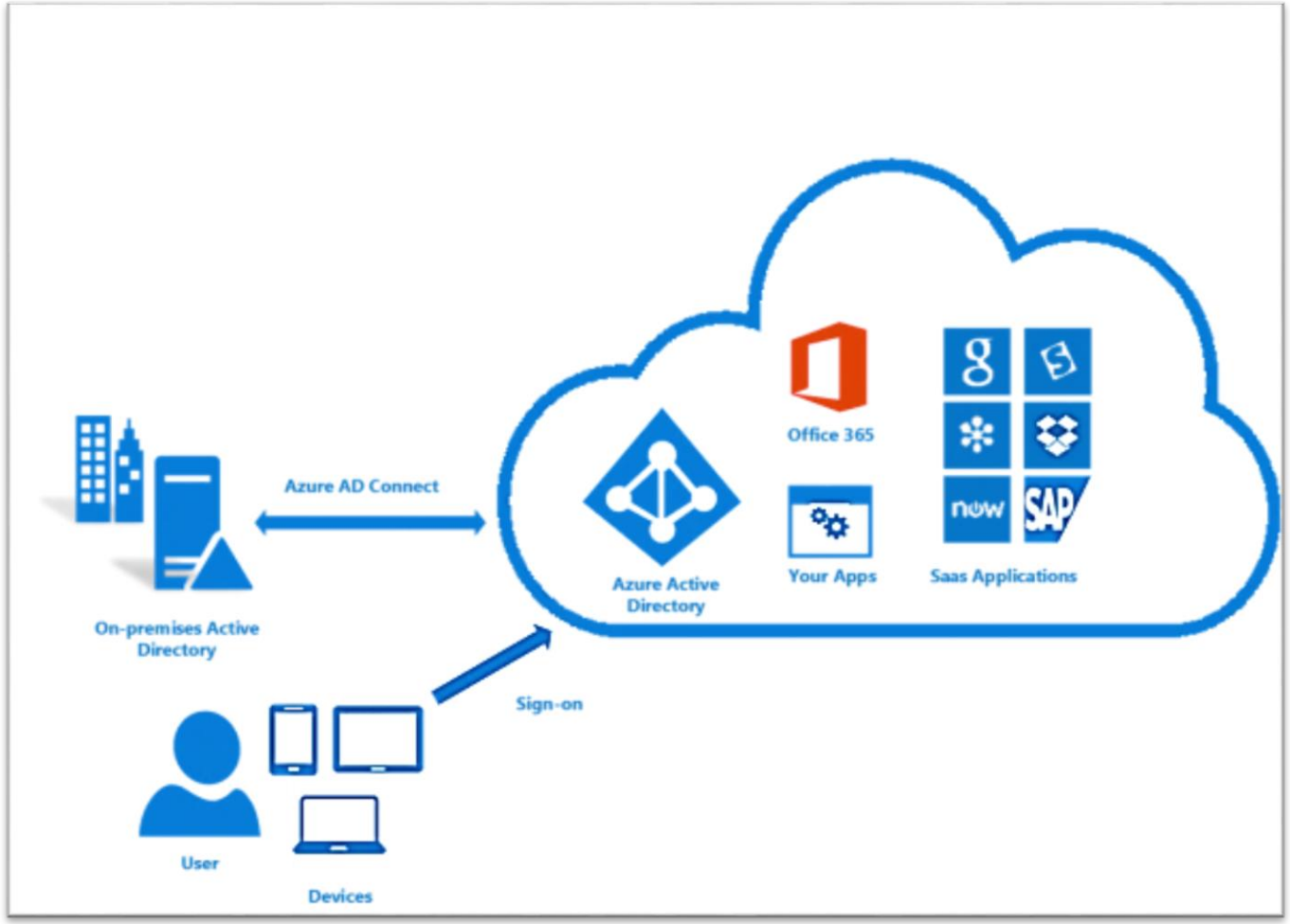
Data Breaches 63%

# Identity is the foundation for enterprise mobility



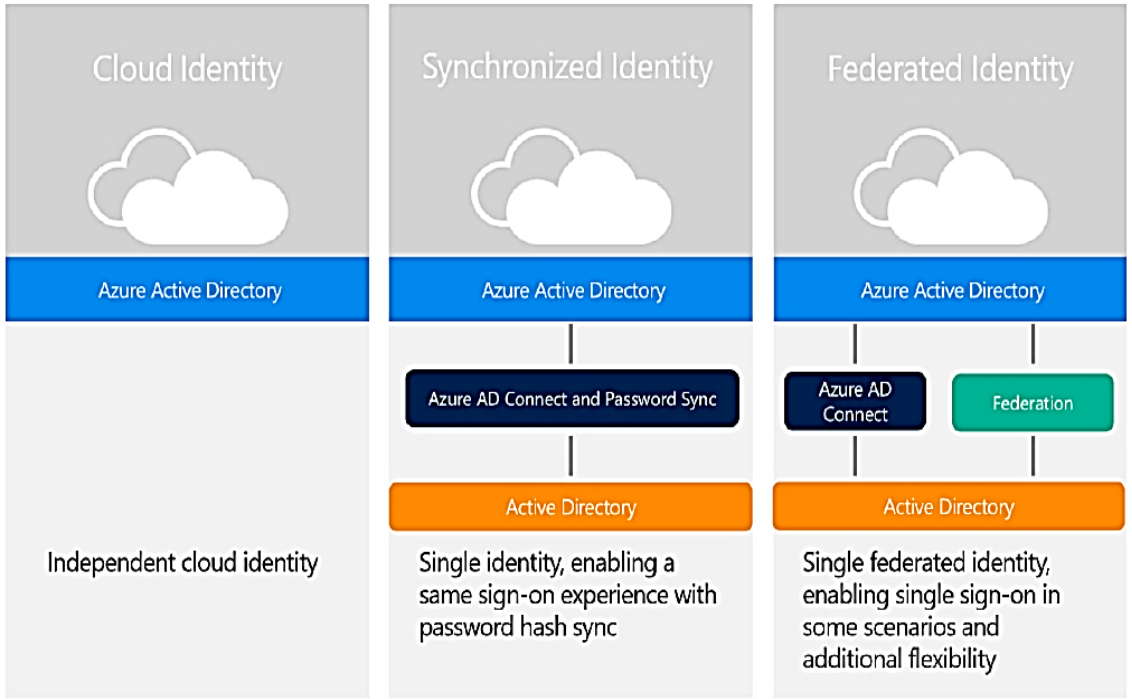
# Project opportunities: “Pure” Cloud/Hybrid Identity

Clear classification of solution (for yourself and Customer) is a very important aspect of the project




- Cloud identities: these are identities that exist solely in the cloud. In the case of Azure AD, they would reside specifically in your Azure AD directory.
- Synchronized: these are identities that exist on-premises and in the cloud. Using Azure AD Connect, these users are either created or joined with existing Azure AD accounts.
- Federated: these identities exist both on-premises and in the cloud. Using Azure AD Connect, these users are either created or joined with existing Azure AD accounts.

# SELECT RIGHT SCENARIO




| Сценарий | PROS | CONS |
|---|---|---|
| **Cloud identities** | • Easier to manage for small organization.<br>• Nothing to install on-premises<br>• No additional hardware needed<br>• Easily disabled if the user leaves the company | • Users will need to sign-in when accessing workloads in the cloud<br>• Passwords may or may not be the same for cloud and on-premises identities |
| **Synchronized** | • On-premises password will authenticate both on-premises and cloud directories.<br>• Easier to manage for small, medium or large organizations<br>• Users can have single sign-on (SSO) for some resources<br>• Microsoft preferred method for synchronization<br>• Easier to manage | • Some customers may be reluctant to synchronize their directories with the cloud due specific company's police |
| **Federated** | • Users can have single sign-on (SSO)<br>• If a user is terminated or leaves, the account can be immediately disabled and access revoked<br>• Supports advanced scenarios that cannot be accomplished with synchronized | • More steps to setup and configure<br>• Higher maintenance<br>• May require additional hardware for the STS infrastructure<br>• May require additional hardware to install the federation server.<br>• Additional software is required if AD FS is used<br>• Require extensive setup for SSO<br>• Critical point of failure, if the federation server is down, users won't be |

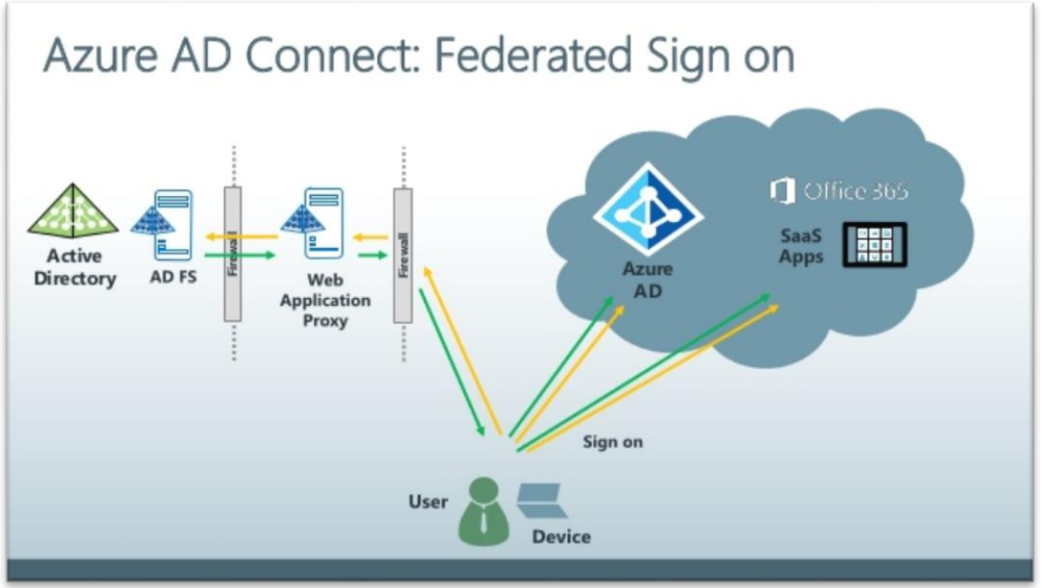
# SINGLE SIGN-ON SCENARIOS

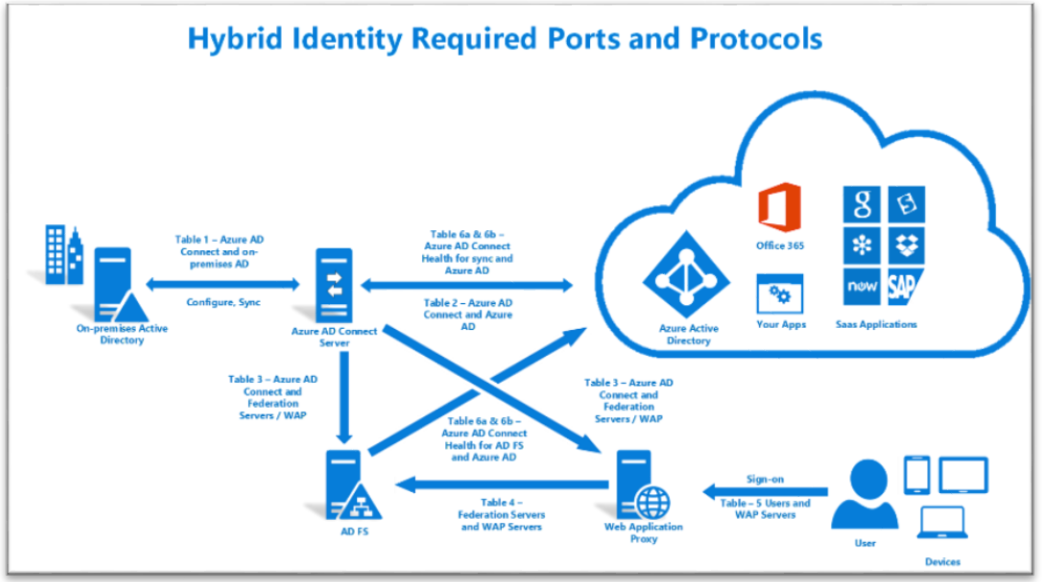
Most required feature for Hybrid Identity solution, KEY differentiator for Federated Identity

| | | Synchronized Identity | Federated Identity |
|---|---|---|---|
| Domain-joined and on the private network | Web Browsers | Forms-based authentication | **Single sign-on**, sometimes required to supply organization ID |
| | Outlook | Prompt for credentials | Prompt for credentials |
| | Lync | Prompt for credentials | **Single sign-on** to Lync, prompted for credentials to authenticate to Exchange |
| | SkyDrive Pro | Prompt for credentials | **Single sign-on** |
| | Office Pro Plus Subscription | Prompt for credentials | **Single sign-on** |
| External or untrusted | Web Browsers | Forms-based authentication | Forms-based authentication |
| | Outlook, Lync, SkyDrive Pro, Office Subscription | Prompt for credentials | Prompt for credentials |
| | Exchange ActiveSync | Prompt for credentials | Prompt for credentials |
| | Mobile Applications | Prompt for credentials | Prompt for credentials |

# Federated Identity & Single Sign-On

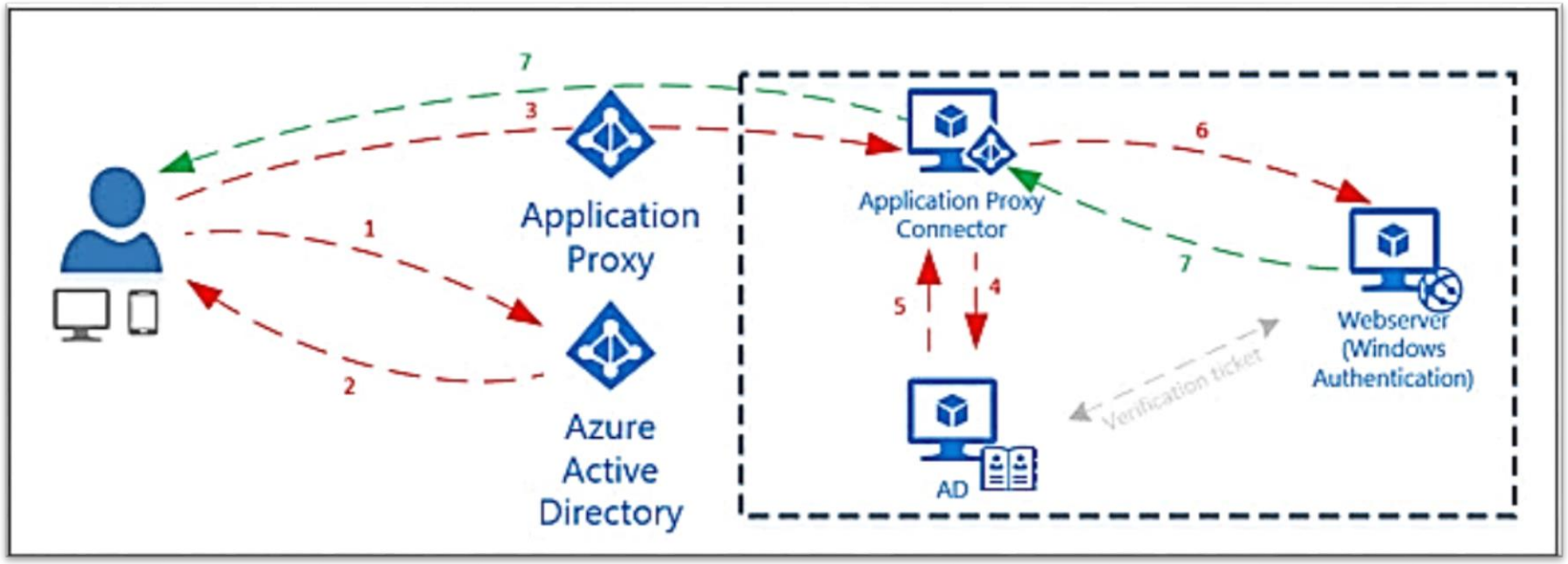
- Deployment and security planning AD FS publications
- Planning the deployment of Microsoft Web Publishing Service Application Proxy



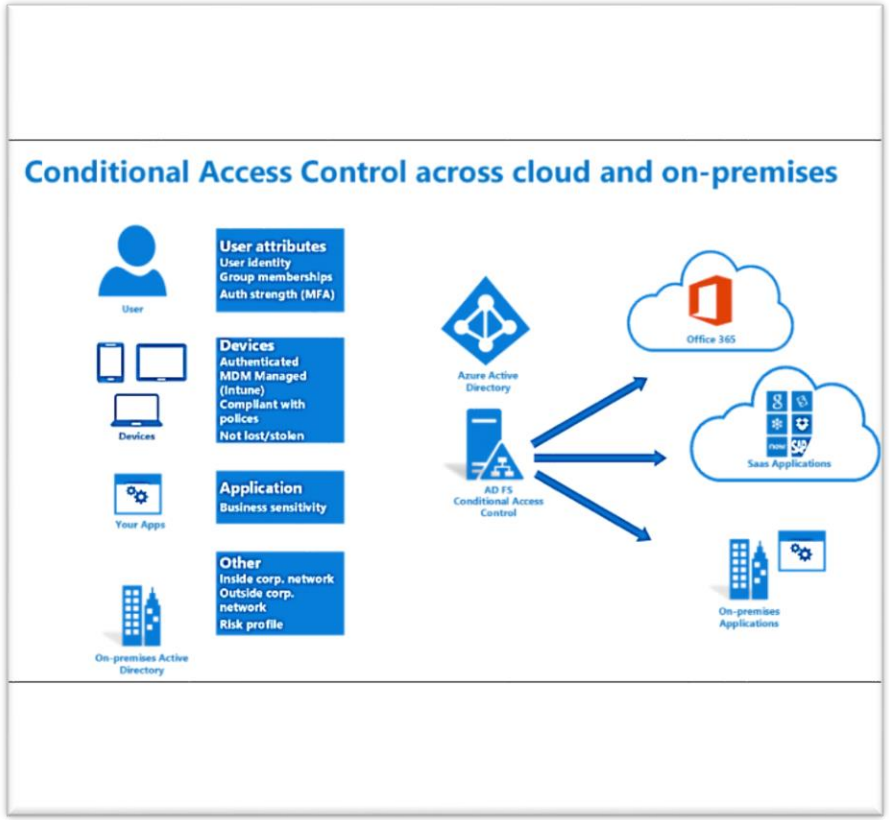
# Publishing on-premises Apps

- Planning & deploy on-premises Microsoft Web Application Proxy for application publishing
- Planning & connect cloud service Azure AD Application Proxy & Azure AD Application Proxy Connector for on-premises application publishing



# On-premises conditional access

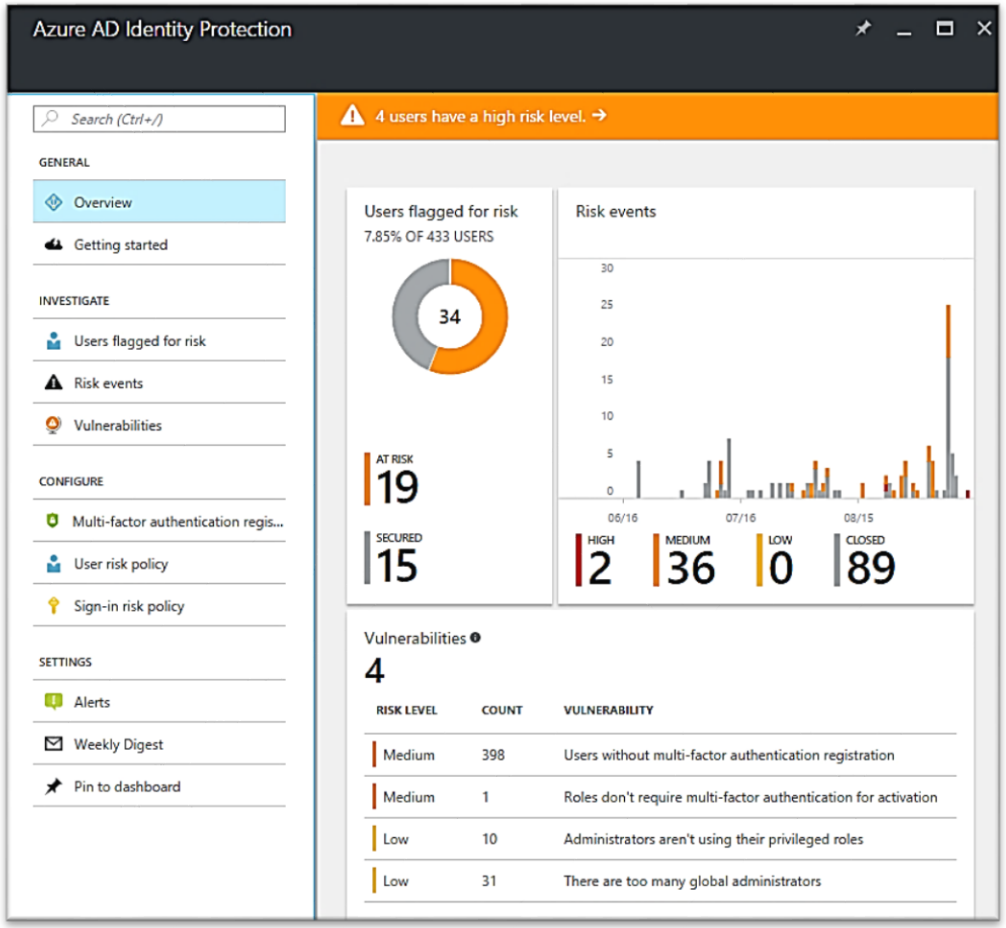
And one more additional layer to protect identity process




- Planning user's **devices' registration** in Azure AD
- Planning Azure AD Connector **Write-Back mode** to Microsoft Active Directory
- Planning & deploy **Conditional Access Policies** for AD FS service
- Discuss additional configuration policies for mobile devices with **Intune**

# ADFS Conditional Access Policies options

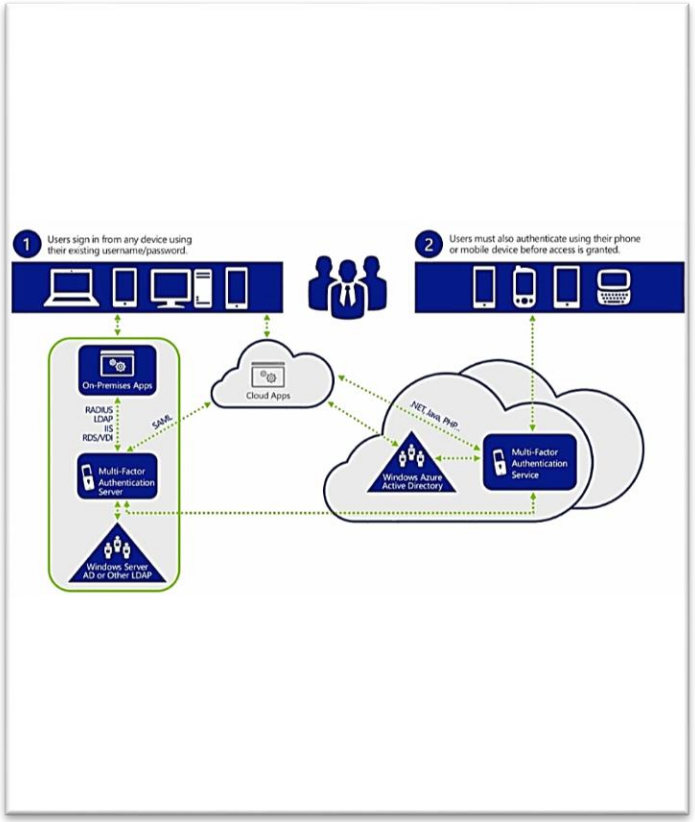
For Azure AD authentication/AD FS




- Group Based
- Connection to **well-know subnets**
- **Connected** to/**Registered** in:
  - **Domain**
  - **Azure AD**
  - **Workplace joined**
- Types of OS and policies compliance
- **Detected risk level** (with Azure Active Directory Identity Protection)
- Could be applied to **selected apps**

# Additional layer of security to prevent breaches

## Determine multi-factor authentication requirement




- What are **the key scenarios** that your Customer wants **to enable multi-factor authentication** for their users?
- **Are the users familiar** with multi-factor authentication?
- **Supported types** of Multi-Factor Authentication in Azure
  - SMS
  - Call
  - App Code/Notification
- MFA cloud/on-premises services
  - Multi-Factor Authentication for Office 365
  - Multi-Factor Authentication for Azure Administrators
  - **Azure Multi-Factor Authentication**
  - **Azure MFA Server on-premises**

# MFA Scenarios comparison

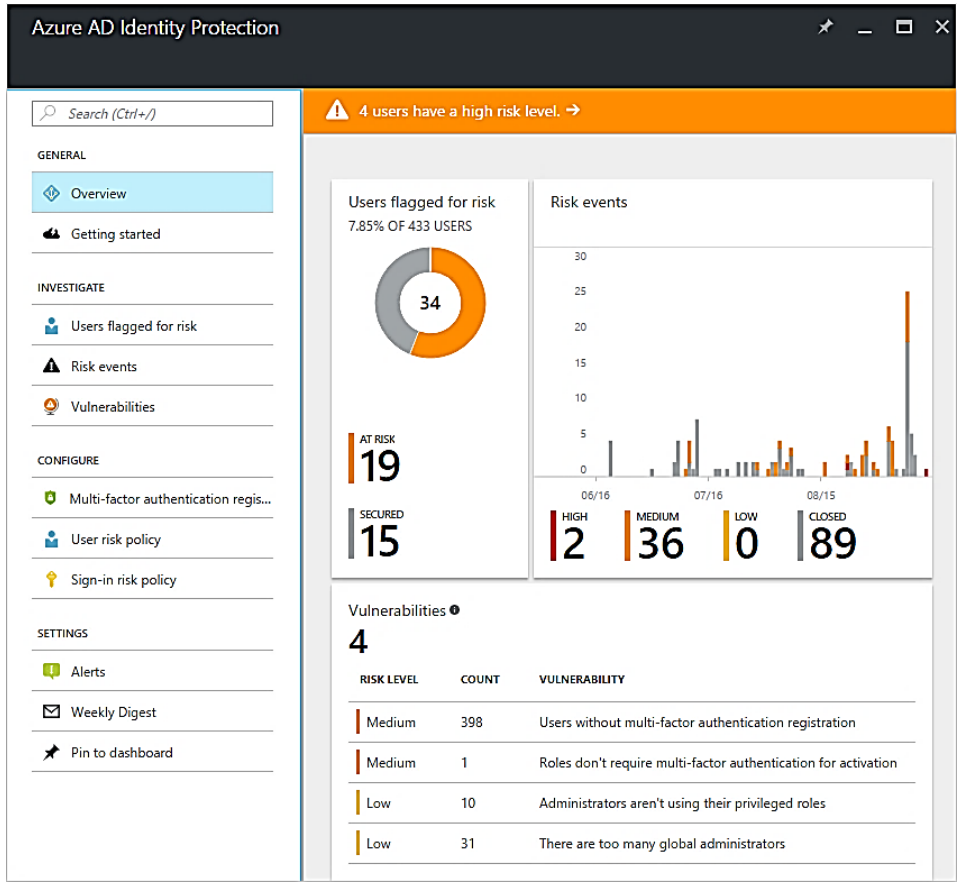
Help to customers to decide right solution

| | Multi-Factor Authentication in the cloud | Multi-Factor Authentication on-premises |
|---|---|---|
| Microsoft apps | + | + |
| SaaS apps in the app gallery | + | + |
| IIS applications published through Azure AD App Proxy | + | + |
| IIS applications not published through the Azure AD App Proxy | | + |
| Remote access as VPN, RDG | | + |

| User Location | Preferred Design |
|---|---|
| Azure Active Directory | **Multi-Factor Authentication in the cloud** |
| Azure AD and on-premises AD using federation with AD FS | **Both** |
| Azure AD and on-premises AD using Azure AD Connect no password sync | **Both** |
| Azure AD and on-premises using Azure AD Connect with password sync | **Both** |
| On-premises AD | **Multi-Factor Authentication Server** |

# Monitoring Azure AD sign-in activities

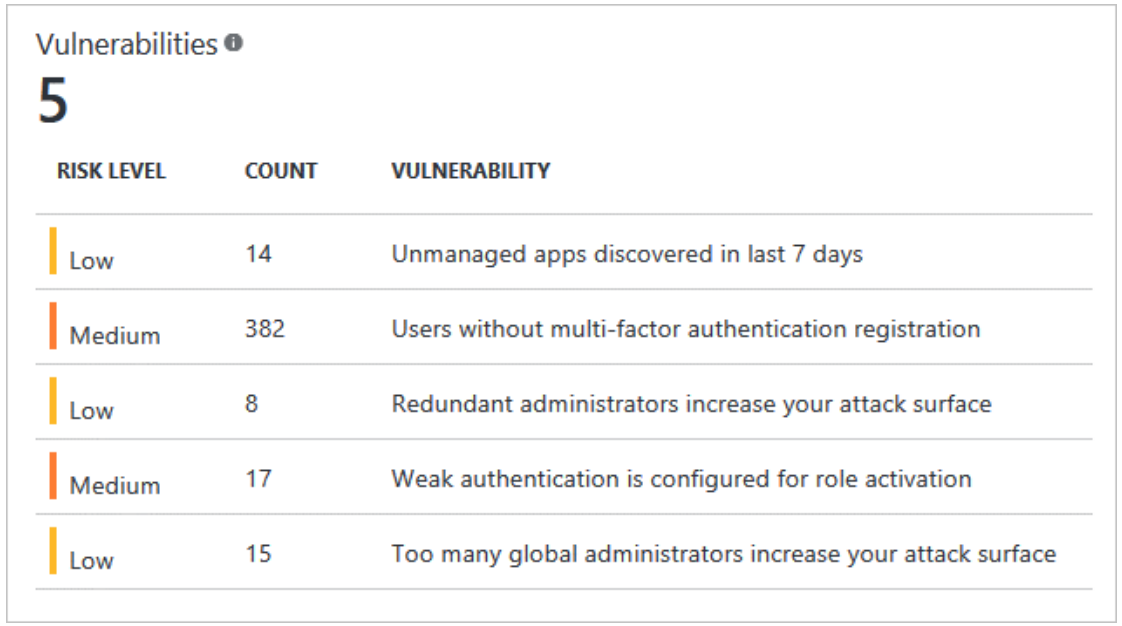
## Discovering compromised identities with Azure Active Directory Identity Protection




- **Detect** vulnerabilities and risky accounts
- **Investigating** risk events
- Risk-based **conditional access policies**

# Azure Active Directory Identity Protection

## Planning vulnerabilities detection



Vulnerabilities

5

| RISK LEVEL | COUNT | VULNERABILITY |
|---|---|---|
| Low | 14 | Unmanaged apps discovered in last 7 days |
| Medium | 382 | Users without multi-factor authentication registration |
| Low | 8 | Redundant administrators increase your attack surface |
| Medium | 17 | Weak authentication is configured for role activation |
| Low | 15 | Too many global administrators increase your attack surface |

- **Multi-factor authentication** registration not configured
- **Unmanaged cloud apps** (with Cloud App Discovery)
- **Security Alerts** (with Privileged Identity Management)

# Azure Active Directory Identity Protection

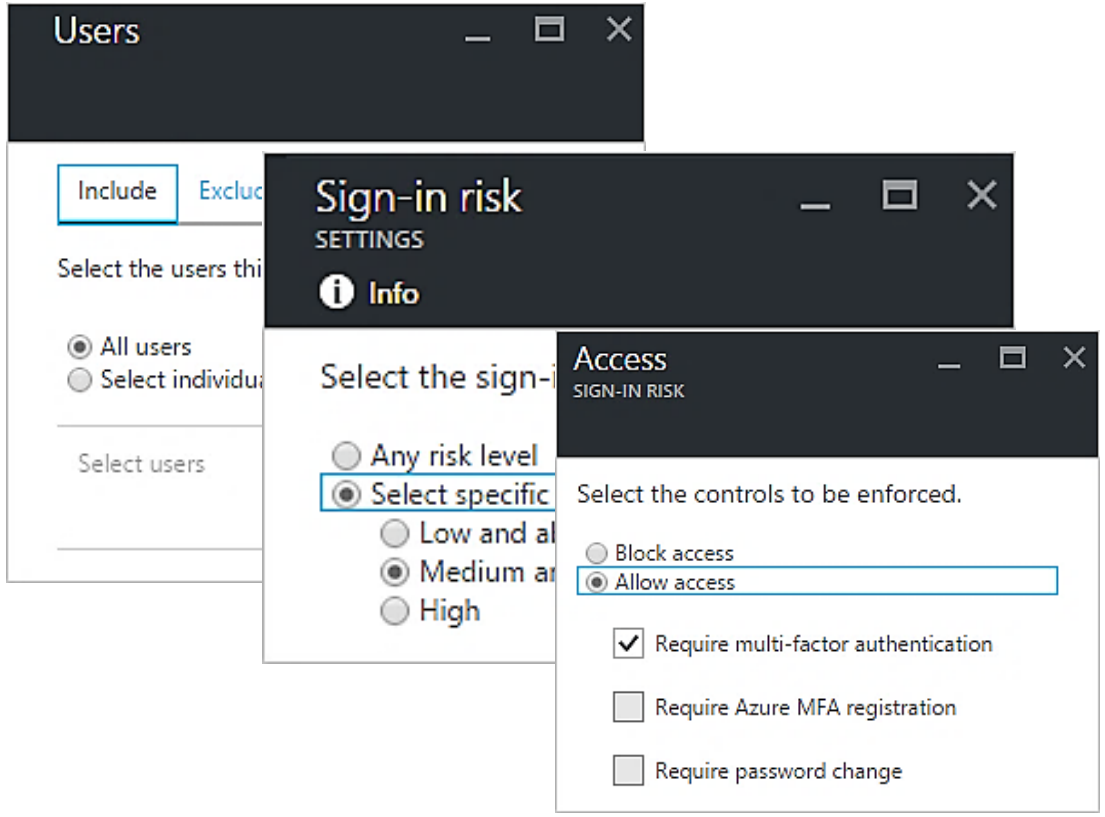
## Planning risk events investigation and supported events type

| RISK LEVEL | DETECTION TYPE | RISK EVENT TYPE | RISK EVENTS CLOSED | LAST UPDATED (UTC) |
|---|---|---|---|---|
| High | Offline | Users with leaked credentials | 44 of 45 | 12/7/2016 1:04 AM |
| Medium | Real-time | Sign-ins from anonymous IP addresses | 76 of 78 | 1/17/2017 2:44 PM |
| Medium | Offline | Impossible travels to atypical locations | 11 of 14 | 1/17/2017 2:44 PM |
| Medium | Real-time | Sign-in from unfamiliar location | 0 of 1 | 11/15/2016 7:18 PM |
| Low | Offline | Sign-ins from infected devices | 76 of 78 | 1/17/2017 2:44 PM |

- Leaked credentials
- Sign-ins from **anonymous IP** addresses
- Impossible travel to **atypical locations**
- Sign-in from **unfamiliar locations**
- Sign-ins from **infected devices**
- Sign-ins from **IP** addresses with **suspicious activity**

# Azure Active Directory Identity Protection

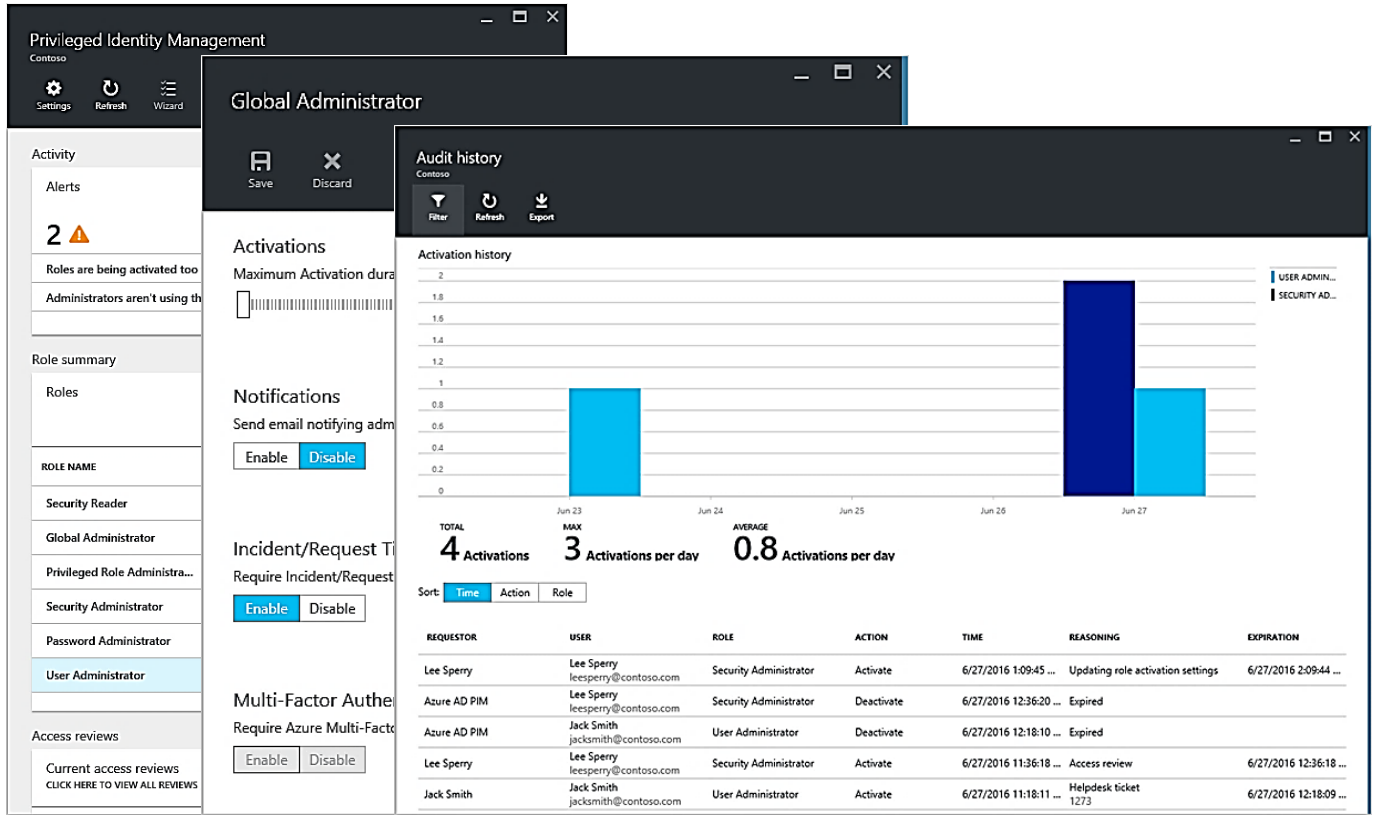
## Planning risk-based conditional access policies




- Policy to **mitigate risky sign-ins** by **blocking** sign-ins or **requiring** multi-factor authentication challenges.
- Policy to **block** or **secure** risky user accounts
- Policy to **require** users to **register** for **multi-factor authentication**

# Manage, control and monitor Admins' access

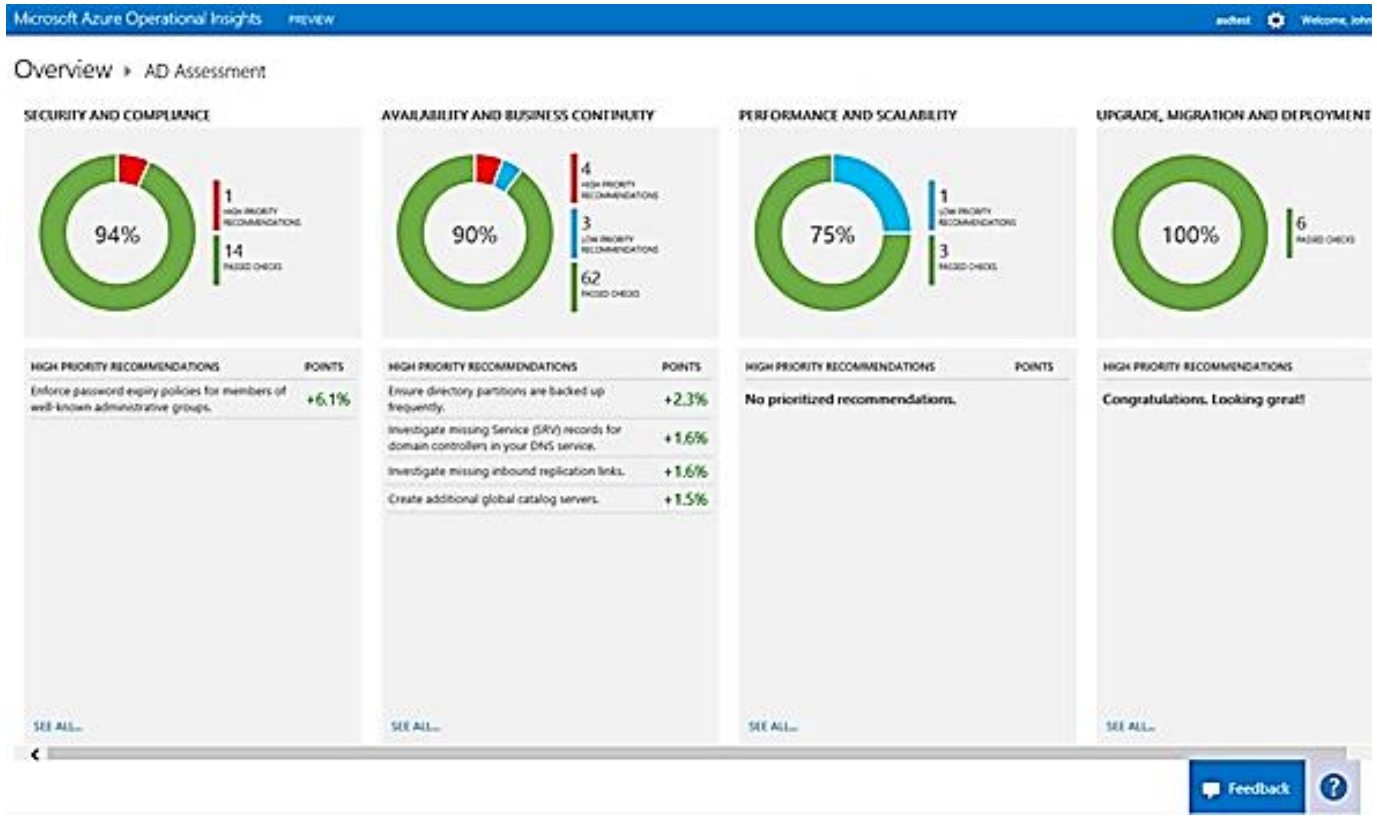
## Azure AD Privileged Identity Management




- See which users are **Azure AD administrators**
- Enable on-demand, "**just in time**" administrative access to Microsoft Online Services like Office 365 and Intune
- Get **reports** about administrator **access history** and changes in administrator assignments
- Get **alerts** about **access** to a privileged role

# Monitoring risk and health of AD on-premises

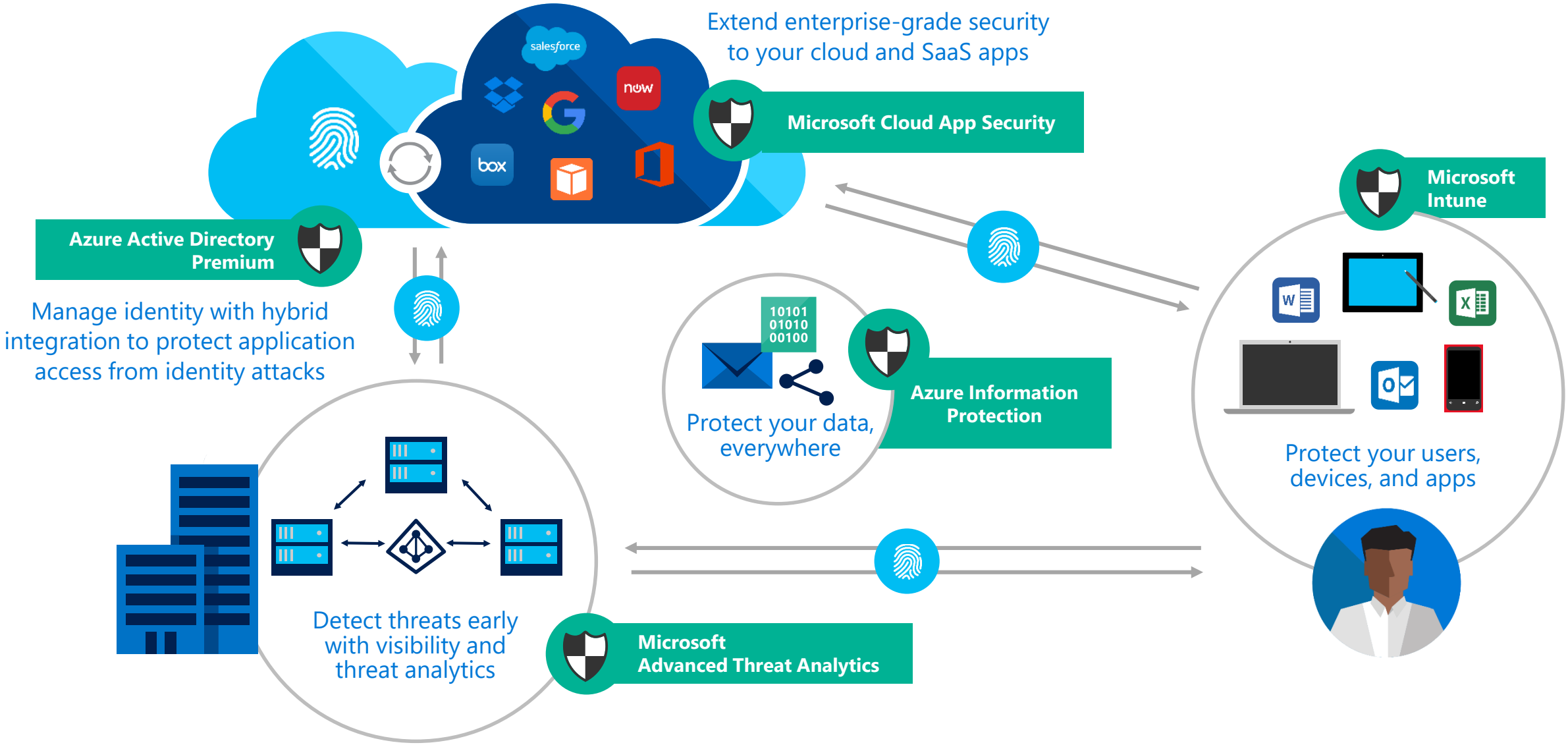
Active Directory Assessment Intelligence Pack in Azure Operational Insights




## FOCUS AREAS

- Security and Compliance
- Availability and Business Continuity
- Performance and Scalability
- Upgrade, Migration and Deployment

# Enterprise Mobility + Security

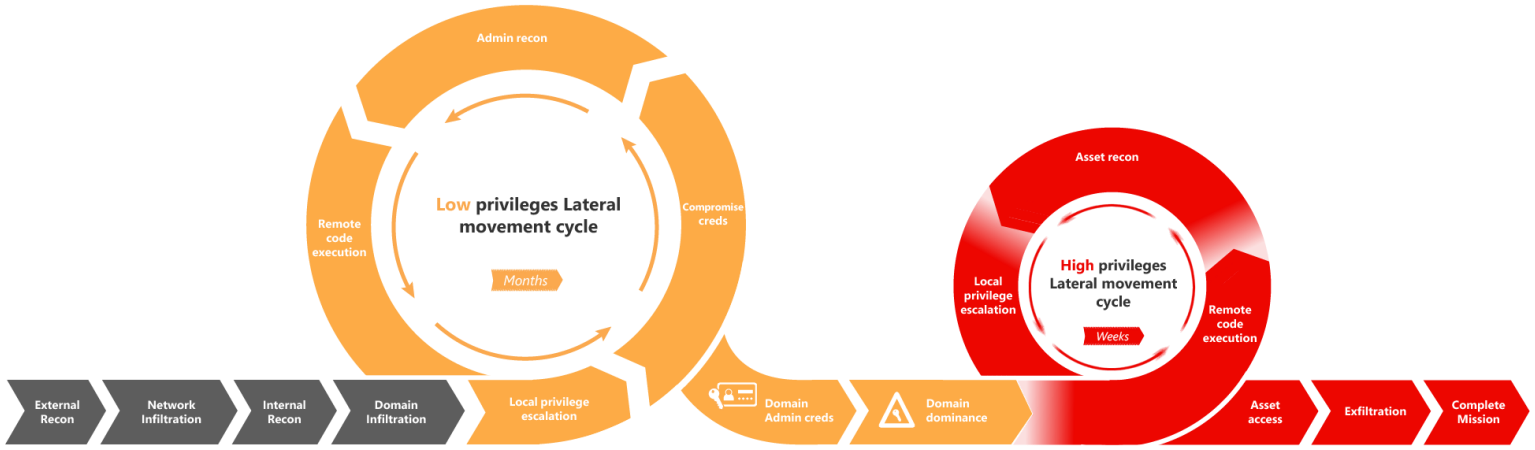


# Identity-driven security

Protect against advanced threats

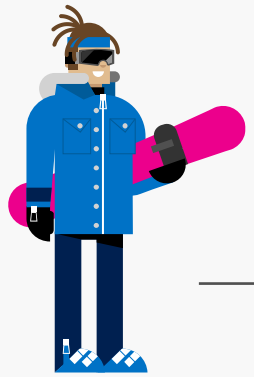
# Cyber Kill CHAIN attack

New types of attacks have a few stages that could be prevented by monitoring & countermeasures




- **Reconnaissance** - Account enumeration
- **Compromised Credential** - Abnormal working hours or location
- **Lateral Movement** - Abnormal authentication or resource access
- **Privilege Escalation** – Log Audit
- **Domain Dominance** - Remote execution

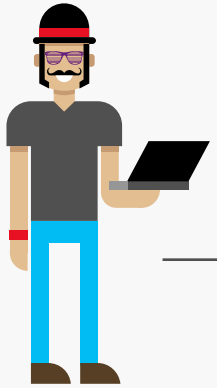
# What is exactly cyber kill chain?



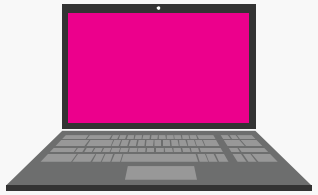
Jeff Victim
(JeffV)

Victim-PC

Ron Helpdesk
(RonHD)



Nuck Chorris
(NuckC)

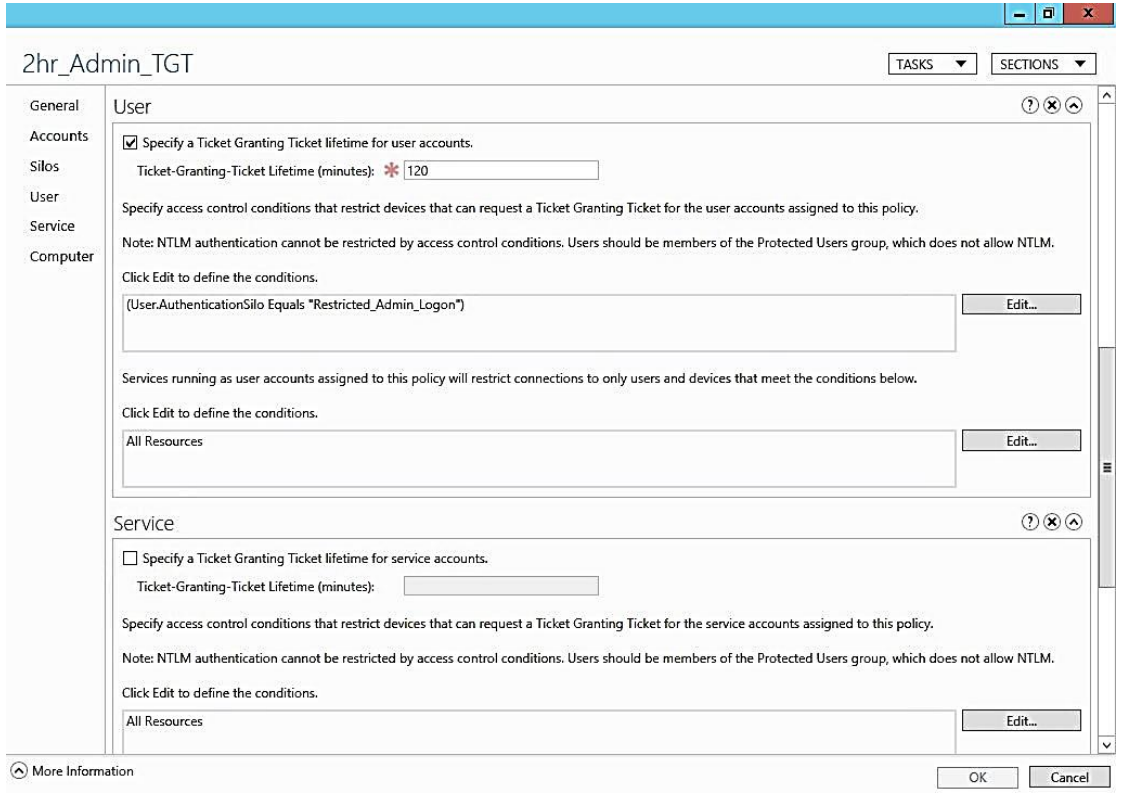


Admin-PC

Domain Controller
(DC1)

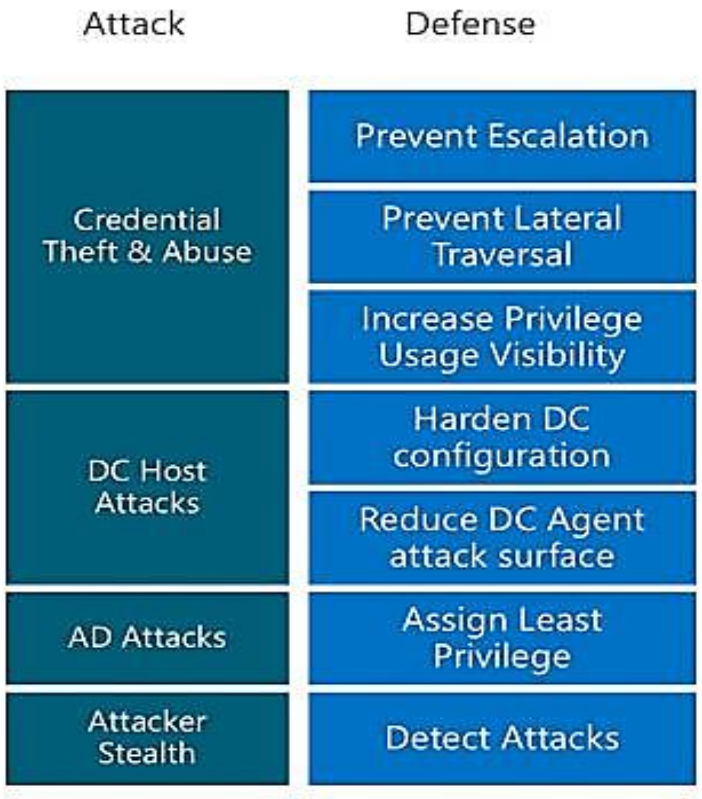
ATA Center

# Opportunities: Authentication Policies and Authentication Policy Silos as good way to modernization AD with EMS




- Good point to start modernization on-premises
- An **authentication policy silo controls** which **accounts can be restricted** by the silo and defines the authentication policies to apply to the members.
- An **authentication policy** defines the Kerberos protocol ticket-granting ticket (TGT) **lifetime properties** and authentication **access control conditions** for an account type.
  - The **TGT lifetime** for the account, which is set to be non-renewable.
  - The **criteria that device accounts need to meet** to sign in with a password or a certificate.
  - The **criteria that users and devices need to meet** to authenticate to services running as part of the account.
- Windows Server 2012 R2 or later required

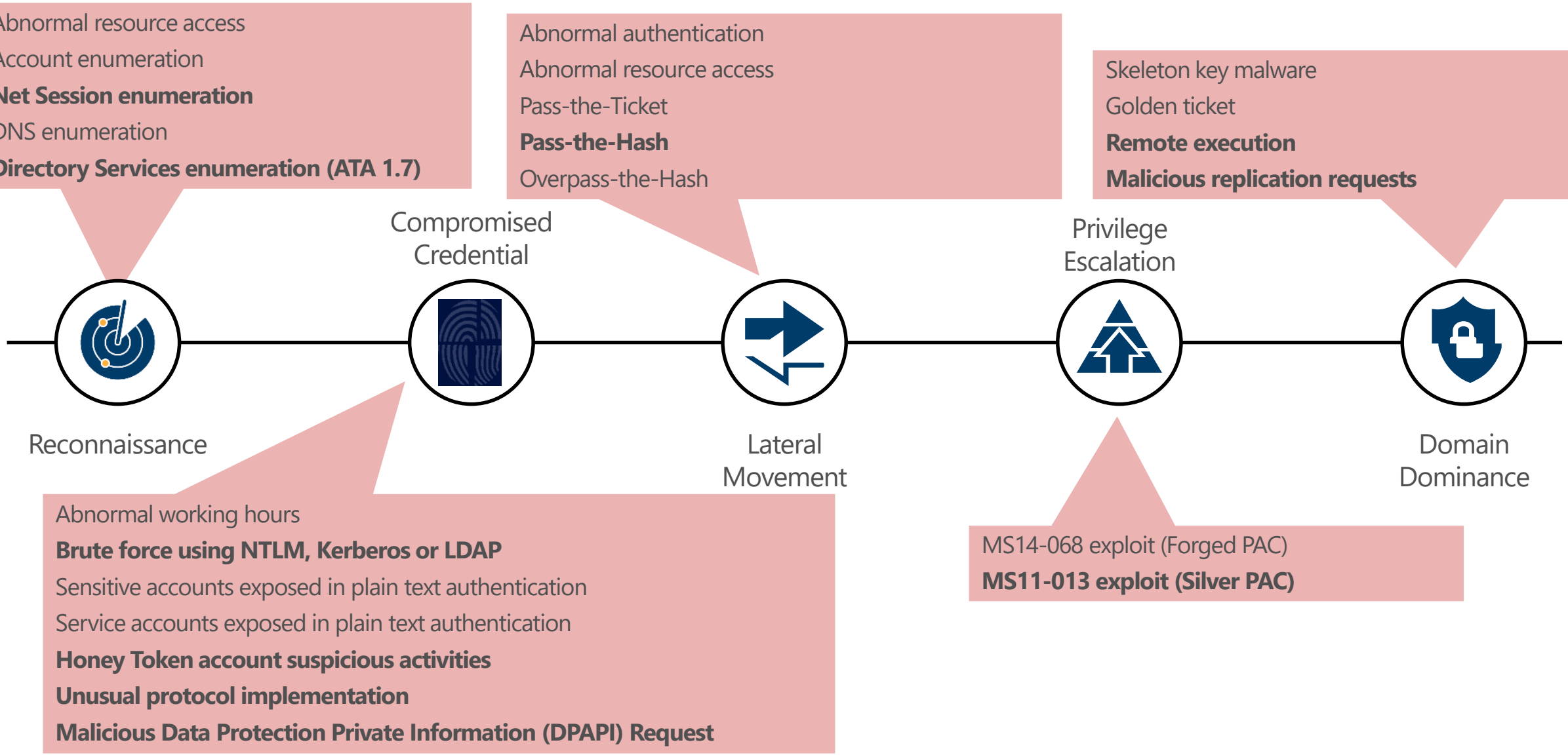
# Opportunities: Securing privileged access & protection on-premises again modern attack types




- Security Privileged Access Roadmap: Stage 1
  - **Separate Admin** account for admin tasks
  - **Privileged Access Workstations** (PAWs) Phase 1: Active Directory admins
  - **Unique** Local Admin **Passwords** for **Workstations**
  - **Unique** Local Admin **Passwords** for **Servers**
- Security Privileged Access Roadmap: Stage 2
  - **PAW** Phases 2 and 3: all **admins** and additional **hardening**
  - Time-bound privileges (**no permanent administrators**)
  - **Multi-factor** for time-bound elevation
  - **Just Enough Admin** (JEA) for DC Maintenance
  - **Lower attack surface** of Domain and DCs
  - **Attack Detection**
- Security Privileged Access Roadmap: Stage 3
  - Modernize **Roles** and **Delegation Model**
  - **Smartcard** or Passport Authentication for **all admins**
  - **Admin Forest** for Active Directory administrators
  - **Code Integrity** Policy for DCs (Server 2016)
  - **Shielded VMs** for virtual DCs (Server 2016 Hyper-V Fabric)

# Protection again cyber kill chain attacks

## Plan & deploy Microsoft Advanced Threat Analytics



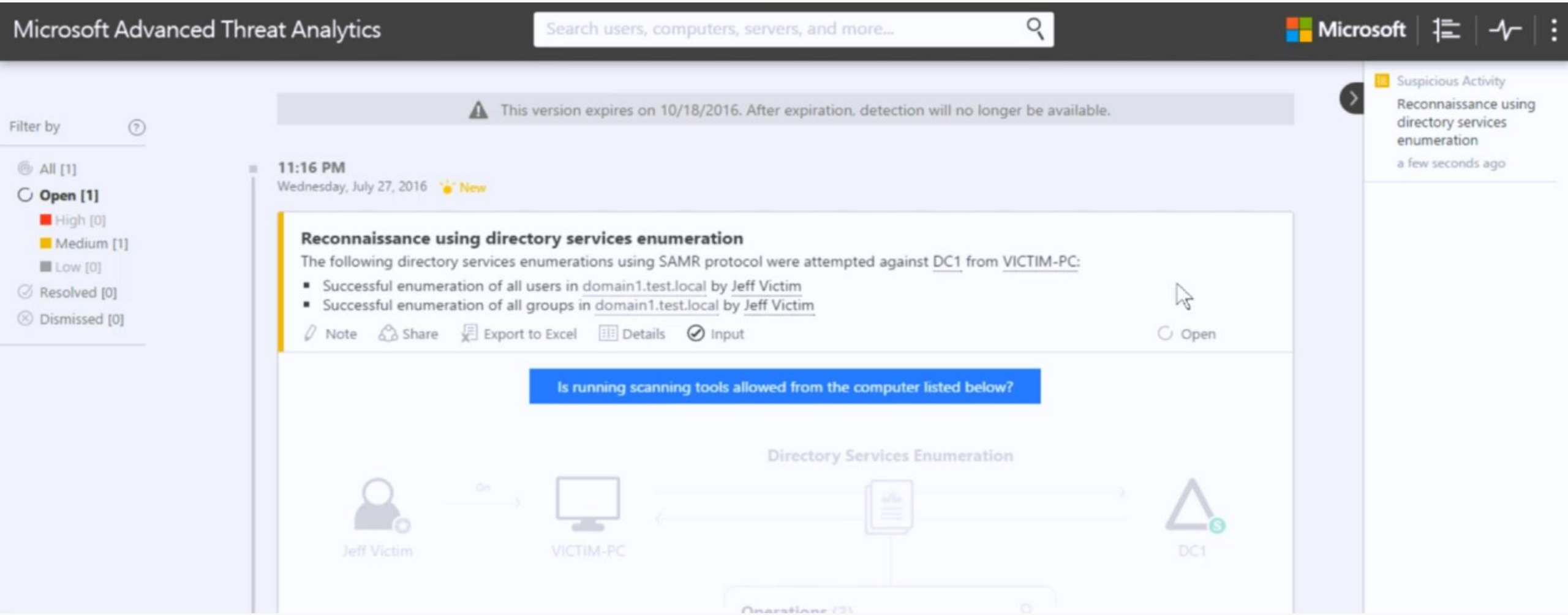
# Reconnaissance

## What we did?

- Collect user and group info (SAM-R)
- Find our next targets (NetSess)

## What's next?

- Gain access to other assets
- Get the Domain Admin credentials


Microsoft Advanced Threat Analytics
Search users, computers, servers, and more...
Microsoft
This version expires on 10/18/2016. After expiration, detection will no longer be available.
Filter by
All [1]
Open [1]
High [0]
Medium [1]
Low [0]
Resolved [0]
Dismissed [0]
11:16 PM
Wednesday, July 27, 2016
New
Reconnaissance using directory services enumeration
The following directory services enumerations using SAMR protocol were attempted against DC1 from VICTIM-PC:
Successful enumeration of all users in domain1.test.local by Jeff Victim
Successful enumeration of all groups in domain1.test.local by Jeff Victim
Note
Share
Export to Excel
Details
Input
Open
Is running scanning tools allowed from the computer listed below?
Directory Services Enumeration
On
Jeff Victim
VICTIM-PC
DC1
Suspicious Activity
Reconnaissance using directory services enumeration
a few seconds ago

**Reconnaissance using directory services enumeration**

The following directory services enumerations using SAMR protocol were attempted against DC1 from VICTIM-PC:

- Successful enumeration of all users in domain1.test.local by Jeff Victim
- Successful enumeration of all groups in domain1.test.local by Jeff Victim

Note Share Export to Excel Details Input Open

**Reconnaissance using SMB Session Enumeration**

SMB session enumeration attempts were successfully performed by Jeff Victim, from VICTIM-PC against DC1, exposing 5 accounts.

Note Share Export to Excel Details Input Open

# Lateral Movement

## What we did?

- Gained helpdesk privileges (Over-pass-the-Hash)
  - mimikatz sekurlsa:logonpasswords
  - mimikatz sekurlsa:pth
- Gained domain admin permission (Pass-the-Ticket)
  - Psexec mimikatz
  - mimikatz sekurlsa:tickets /export
  - mimikatz sekurlsa:ptt

## What Next?

- Access sensitive data
- Improve persistency in the network

Filter by

All [5]
Open [5]
High [1]
Medium [4]
Low [0]
Resolved [0]
Dismissed [0]

• Disable Nick Chorns's account

11:21 PM
Wednesday, July 27, 2016 New

**Unusual protocol implementation**

Ron Helpdesk successfully authenticated from VICTIM-PC against DC1 using an unusual protocol implementation. This may be a result of malicious tools used to execute attacks such as Pass-The-Hash and brute force.

Note Share Export to Excel Details Input Open

Is there a service with custom protocol implementation running on the computer listed below?




**Computers (1)**

VICTIM-PC No Yes

Save Cancel

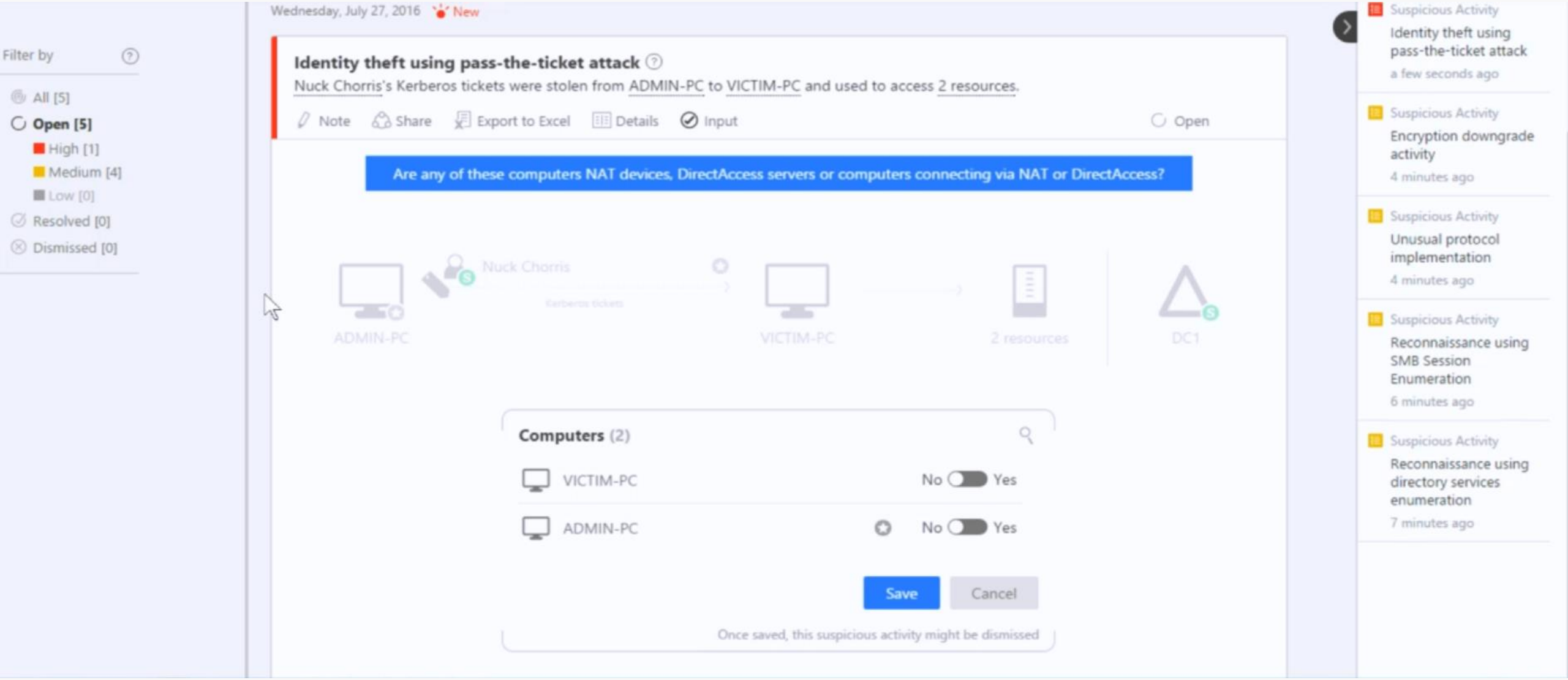
Suspicious Activity
Identity theft using pass-the-ticket attack
a minute ago

Suspicious Activity
Encryption downgrade activity
5 minutes ago

Suspicious Activity
Unusual protocol implementation
5 minutes ago

Suspicious Activity
Reconnaissance using SMB Session Enumeration
7 minutes ago

Suspicious Activity
Reconnaissance using directory services enumeration
8 minutes ago


Filter by
All [5]
Open [5]
High [1]
Medium [4]
Low [0]
Resolved [0]
Dismissed [0]
Wednesday, July 27, 2016
New
Identity theft using pass-the-ticket attack
Nuck Chorris's Kerberos tickets were stolen from ADMIN-PC to VICTIM-PC and used to access 2 resources.
Note
Share
Export to Excel
Details
Input
Open
Are any of these computers NAT devices, DirectAccess servers or computers connecting via NAT or DirectAccess?
Nuck Chorris
Kerberos tickets
ADMIN-PC
VICTIM-PC
2 resources
DC1
Computers (2)
VICTIM-PC
No
Yes
ADMIN-PC
No
Yes
Save
Cancel
Once saved, this suspicious activity might be dismissed
Suspicious Activity
Identity theft using pass-the-ticket attack
a few seconds ago
Suspicious Activity
Encryption downgrade activity
4 minutes ago
Suspicious Activity
Unusual protocol implementation
4 minutes ago
Suspicious Activity
Reconnaissance using SMB Session Enumeration
6 minutes ago
Suspicious Activity
Reconnaissance using directory services enumeration
7 minutes ago

### Encryption downgrade activity

The encryption method of the Encrypted_Timestamp field of AS_REQ message from VICTIM-PC has been downgraded based on previously learned behavior. This may be a result of a credential theft using Overpass-The-Hash from VICTIM-PC.

Note Share Export to Excel Details Open

### Unusual protocol implementation

Ron Helpdesk successfully authenticated from VICTIM-PC against DC1 using an unusual protocol implementation. This may be a result of malicious tools used to execute attacks such as Pass-The-Hash and brute force.

Note Share Export to Excel Details Input Open

### Identity theft using pass-the-ticket attack

Nuck Chorris's Kerberos tickets were stolen from ADMIN-PC to VICTIM-PC and used to access 3 resources.

Note Share Export to Excel Details Input Open

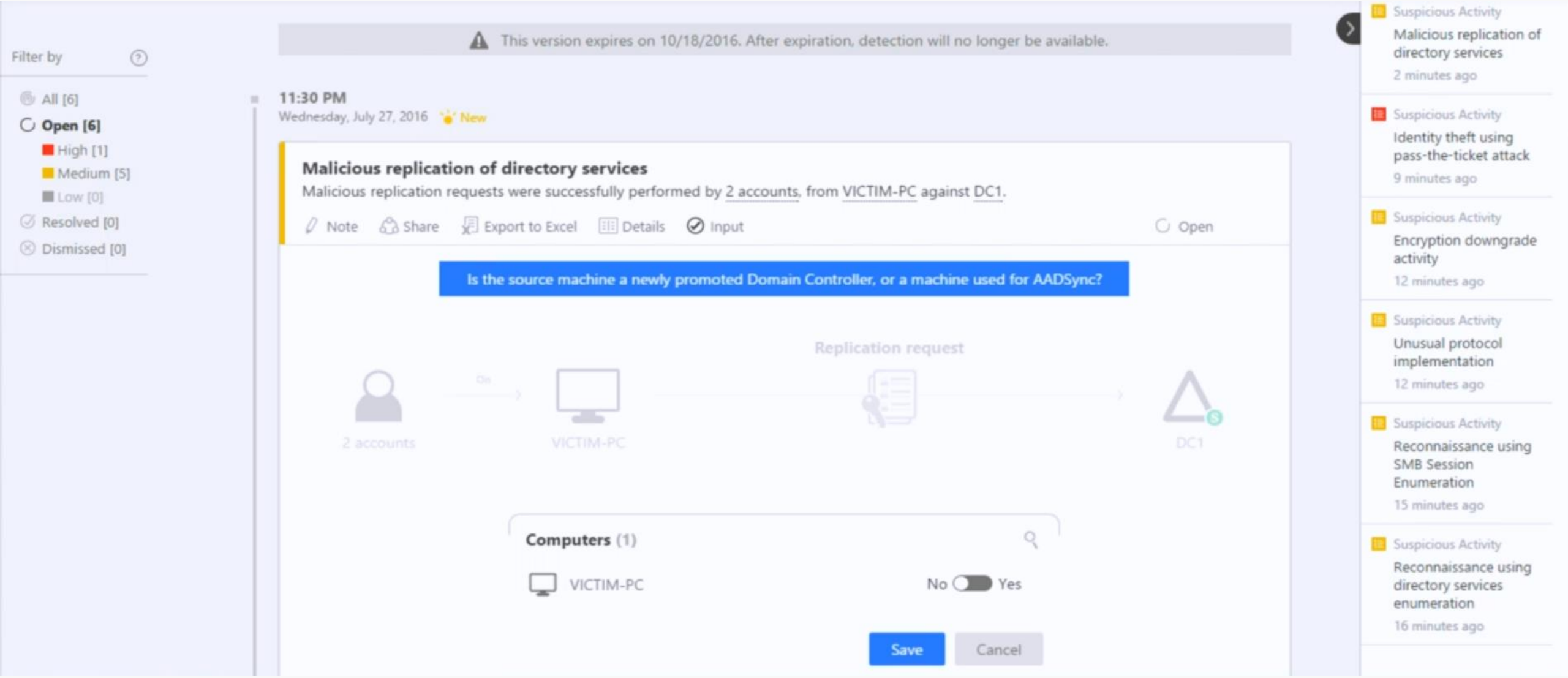
# Domain Dominance

## What we did?

- Compromised the KRBTGT account (DcSync)
  - mimikatz privilege::debug lsadump::scsync /user:domain\krbtgt
- Generated Golden ticket to access high value assets
  - mimikatz privilege::debug kerberos::golden

## What's next?

- Involve SMEs to identify "crown jewels"
- Exfiltrate sensitive data


This version expires on 10/18/2016. After expiration, detection will no longer be available.
Filter by
All [6]
Open [6]
High [1]
Medium [5]
Low [0]
Resolved [0]
Dismissed [0]
11:30 PM
Wednesday, July 27, 2016
New
Malicious replication of directory services
Malicious replication requests were successfully performed by 2 accounts, from VICTIM-PC against DC1.
Note
Share
Export to Excel
Details
Input
Open
Is the source machine a newly promoted Domain Controller, or a machine used for AADSync?
Replication request
On
2 accounts
VICTIM-PC
DC1
Computers (1)
VICTIM-PC
No
Yes
Save
Cancel
Suspicious Activity
Malicious replication of directory services
2 minutes ago
Suspicious Activity
Identity theft using pass-the-ticket attack
9 minutes ago
Suspicious Activity
Encryption downgrade activity
12 minutes ago
Suspicious Activity
Unusual protocol implementation
12 minutes ago
Suspicious Activity
Reconnaissance using SMB Session Enumeration
15 minutes ago
Suspicious Activity
Reconnaissance using directory services enumeration
16 minutes ago

Microsoft Advanced Threat Analytics

Search users, computers, servers, and more...

Microsoft

This version expires on 10/18/2016. After expiration, detection will no longer be available.

Filter by

- All [7]
- **Open [7]**
  - High [1]
  - Medium [6]
  - Low [0]
- Resolved [0]
- Dismissed [0]

**11:33 PM**
Wednesday, July 27, 2016 New

### Encryption downgrade activity

The encryption method of the TGT field of TGS_REQ message from VICTIM-PC has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on VICTIM-PC.

Note Share Export to Excel Details Open


Suspicious Activity
Encryption downgrade activity
a few seconds ago

Suspicious Activity
Malicious replication of directory services
3 minutes ago

Suspicious Activity
Identity theft using pass-the-ticket attack
11 minutes ago

Suspicious Activity
Encryption downgrade activity
14 minutes ago

Suspicious Activity
Unusual protocol implementation
14 minutes ago

Suspicious Activity

## Malicious replication of directory services

Malicious replication requests were successfully performed by Nuck Chorris, from VICTIM-PC against DC1.

Note Share Export to Excel Details Input Open

## Encryption downgrade activity

The encryption method of the TGT field of TGS_REQ message from VICTIM-PC has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on VICTIM-PC.

Note Share Export to Excel Details Open

# Windows Defender Advanced Threat Protection

Detect advanced attacks and remediate breaches

## Built in to Windows 10

No additional deployment & infrastructure.
Continuously up-to-date, lower costs.

## Behavior-based, cloud-powered breach detection

Actionable, correlated alerts for known and unknown adversaries.
Real-time and historical data.

## Rich timeline for investigation

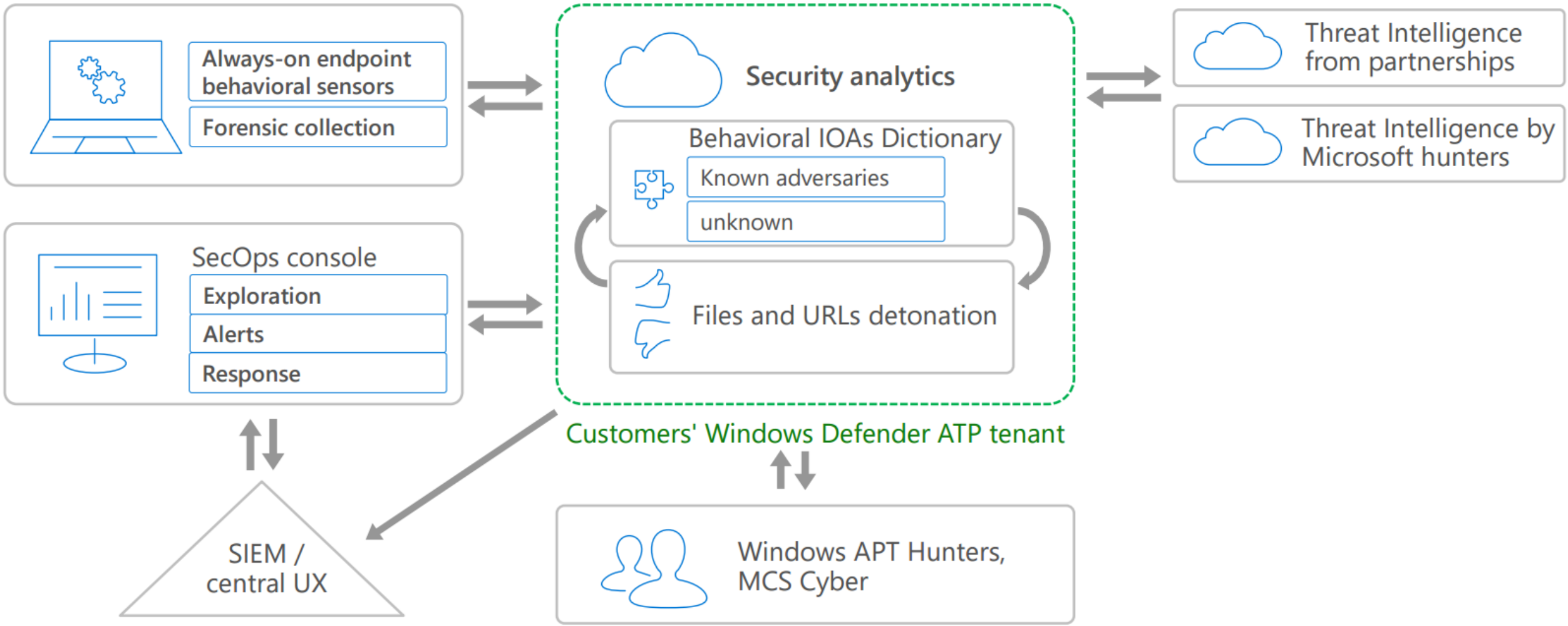
Easily understand scope of breach. Data pivoting across endpoints. Deep file and URL analysis.

## Unique threat intelligence knowledge base

Unparalleled threat optics provide detailed actor profiles
1st and 3rd party threat intelligence data.

## Response based on the Windows stack

Rich SOC toolset ranging from machine-specific intervention or forensic actions to cross-machine blacklisting


Always-on endpoint behavioral sensors
Forensic collection
SecOps console
Exploration
Alerts
Response
Security analytics
Behavioral IOAs Dictionary
Known adversaries
unknown
Files and URLs detonation
Threat Intelligence from partnerships
Threat Intelligence by Microsoft hunters
Customers' Windows Defender ATP tenant
SIEM / central UX
Windows APT Hunters, MCS Cyber

# WHAT'S NEW IN THE CREATORS UPDATE

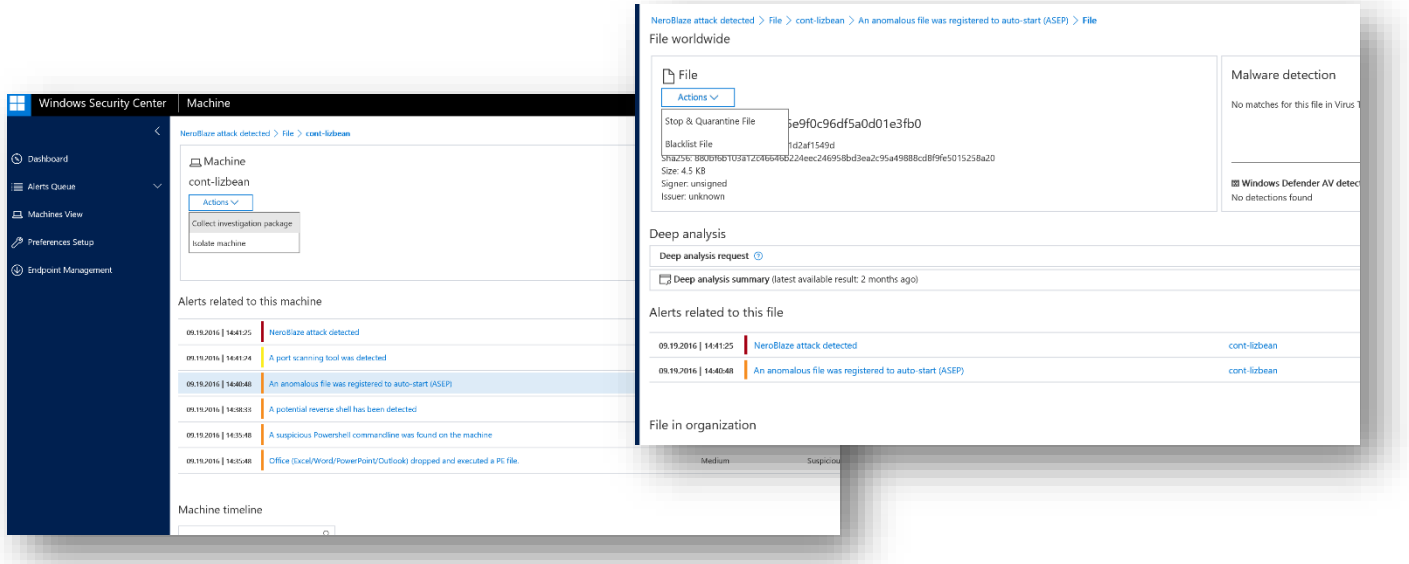
- Response
  - Machine isolation
  - Machine snapshot collection
  - Kill & Clean running processes / files
  - Blacklist from my network (requires WD-AV)
- Enhanced detection
  - Sensor enhancements – memory and kernel attacks
  - Customer specific TI feeds
  - 3rd party TI feeds – FireEye iSight Threat Intelligence
- Integration across the Microsoft security stack
  - Exposing Windows Defender Anti-malware and Device Guard events in the Windows Security Center
  - Office365 ATP integration
- Long list investigation enhancements – listening to customers feedback
  - User view
  - Alert process tree and security graph
  - Virus-total integration
  - …

# RESPONSE

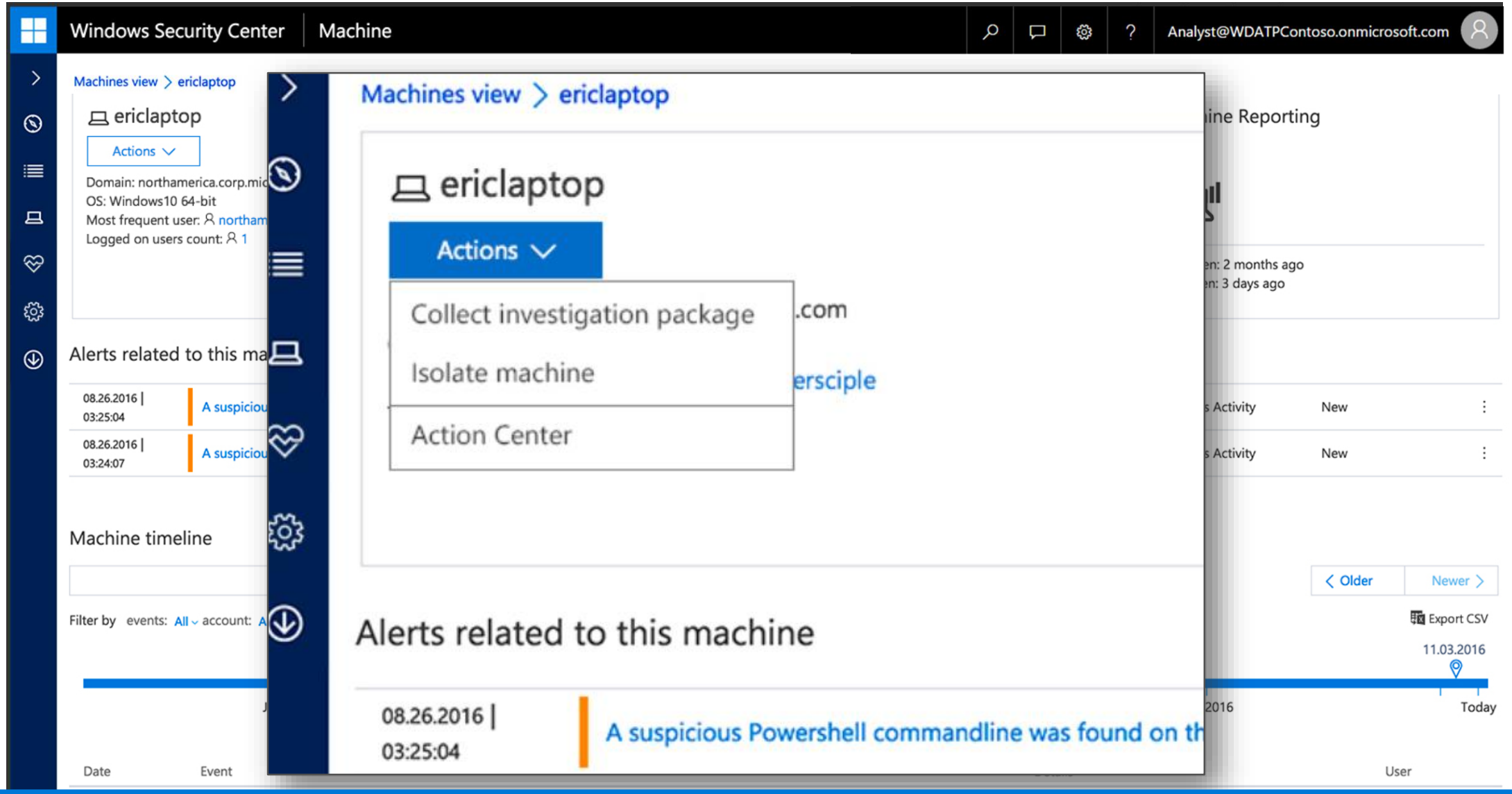
# WHY IS RESPONSE **IMPORTANT**?

Security operations can respond to compromises on their endpoints by taking action to contain the incident and remediate infected endpoints. **The ability to contain attack fast means reducing/preventing further damage to the business**

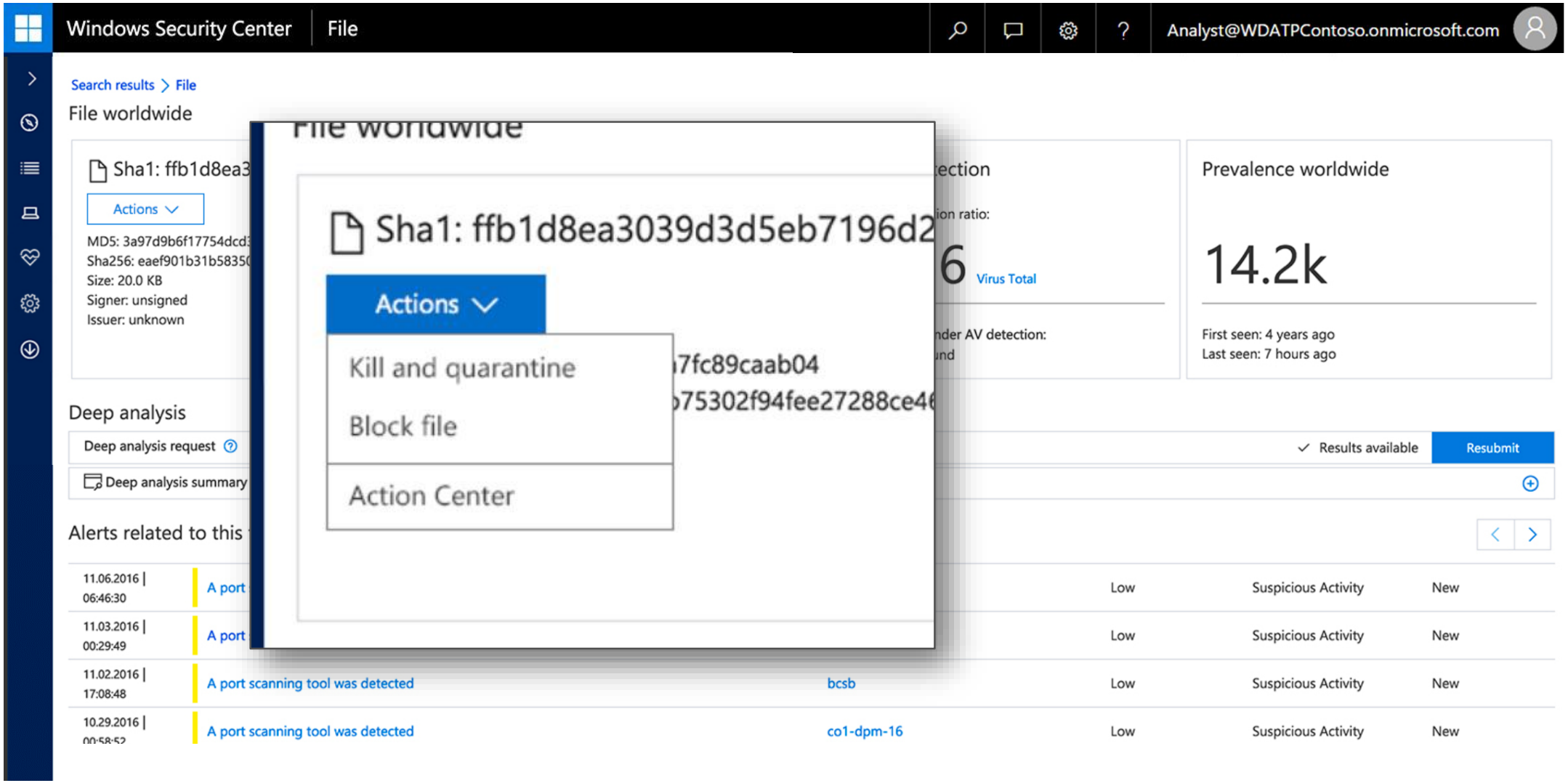
1. **STOP running processes:** Contain the specific attack across the org
2. **BLOCK files**: Assure the specific attack vector will not return to the org from the Internet
3. **ISOLATE Machine:** Stop the bleeding – stop exfiltration & lateral movement
4. **COLLECT forensic data**: Collect more data to better understand the attacker



# MACHINE LEVEL RESPONSE



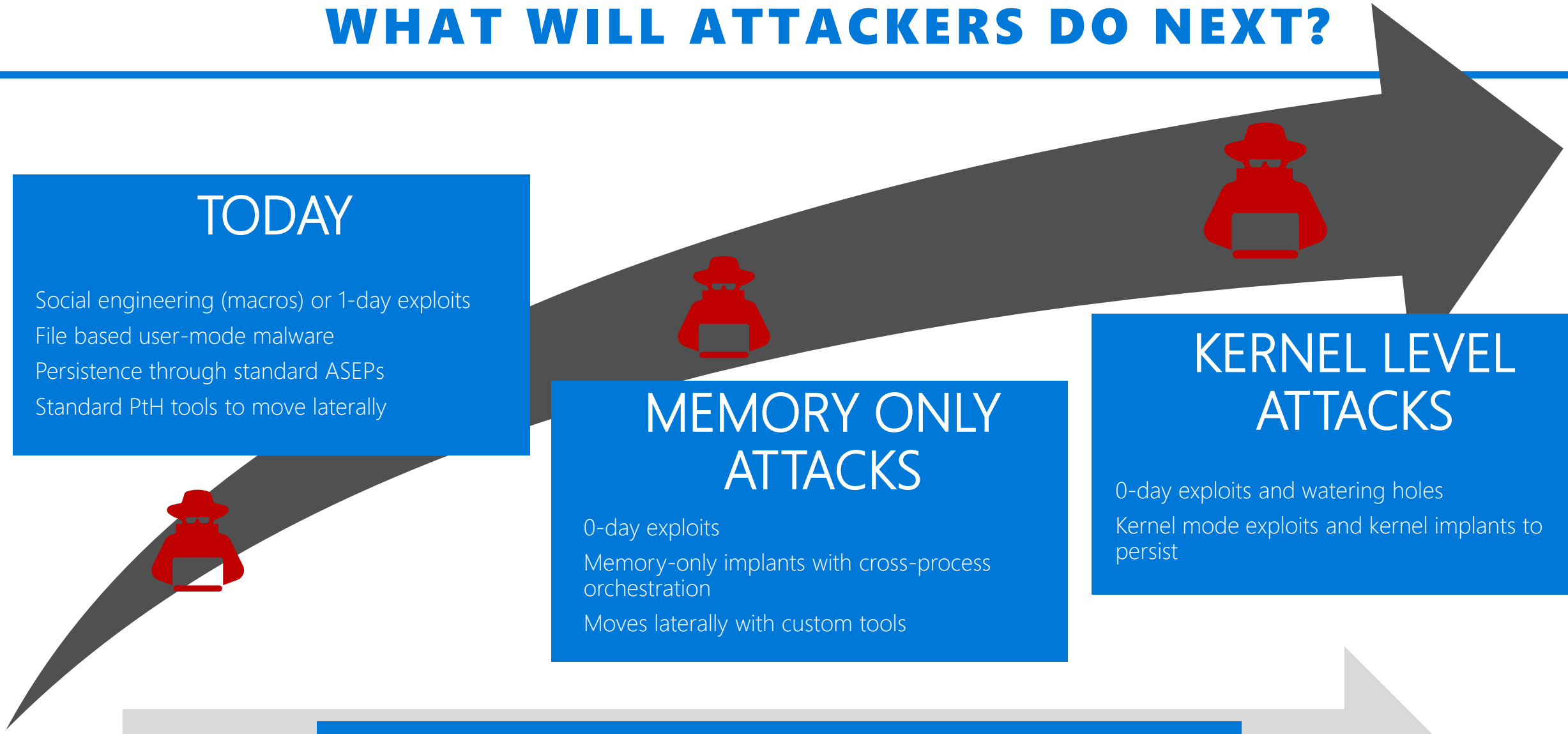
# FILE LEVEL RESPONSE



# NEW SENSORS

Windows

# WHAT WILL ATTACKERS DO NEXT?



## TODAY

Social engineering (macros) or 1-day exploits

File based user-mode malware

Persistence through standard ASEPs

Standard PtH tools to move laterally

## MEMORY ONLY ATTACKS

0-day exploits

Memory-only implants with cross-process orchestration

Moves laterally with custom tools

## KERNEL LEVEL ATTACKS

0-day exploits and watering holes

Kernel mode exploits and kernel implants to persist

## Evolve optics & detection

machine1

## Machine
machine1

Domain:
OS: Windows10 64-bit

## Machine IP Addresses

Last external IP: 167.220.1.71
Last internal IP: 10.216.162.141

## Machine Reporting

First seen: a month ago
Last seen: 35 minutes ago

## Alerts related to this machine

| | | | | |
|---|---|---|---|---|
| 11.01.2016 \| 15:48:09 | Process has injected code into another process. | Medium | Installation | New |
| 11.01.2016 \| 15:48:05 | Indicators of successful exploitation have been observed | High | Exploit | |
| 10.31.2016 \| 21:44:41 | Process has injected code into another process. | Medium | Installation | New |
| 10.27.2016 \| 18:55:19 | Indications of successful exploitation has been observed | High | Exploit | New |
| 10.27.2016 \| 17:59:03 | Indications of successful exploitation has been observed | High | Exploit | New |

## Machine timeline

Older | Newer

Filter by events: All account: All

11.17.2016

Jun 2016 | Jul 2016 | Aug 2016 | Sep 2016 | Oct 2016 | Nov 2016 | Today

| Date | Event | Details | User |
|---|---|---|---|
| 11.17.2016 | | | |
| 14:51:39 | svchost.exe ran backgroundtaskhost.exe | services.exe > svchost.exe > process | SYSTEM |
| 14:51:38 | BackgroundTransferHost.exe communicated with 2 IPs | svchost.exe > BackgroundTransferHost.exe > 2 IPs | kapi3845 |

machine1

## Machine
machine1

Domain:
OS: Windows10 64-bit

## Machine IP Addresses

Last external IP: 167.220.1.71
Last internal IP: 10.216.162.141

## Machine Reporting

First seen: a month ago
Last seen: 35 minutes ago

## Alerts related to this machine

| | | | | |
|---|---|---|---|---|
| 11.01.2016 \| 15:48:09 | Process has injected code into another process. | Medium | Installation | |
| 11.01.2016 \| 15:48:05 | Indicators of successful exploitation have been observed | High | Exploit | New |
| 10.31.2016 \| 21:44:41 | Process has injected code into another process. | Medium | Installation | New |
| 10.27.2016 \| 18:55:19 | Indications of successful exploitation has been observed | High | Exploit | New |
| 10.27.2016 \| 17:59:03 | Indications of successful exploitation has been observed | High | Exploit | New |

## Machine timeline

Older | Newer

Filter by events: All account: All

11.17.2016

Jun 2016 | Jul 2016 | Aug 2016 | Sep 2016 | Oct 2016 | Nov 2016 | Today

| Date | Event | Details | User |
|---|---|---|---|
| 11.17.2016 | | | |
| 14:51:39 | svchost.exe ran backgroundtaskhost.exe | services.exe > svchost.exe > process | SYSTEM |
| 14:51:38 | BackgroundTransferHost.exe communicated with 2 IPs | svchost.exe > BackgroundTransferHost.exe > 2 IPs | kapi3845 |

## Machine

pi3-fuzz

Domain:
OS: Windows10 64-bit

## Machine IP Addresses

Last external IP: 167.220.1.212
Last internal IP: 10.200.156.210

## Machine Reporting

First seen: 21 days ago
Last seen: 24 minutes ago

## Alerts related to this machine

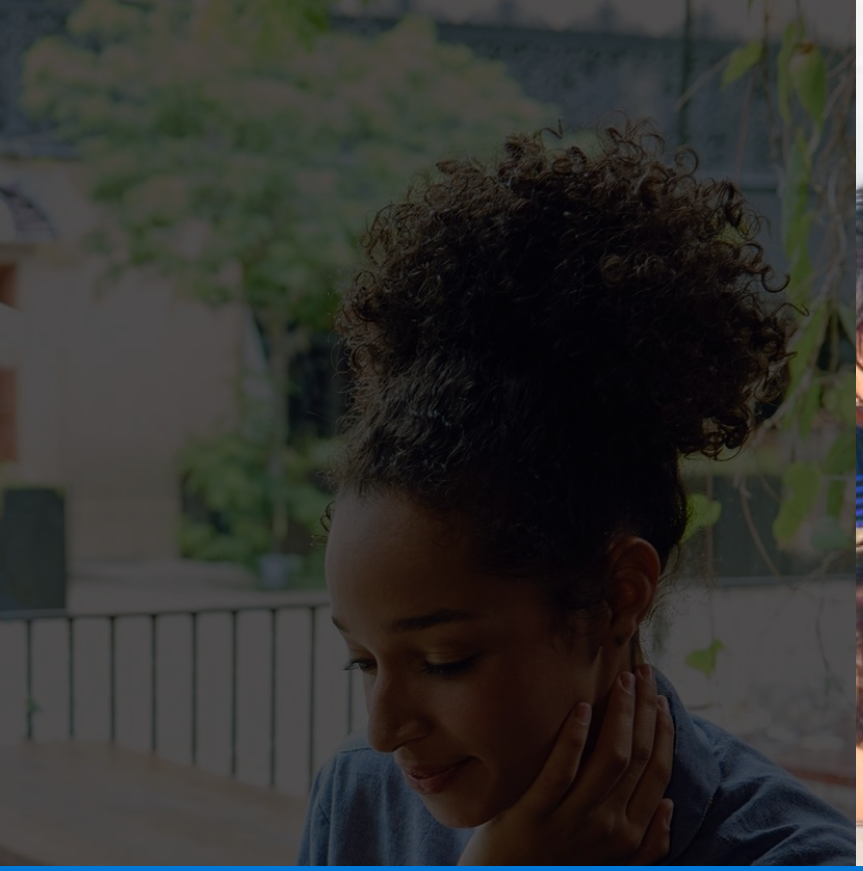
| | | | |
|---|---|---|---|
| 10.31.2016 \| 22:36:17 | An attacker has maliciously modified the Windows Kernel state | Medium | Malware |

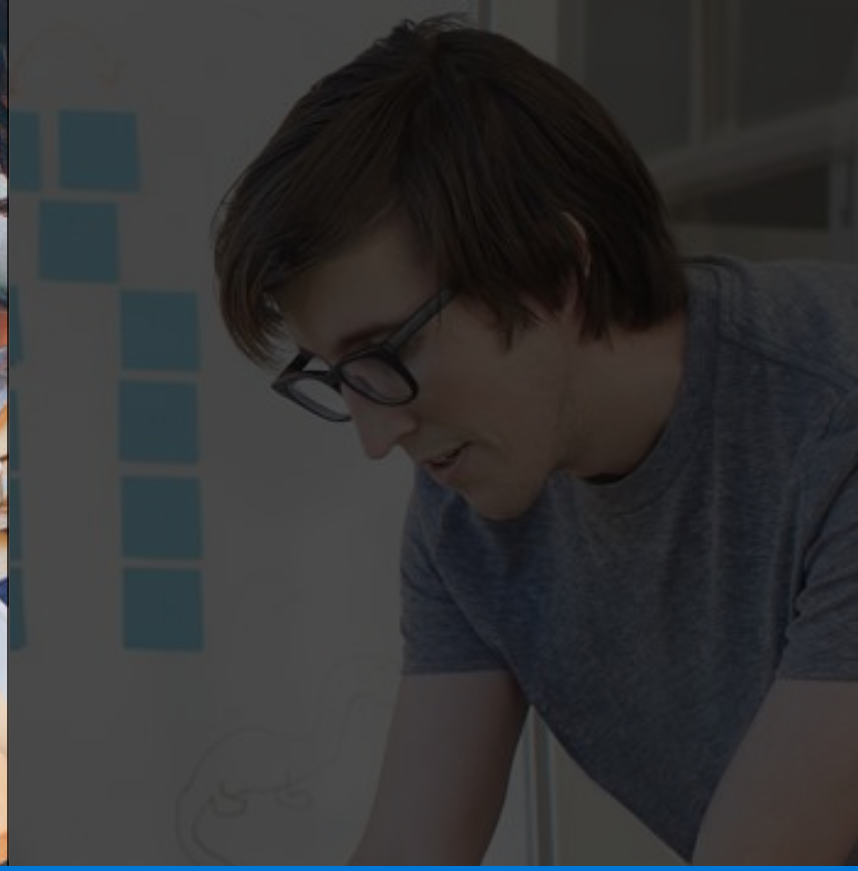
## Machine timeline

Older | Newer

Filter by events: All account: All

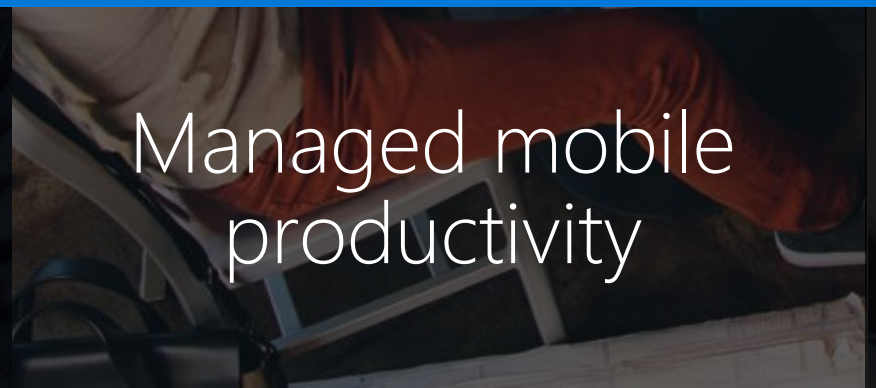

| Date | Event | Details | User |
|---|---|---|---|
| 11.17.2016 | | | |
| 15:17:31 | svchost.exe changed 1 registry value | services.exe > svchost.exe > PinRulesLastSyncTime | NETWOR... |
| 15:10:56 | svchost.exe ran dllhost.exe | services.exe > svchost.exe > process | SYSTEM |
| 14:58:39 | MsMpEng.exe created a PE file under ProgramData folder | services.exe > MsMpEng.exe > file | SYSTEM |
| 14:58:39 | MsMpEng.exe created mpengine.dll | services.exe > MsMpEng.exe > mpengine.dll | SYSTEM |
| 14:58:27 | MpSigStub.exe created 2 files | AM_Delta_Patch_1.231.2177.0.exe > MpSigStub.exe > 2 files | SYSTEM |
| 14:58:14 | svchost.exe created a PE file under Windows folder | services.exe > svchost.exe > file | SYSTEM |
| 14:58:14 | svchost.exe created AM_Delta_Patch_1.231.2177.0.exe | services.exe > svchost.exe > AM_Delta_Patch_1.231.2177.0.exe | SYSTEM |



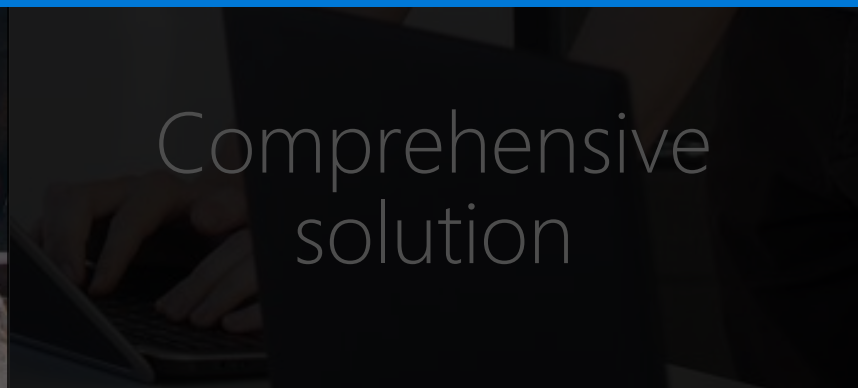


# ENTERPRISE MOBILITY + SECURITY

Identity-driven security



Managed mobile productivity



Comprehensive solution

# Before we start ANY Cloud project

Defense-in-Depth MUST NECESSARILY BE implemented for on-premises infrastructure before any other projects

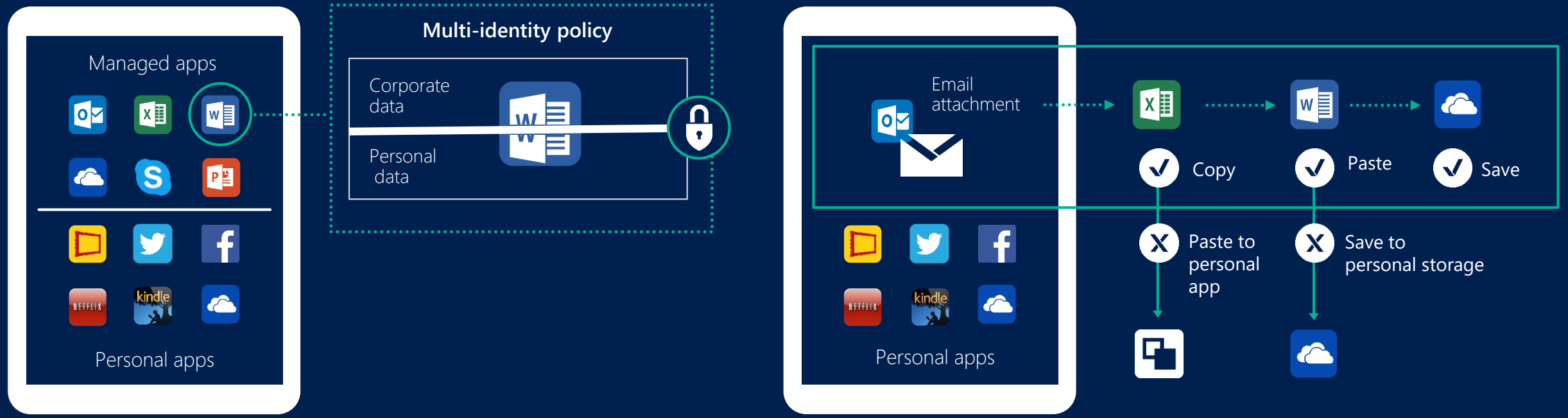
| Security layer | Includes… |
|---|---|
| Data | Access control list (ACL), encryption (Encrypting File System [EFS], BitLocker), data classification with RMS |
| Application | Application design using the security development lifecycle, antivirus, application hardening |
| Host | Operating system hardening, authentication, update management, host intrusion detection system |
| Internal network | Network segmentation, network encryption (Internet Protocol security [IPSec]), network intrusion detection system |
| Perimeter | Firewalls, network access control, network access protection (NAP) |
| Physical security | Guards, locks, tracking devices, surveillance cameras |
| People, policies, processes | Security awareness training, documentation, banners, warning signs |

- Start any new security project's discussion with Defense-in-Depth methodology/strategy
- Cloud (and hybrid cloud especially) solutions are just reflection of customer on-premises infra's security
- Most common attacks to the cloud start with on-premises' breaches

# Managed mobile productivity

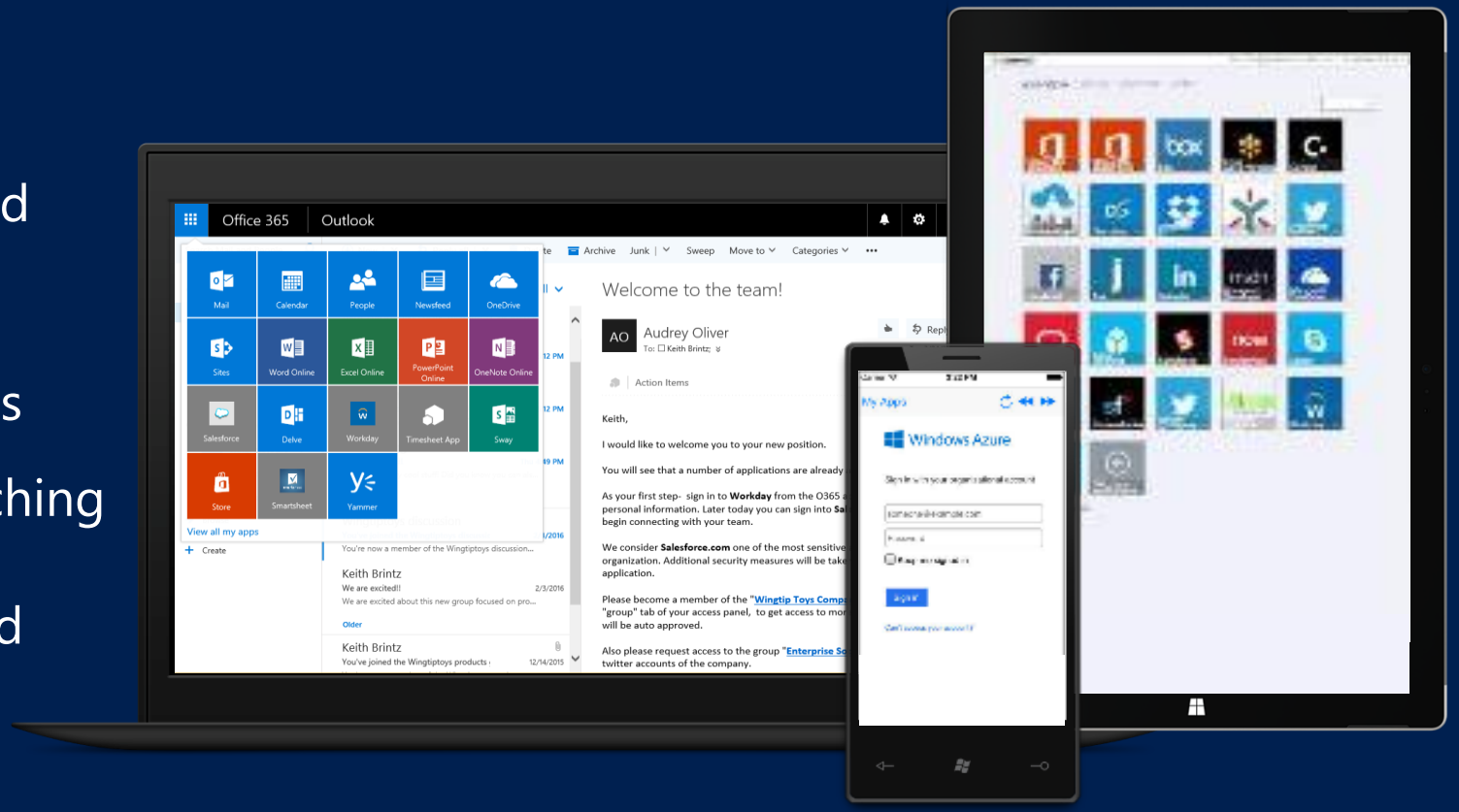
Unsecured apps 80%

# Mobile app management



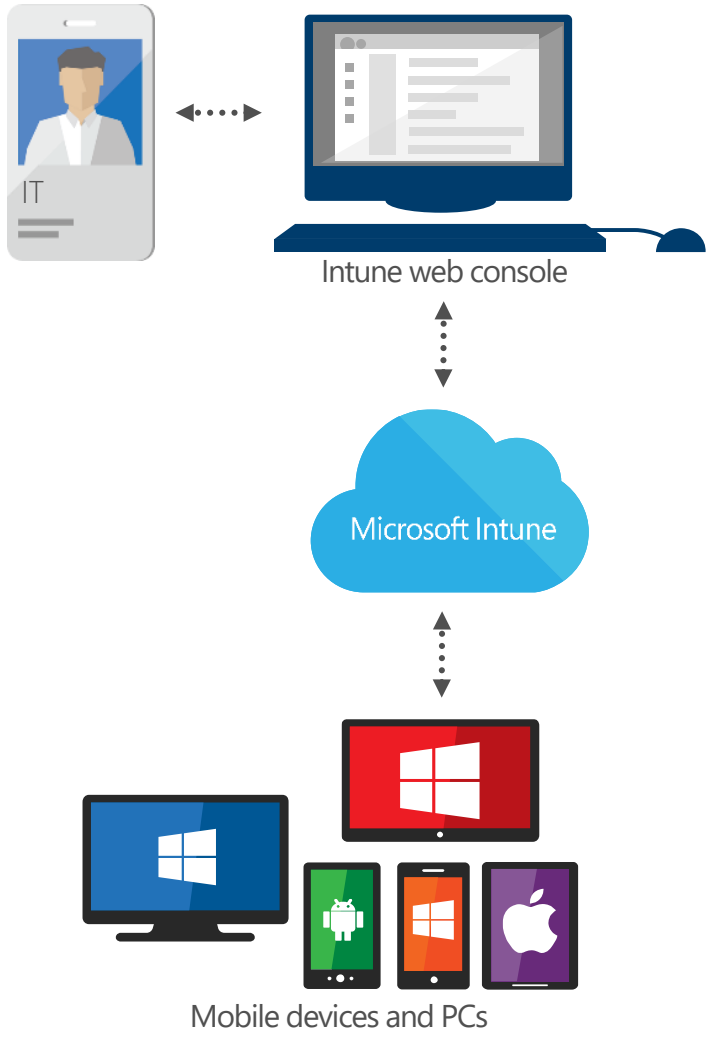
# Making the lives of users (and IT) easier

- Company branded, personalized application Access Panel:
  http://myapps.microsoft.com
  + iOS and Android Mobile Apps
- Integrated Office 365 app launching
- Manage your account, apps and groups
- Self-service password reset
- Application access requests

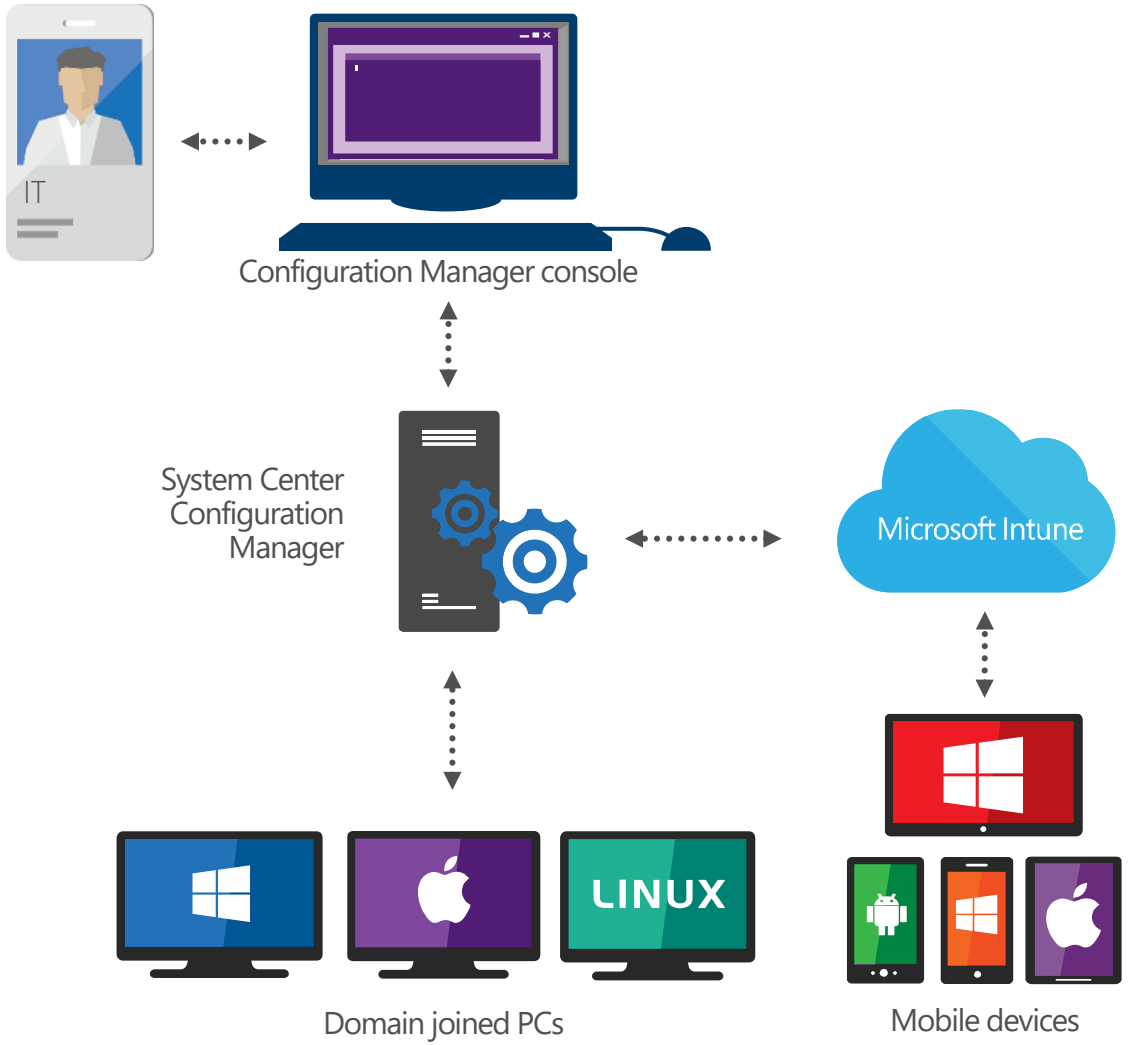


# Intune Deployment for MDM

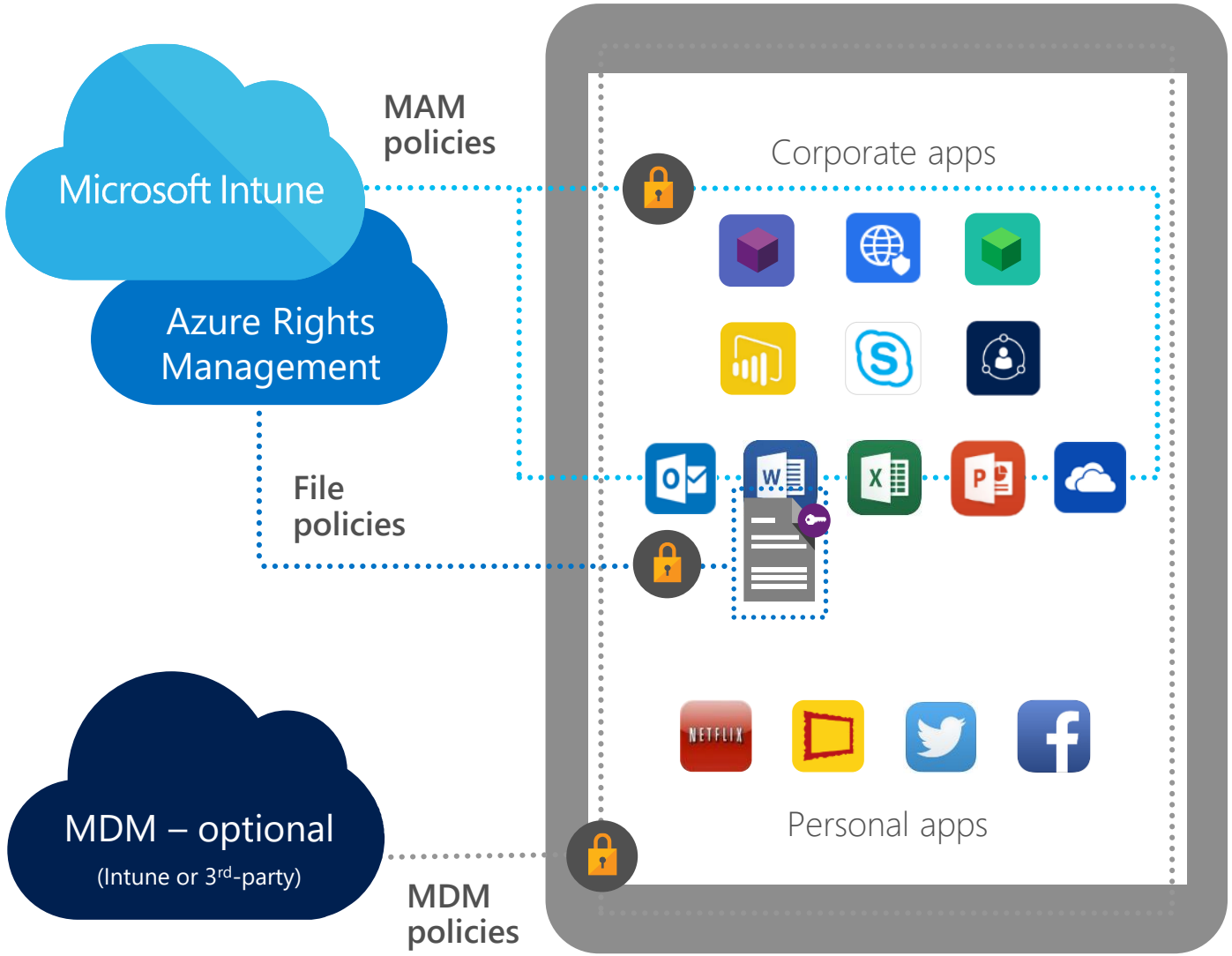
## Intune standalone (cloud only)




## Configuration Manager integrated with Intune (hybrid)



# Intune Deployment for MAM




**Familiar Office experience**

- **Seamless "enrollment"** into app management
- Use for **personal** and **corporate** accounts

**Comprehensive protection**

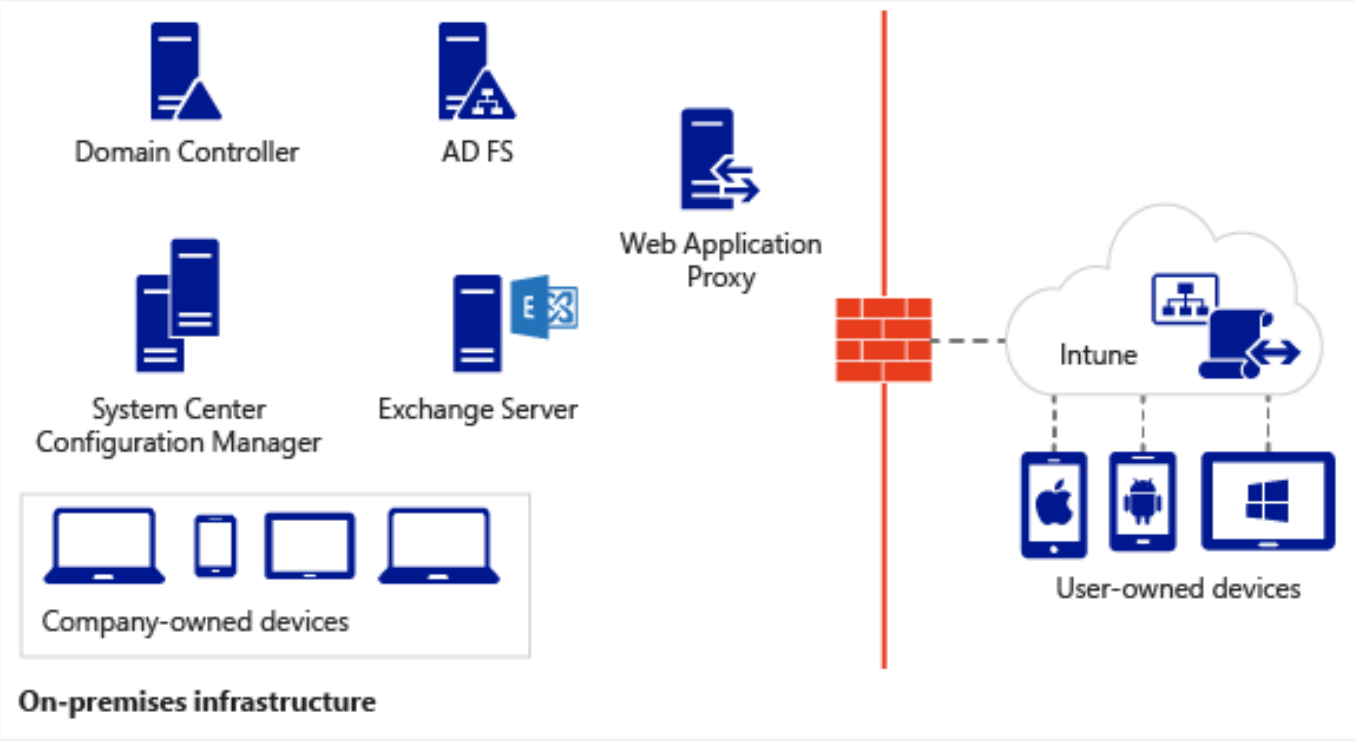
- **App encryption** at rest
- **App access control** – PIN or credentials
- Save as/copy/paste **restrictions**
- App-level **selective wipe**
- Extend **protection** to a file level with **Azure RMS**

**Might be a good solution for these scenarios:**

- **BYOD** when MDM is not required
- Extending **app access** to vendors and partners
- Already have an **existing MDM** solution

# STEP 1: Identify business needs - Device ownership

You must understand the device ownership policy for customer's company




- Who owns the mobile device?
  - The employee (**BYOD**)?
  - The **company**?
  - **Both**?

# STEP 1A: Device ownership comparison

Strategy adoption

| Scenario | PROS | CONS |
|---|---|---|
| **Employee owns the device (BYOD)** | • Your company **does not need to buy** mobile devices for the employees<br>• Usually **allows employees to be more productive** since they will be using the mobile device of their choice<br>• Support **costs may decrease** since the organization will have limited support over the mobile devices | • **Increases the amount of security considerations** to protect company's data located on personal devices<br>• **Increases likelihood of data leakage**, especially when appropriate security controls aren't in place<br>• **Limited management capability** due to privacy restrictions |
| **Company-owned device** | • **Full management capability**, including device hardening and security controls<br>• **More control** over mobile devices<br>• **Capability of defining** which mobile devices will be used by employees | • **Potential increases in support costs**, since the organization will maintain the mobile devices<br>• **Less flexibility** for end users, which may affect their productivity<br>• **Cost increases**, since the organization will have to buy mobile devices |

# STEP 2: Identify business needs - Platforms

Understanding which mobile device operating systems will be used by the company is very important for adoption and supportability decisions


- Which mobile device **operating systems** will be supported?
  - Android?
  - iOS?
  - Windows?
  - Windows Phone?
  - All of them?
  - A mix of the above options?
- Which **mobile OS version** will be supported?
  - Only the latest?
  - Current -1 (current version plus the previous version)?

# STEP 2A: Supported mobile device platforms

| Сценарий | PROS | CONS |
|---|---|---|
| **Intune (standalone)** | • **Always-on** cloud service that **supports the latest MDM** features and updates<br>• **Supports provisioning all major mobile device** operating systems (Android, iOS, Windows 8, Windows 10, and Windows Phone).<br>• Allows you to **manage any mobile device** from any location<br>• More **advanced management options** for mobile devices<br>• **Mobile application management** capability | • **Lack of integration** with current device management solution located on-premises will introduce an additional management interface for you to use<br>• Policies created using the on-premises MDM solution are **not replicated to the cloud** service |
| **MDM for Office 365** | • **Integrated with Office 365**<br>• If you're **already using** Office 365, the MDM capabilities are easily leveraged to manage mobile devices<br>• If you're already using Office 365, you **won't need** to use another console to manage mobile devices | • **Limited set** of capabilities to manage mobile devices<br>• **Lack of integration** with current device management solution located on-premises will introduce an additional management interface for you to use |
| **Hybrid (Intune with ConfigMgr)** | • **Native integration** between Intune and ConfigMgr<br>• Allows you to use a **centralized console** to deploy policies and manage on-premises PCs, servers, and mobile devices | • **Requires additional configuration** steps to connect Intune and ConfigMgr<br>• If the organization **does not have a current ConfigMgr** infrastructure on-premises, it will require to plan, install and configure this platform prior to the integration |

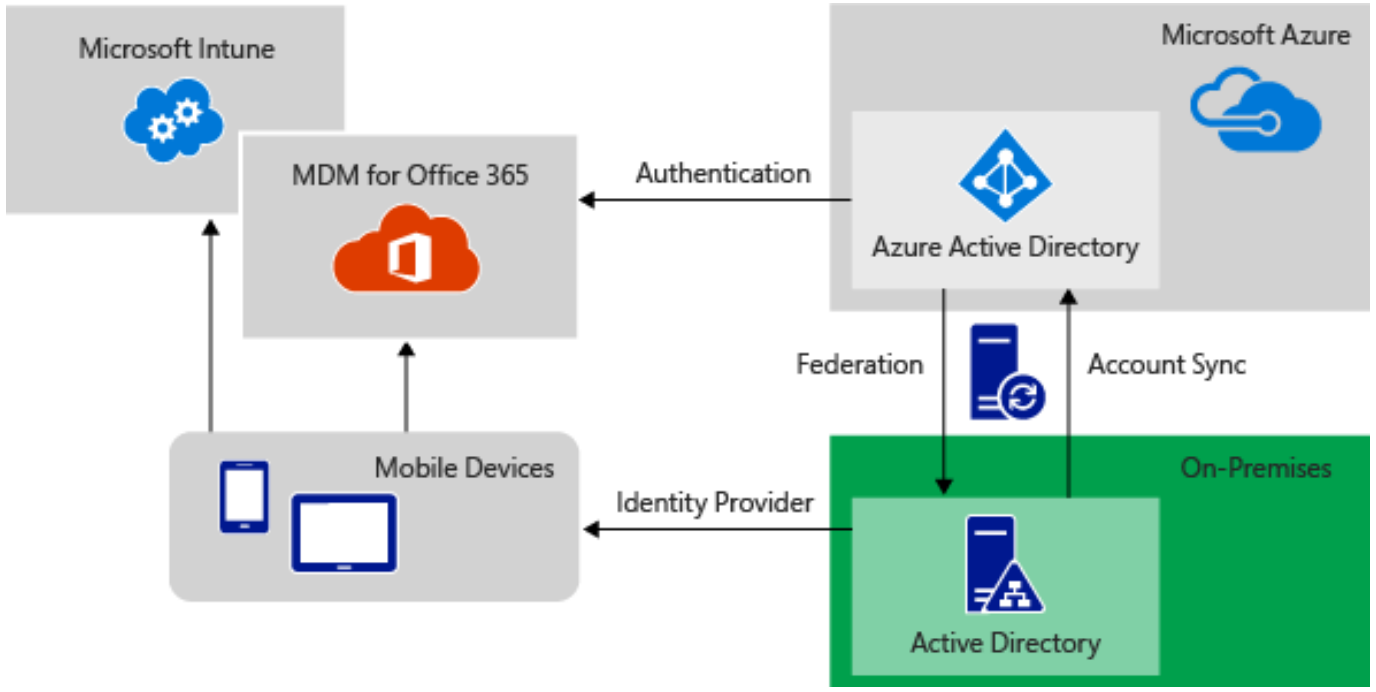
# STEP 3: Identify business needs – Applications

- Do the apps require **integration with cloud services**?
- Were the apps developed **to run on a specific operating system**, or are they capable of running on any operating system?
- Does company plan to enable users to **use apps via remote desktop** from their own devices?
- Do the apps require **full-time access to corporate resources**, or can they run in offline mode?
- Will all **apps be available to BYOD users**?
- **How does customer plan to deploy** these apps to users' devices?
- What are the **deployment options** for these apps?
- Does **the installation requirement** vary according to the target device, or is it the same?
- **How much space** in a target device is necessary in order to install each app?
- Do the **apps encrypt the data** before transmitting it through the network from the users' devices to the app server on the back end?
- Can the **apps be remotely uninstalled** via the network, or do they need to be uninstalled via the devices' consoles?
- Do the apps work **in a low-latency network**?
- Do the apps provide **authentication capabilities**?

# STEP 3A: Mobile Apps Management comparison

| | | |
|---|---|---|
| Intune (standalone) | • Allows you **to manage mobile apps** through their lifecycle, including app deployment from installation files and app stores, detailed monitoring of app status, and app removal.<br>• Allows you to **specify a list of compliant apps** that users are allowed to install and noncompliant apps, which must not be installed by users.<br>• Allows you to **set restrictions for apps** by using a mobile application management policy. This helps you to increase the security of your company data by restricting operations such as copy and paste, external data backup, and the transfer of data between apps. | • **Lacks integration with on-premises** device management solutions, which introduces an additional management interface for you to use when managing mobile devices if you have an on-premises solution. Policies created using an on-premises MDM platform aren't replicated to the cloud service, requiring two sets of management and compliance policies (if you have ab on-premises MDM solution) |
| MDM for Office 365 | • Provides MDM capabilities across OS **platforms such as password requirements** | • **Limited set of capabilities to control apps**<br>• **Lacks integration** with on-premises device management solutions, which introduces an additional management interface for you to use when managing mobile devices if you have an on-premises solution.<br>• **No ability to deploy apps** and apply mobile application management capabilities<br>• **No advanced MDM capabilities** |
| Hybrid (Intune with ConfigMgr) | • **Inherits app control settings** from Intune standalone<br>• **Provides an integrated management** experience (between Intune and ConfigMgr)<br>• **Leverages Configuration Manager App management capabilities**.<br>• Allows you to **use a single console to deploy policies** and manage application policies for on-premises PCs, servers, and mobile devices | • Requires **additional steps to set up** the integration<br>• If your organization **does not have a current on-premises ConfigMgr** infrastructure, you must plan, install, and configure the ConfigMgr platform first |

# STEP 4: Identify business needs - Identity




- Does your organization **have a current directory service** that is used for authentication and authorization?
- Does your organization need to **have centralized authentication**, or can it be hybrid?
- Does your organization plan to **have multi-factor authentication** for mobile users?
- SSO required?

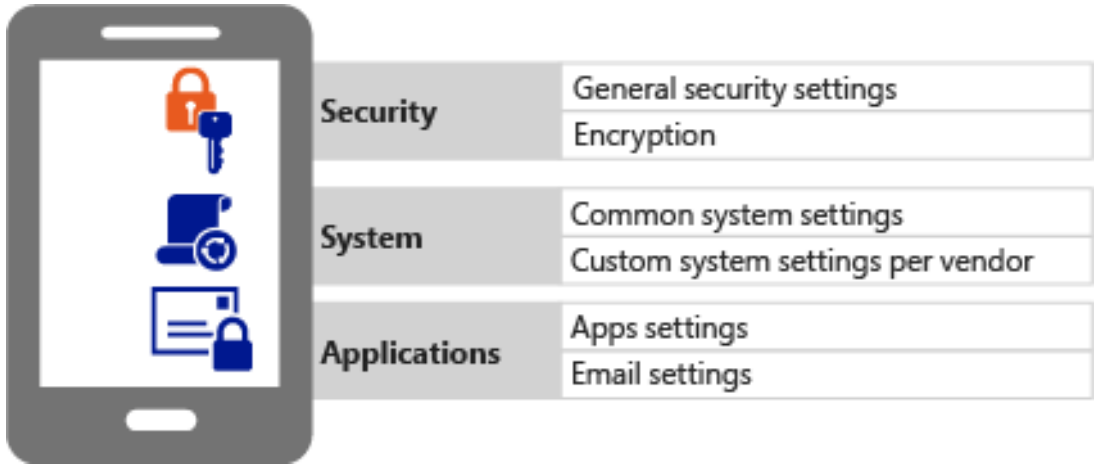
# STEP 4A: MDM's identity support comparison

| | | |
|---|---|---|
| Intune (standalone) | • **Can use on-premises directory services**, such as Active Directory for authentication<br>• **Can use cloud-based directory services**, such as Azure AD for authentication<br>• Can integrate with **multi-factor authentication** | • **Azure AD cloud service is not included** when customer purchases an Intune subscription |
| MDM for Office 365 | • **Can use on-premises directory**, such as Active Directory for authentication<br>• **Can use cloud** based directory, such as Azure AD for authentication<br>• Can integrate with **multi-factor authentication** | • **Azure AD cloud service is not included** when customer purchases an Office 365 subscription |
| Hybrid (Intune with ConfigMgr) | • **Can use on-premises directory**, such as Active Directory for authentication<br>• **Can use cloud based directory**, such as Azure AD for authentication<br>• Can integrate with **multi-factor authentication** | • **Azure AD cloud service is not included** when you purchase an Intune subscription |
| Enterprise Mobility + Security | • Leverages **Azure AD Premium** to provide access control<br>• Azure AD Premium license is **already included with EMS**<br>• **Does not required on-premises** directory services<br>• **Can synchronize** with on-premises Active Directory services<br>• **MFA** is natively **available** with **EMS** | • **Not available** for customers that are not adopting a cloud-based solution |

# STEP 4B: MDM's identity support comparison

| | | |
|---|---|---|
| Intune (standalone) | • **Tightly integrated with Azure Active Directory** for managing user and device identity and authentication<br>• **Supports user credential self-management** and single sign-on experiences that can leverage existing on-premises account credentials<br>• Supports **single sign-on access** to thousands of pre-integrated SaaS applications<br>• Supports **application access security** by enforcing rules-based multifactor authentication (MFA) for both on-premises and cloud applications | • Advanced directory services connectivity features and functionality **require pairing** with Azure Active Directory Premium |
| MDM for Office 365 | • **Integrated with Office 365 tenants**, which use the Azure Active Directory backbone for managing user and device identity and authentication<br>• **On-premises directory** services can be connected as a part of connecting services with Office 365<br>• Supports user **self-management** and single sign-on experiences that can leverage existing on-premises account credentials | • **Doesn't support mobile application management** integration with other SaaS solutions or applications<br>• Doesn't support multi-factor authentication |
| Hybrid (Intune with ConfigMgr) | • **All the advantages of Intune standalone**, plus the following:<br>  • Direct integration with on-premises directory services through ConfigMgr infrastructure | • For organizations that **don't have a current ConfigMgr** infrastructure configured, it will need to be planned, installed and configured prior to integrating with Intune<br>• Requires **additional on-premises deployment** requirements and configuration changes for organizations with ConfigMgr |

# STEP 5: Identify business needs - Hardening devices



| | |
|---|---|
| **Security** | General security settings |
| | Encryption |
| **System** | Common system settings |
| | Custom system settings per vendor |
| **Applications** | Apps settings |
| | Email settings |

- Options that should be supported by the MDM solution to harden mobile devices:
  - **Requiring a password** to unlock mobile devices
  - Requiring a **password type** – minimum number of characters and character types
  - **Minimum password** length
  - Number of **repeated sign-in failures** to allow before the mobile device is wiped
  - **Minutes of inactivity** before the device screen turns off
  - **Remembering password history** – preventing the reuse of previous passwords
  - **Password expiration** (days)
  - **Requiring encryption** on the mobile device
  - Requiring encryption on **storage cards**
  - **Allowing idle return** without a password

# STEP 5A: MDM's identity support comparison

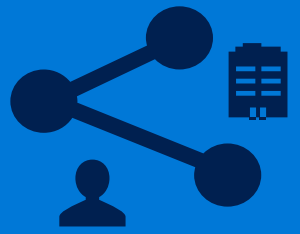
| | | |
|---|---|---|
| Intune (standalone) | • Allows you to enforce policies for enrolled devices:<br>  • **Encryption, Malware, Apps**<br>  • **Emails, Email Profile**<br>  • **Jailbroken**<br>  • **System, Security**<br>• Supports policy deployment for major mobile device platforms, including (Android, iOS, Windows 10, Windows 8.x, and Windows Phone) | • **Lacks integration** with current on-premises MDM platform, will introduce an additional management interface for you to use when managing mobile devices<br>• **Some policies may not be available** for some mobile platforms |
| MDM for Office 365 | • Allows you to enforce policies for enrolled devices:<br>  • **Encryption, Apps**<br>  • **Jailbroken**<br>  • **Security**<br>• Supports policy deployment for major mobile device platforms, including (Android, iOS, Windows 10, Windows 8.x, and Windows Phone) | • **Lacks integration** with current on-premises MDM platform, will introduce an additional management interface for you to use when managing mobile devices<br>• **Some policies may not be available** for some mobile platforms<br>• **Doesn't allow as much granularity** as Intune |
| Hybrid (Intune with ConfigMgr) | • Allows you to enforce policies for enrolled devices:<br>  • **Encryption, Malware, Apps**<br>  • **Emails**<br>  • **Jailbroken**<br>  • **System, Security**<br>• Supports policy deployment for major mobile device platforms, including (Android, iOS, Windows 10, Windows 8.x, and Windows Phone)<br>• **Single management console for mobile devices** registered from the cloud and on-premises devices | • If company **doesn't have a current on-premises ConfigMgr** infrastructure, it will require resources to plan, install and configure ConfigMgr prior to integration |

# Managed mobile productivity


Secure access to company data with maximum productivity

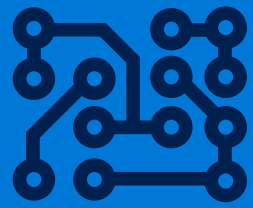
# Data level protection

Protect your data at all times



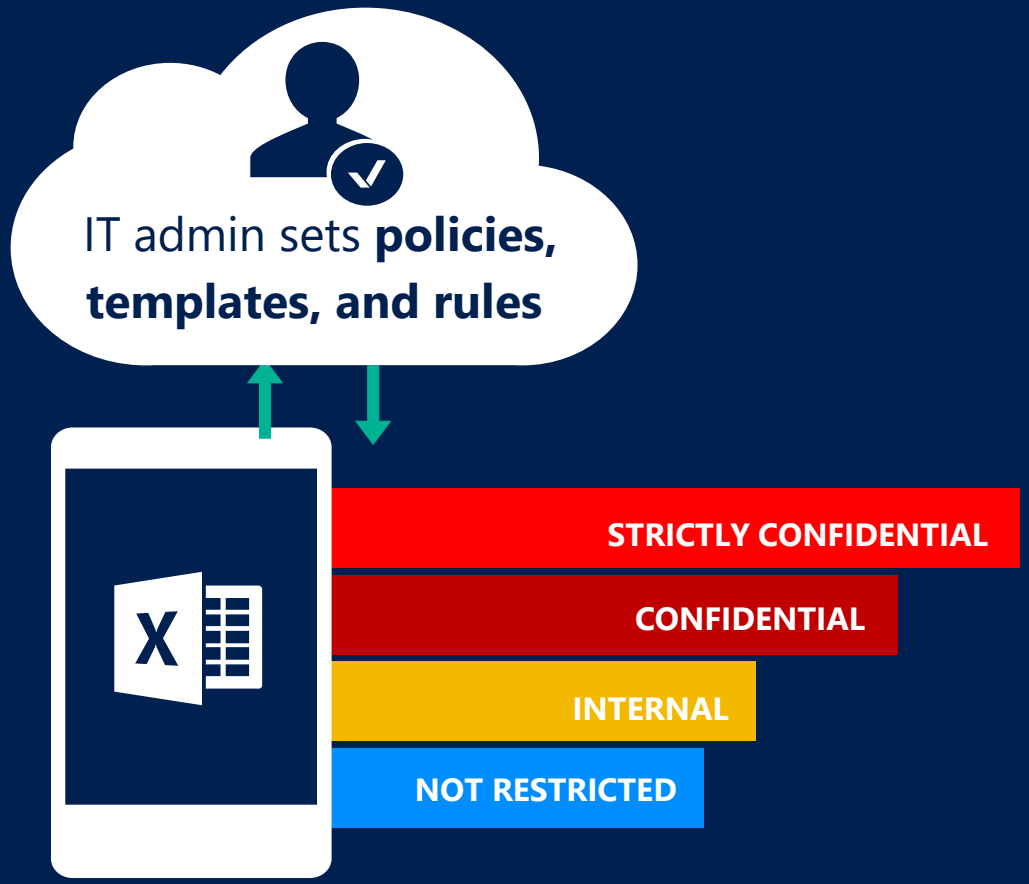
Enable safe sharing internally and externally

Empower users to make right decisions



Maintain visibility and control

# Classify and label data based on sensitivity





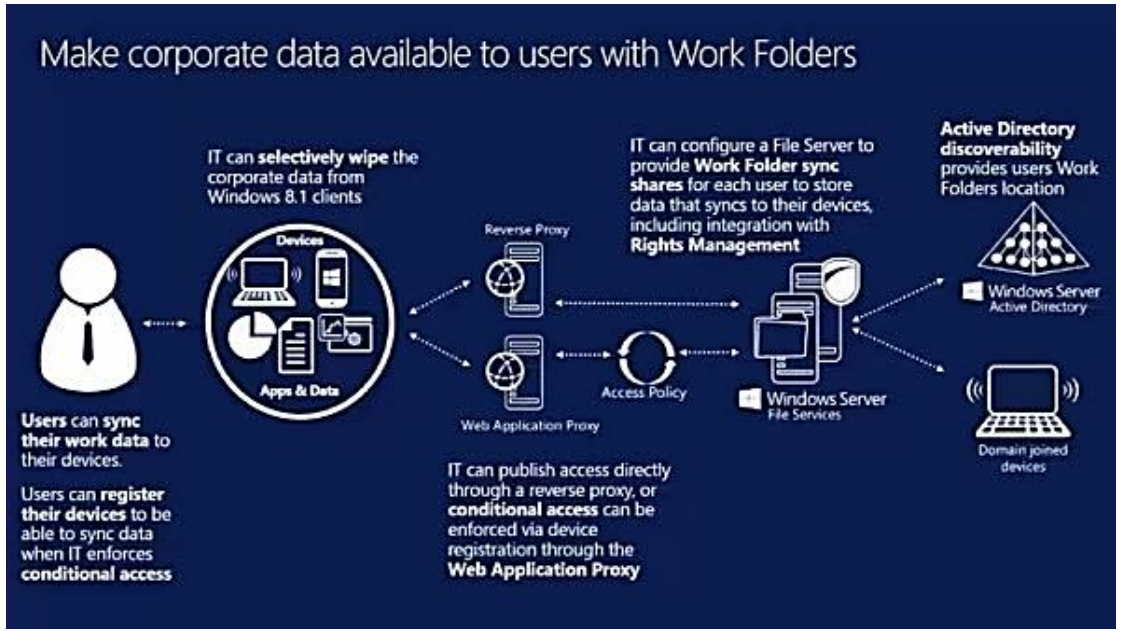
Classify data according to policies – automatically or by user

Add persistent labels defining sensitivity to files

# Opportunities: data leakage cloud prevention's matrix

| Scope/threat | Hacking | Device lost | Accidental access | Data theft |
|---|---|---|---|---|
| Data at rest in mobile Devices | Intune (configuration, compliance), Hybrid Identity/MFA, VBS, DG | Encryption (BitLocker/RMS, Work Folders), Intune (WIP, wipe), MFA | Data Classification/RMS/WIP | RMS/Intune App Policy/WIP |
| Data transfer | DiD | | | |
| Data at rest in on-premises | DiD | Work Folders, Registered Devices, MFA | Data Classification/RMS | RMS |
| Data at rest in cloud | DiD | Work Folders, Hybrid Identity, MFA, Cloud Storages (OneDrive for Business, SharePoint Online), conditional access policies | Azure RMS/Azure IP | Azure RMS/Azure IP |

# Opportunities: Secured access to on-premises data with Work Folders & Azure AD/RMS

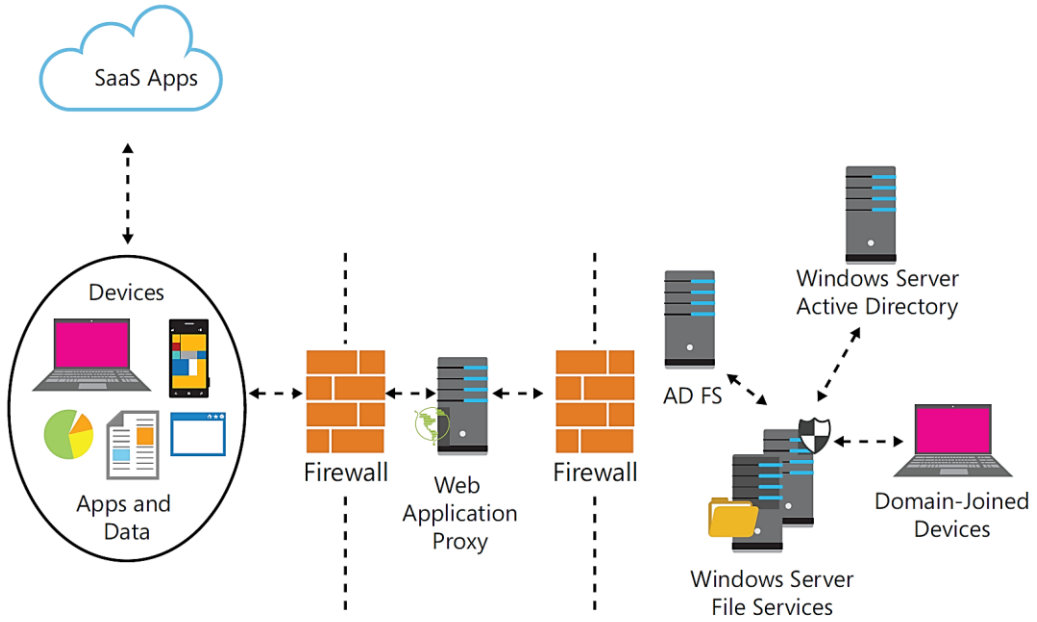



- By **mobile devices** (Windows, iOS, Android)
- **Encrypted at rest** in on-premises servers and in mobile devices
- Work Folder **policies**
- **Intune/Group Policy** enrollment
- Data **synchronization**
- **Azure AD/ADFS federation** for mobile users
- ADFS **conditional access policies**
- **HTTPS** access point
- Publishing by **Web Application Proxy**
- Could be deployed in **Azure IaaS**
- Compatible with **RMS/Azure RMS**

# RMS/Azure RMS Scenarios Comparison

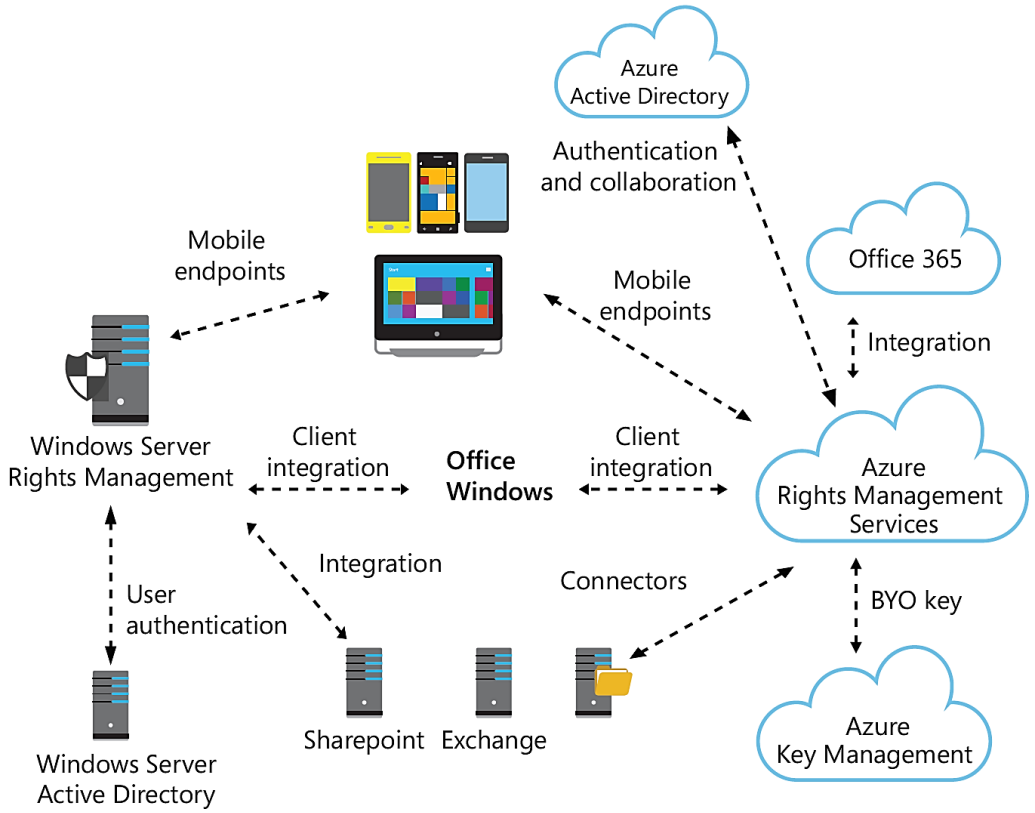
| Scenarios | PROS | CONS |
|---|---|---|
| **Centralized on-premises (Active Directory Rights Management Server)** | • **Full control over the server infrastructure** responsible for classifying the data<br>• **Built-in capability in Windows Server**, no need for extra license or subscription<br>• Can be **integrated with Azure AD** in a hybrid scenario<br>• Supports **information rights management** (IRM) capabilities **in Microsoft Online services** such as Exchange Online and SharePoint Online, as well as Office 365.<br>• Supports **on-premises Microsoft server** products, such as Exchange Server, SharePoint Server, and file servers that run Windows Server and File Classification Infrastructure (FCI). | • **Higher maintenance** (keep up with updates, configuration and potential upgrades) since IT owns the Server<br>• **Require a server** infrastructure on-premises<br>• **Doesn't leverage Azure** capabilities **natively** |
| **Centralized in the cloud (Azure RMS)** | • **Easier to manage** compared to the on-premises solution<br>• Can **be integrated with AD DS** in a hybrid scenario<br>• **Fully integrated with Azure AD**<br>• **Doesn't require a server on-premises** in order to deploy the service<br>• **Supports on-premises Microsoft server** products such as Exchange Server, SharePoint Server, and file servers that run Windows Server and File Classification Infrastructure (FCI).<br>• **IT can** have complete control over their tenant's **key with BYOK capability**. | • Your **organization must have a cloud subscription** that supports **RMS**<br>• Your **organization must have** an **Azure AD directory** to support user authentication for RMS |
| **Hybrid (Azure RMS integrated with On-Premises Active Directory Rights Management Server)** | • This **scenario accumulates the advantages of both**, centralized on-premises and in the cloud. | • Your **organization must have a cloud subscription** that supports RMS<br>• Your **organization must have** an **Azure AD directory** to support user authentication for RMS<br>• **Requires a connection** between **Azure cloud service and on-premises** infrastructure |

# Opportunities: hybrid data protection with RMS on-premises



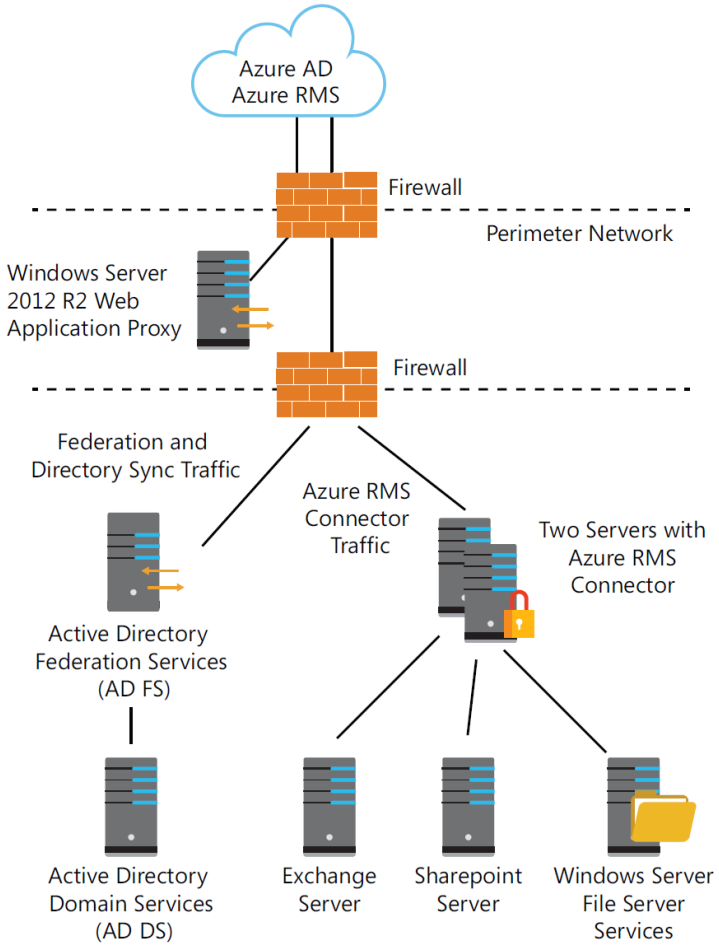

- Planning and deploy AD RMS on-premises servers
- Configure a set of RMS templates/custom templates for documents/emails etc.
- Planning and deploy File Classification Infrastructure for Windows Server File Services
- Configure File Classification on File Servers and turn on RMS Encryption
- Planning and deploy Hybrid Identity with Azure AD/ADFS federation
- Publishing services with WAP

# Opportunities: Planning Azure RMS



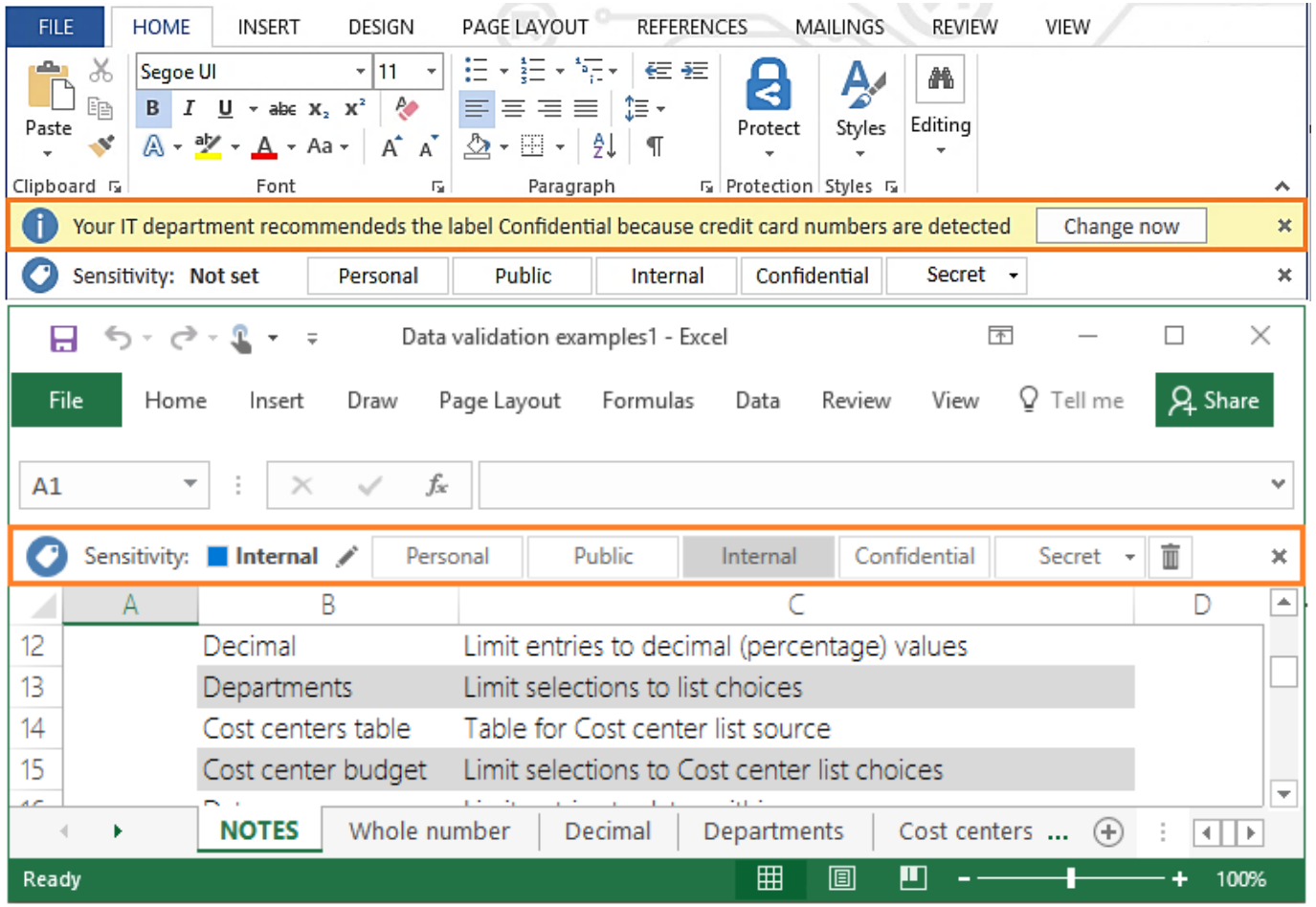

- Bring Your Own Key (BYOK)
- Planning and deploy Hybrid Identity
- Planning hybrid RMS solution with Azure Rights Management connector:
  - Exchange Server
  - Office SharePoint Server
  - Windows Server 2012 FS FCI
- Planning RMS clients' deployment
- Planning Azure Information Protection policies, classifications, tags

# planning Azure RMS connector

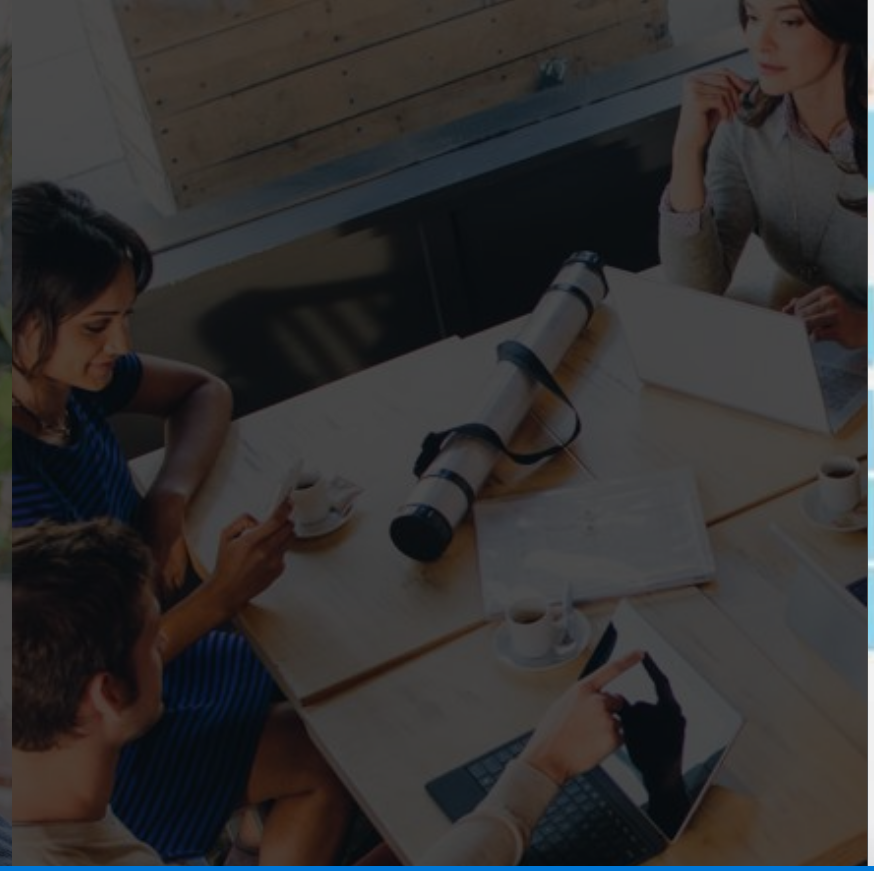



- Azure RMS connector supports:
  - Exchange Server
  - Office SharePoint Server
  - Windows Server 2012 FS FCI
- AD/Azure AD federation with ADFS is required
- Two Azure RMS connector's nodes are recommended for fault tolerance and load balancing.
- Valid & trusted CA certificate.

# Opportunities: Planning Azure Information Protection

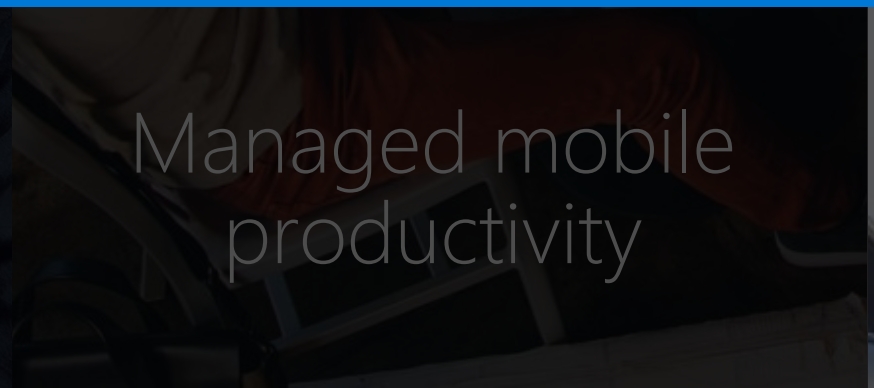


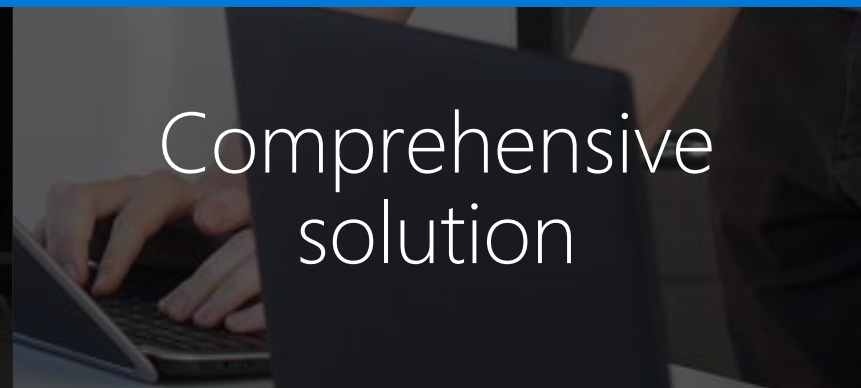

- Azure Information Protection is a cloud-based solution to classify, label, and protect documents and emails.
- Rules detect sensitive data (credit card information, for example).
- The protection technology uses Azure Rights Management (often abbreviated to Azure RMS)
- Configure and deploy classification and labeling
- Prepare for Rights Management data protection
- Install the client and configure applications and services for Rights Management
- Configure your Azure Information Protection policy, applications, and services for Rights Management data protection
- Use and monitor your data protection solutions

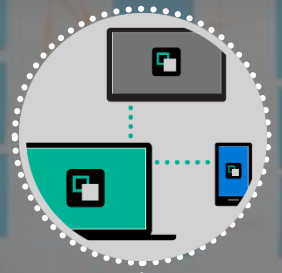

# ENTERPRISE MOBILITY + SECURITY


Identity-driven security


Managed mobile productivity


Comprehensive solution

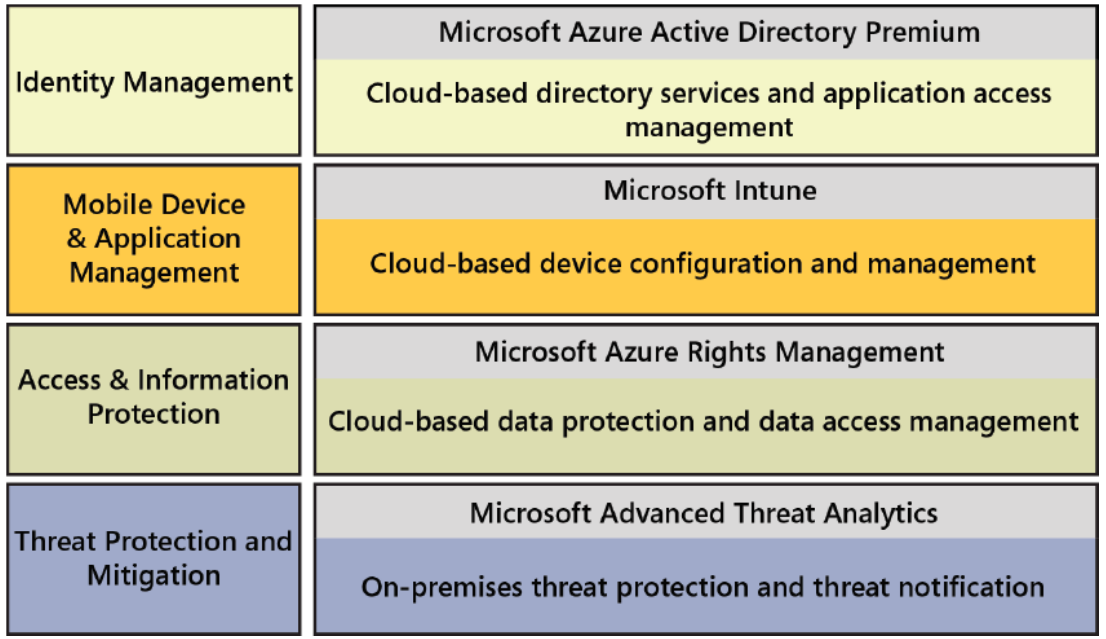
# Comprehensive solution



Global IT Budget growth 2016

0.6%

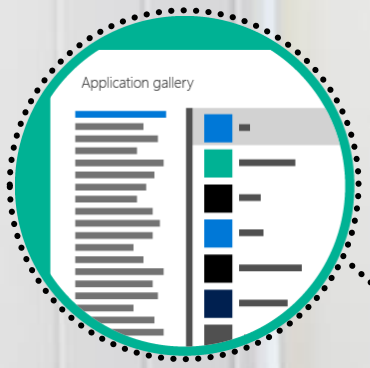
# Identity, Mobile & Data protection services in EMS




| | Enterprise Mobility Suite | Office 365 |
|---|---|---|
| **Identity management** | Azure AD Premium<br>■ Single sign-on for SaaS apps<br>■ Advanced multifactor authentication<br>■ Microsoft Identity Management (MIM) | Identity management enabled by Azure AD<br>■ Basic single sign-on for Office 365<br>■ Basic multifactor authentication for Office 365 |
| **Mobile device and app management** | Microsoft Intune<br>■ MDM and MAM support<br>■ Advanced device and app policies<br>■ System Center integration | MDM for Office 365 enabled by Microsoft Intune<br>■ Basic device settings management<br>■ Selective wipe/device reset<br>■ Built into Office 365 Management Console |
| **Access and data protection** | Azure RMS<br>■ Protection for content in Office apps (on-premises or Office 365) and Windows Server files<br>■ Email notifications for shared documents | RMS protection enabled by Azure RMS<br>■ Protection for content in Office apps (on-premises or Office 365)<br>■ Access to RMS Software Development Kit (SDK) |
| **Threat protection** | Advanced Threat Analytics<br>■ Detects abnormal user behavior<br>■ Detects malicious attacks<br>■ Identifies known risks | Advanced Threat Analytics<br>■ Detects abnormal user behavior<br>■ Detects malicious attacks<br>■ Identifies known risks |

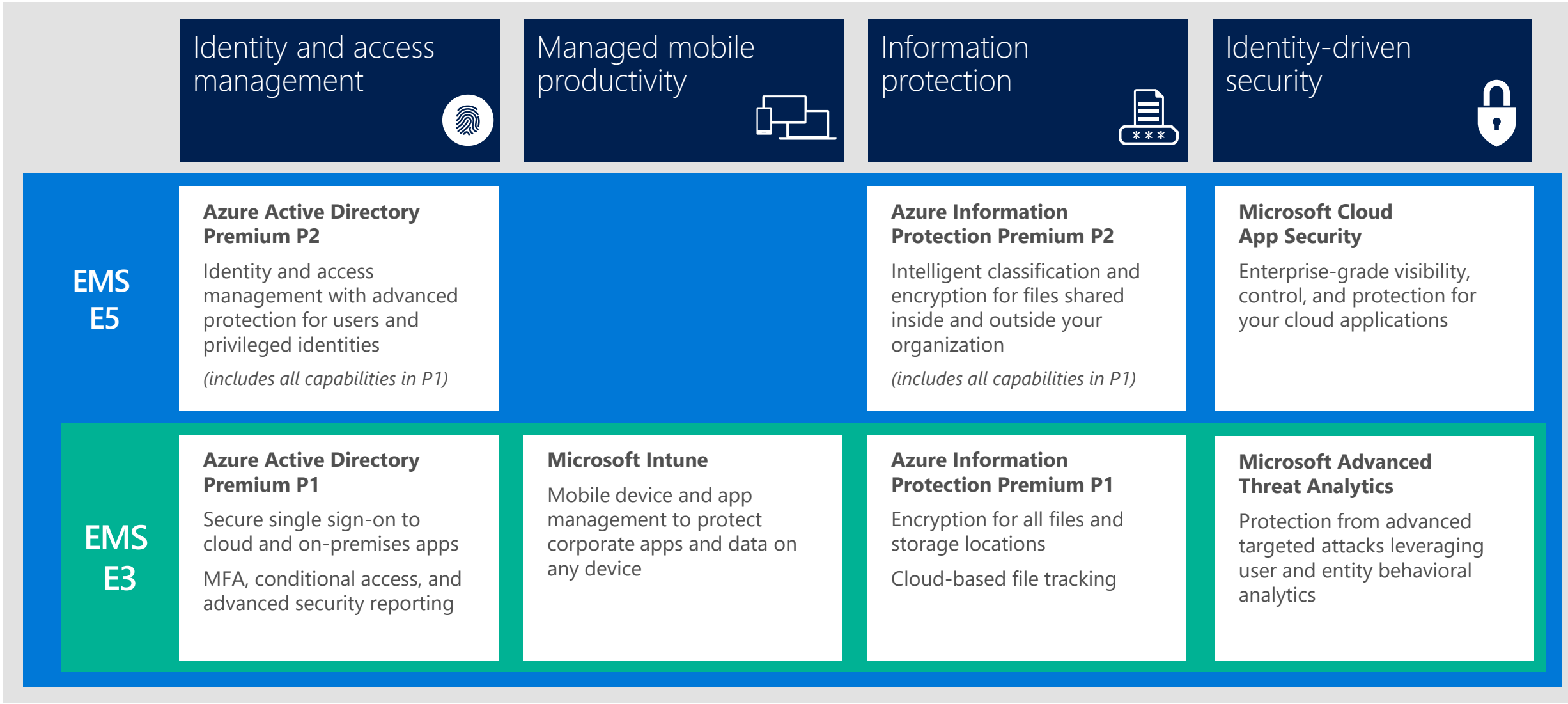
COMPREHENSIVE SOLUTION

# Comprehensive solution




## Stay secure and maximize your budget

# Enterprise Mobility + Security



# Secure Productive Enterprise

Delivered through enterprise cloud services

Office 365

Enterprise Mobility + Security

Windows 10 Enterprise

Microsoft

# EMS Benefits for O365 customers

| | Identity and access management | Managed mobile productivity | Information protection | Identity-driven security |
|---|---|---|---|---|
| Enterprise Mobility + Security | **Azure AD for O365+**<br>• Advanced security reports<br>• Single sign-on for all apps<br>• Advanced MFA<br>• Self-service group management & password reset & write back to on-premises,<br>• Dynamic Groups, Group based licensing assignment | **MDM for O365+**<br>• PC management<br>• Mobile app management (prevent cut/copy/paste/save as from corporate apps to personal apps)<br>• Secure content viewers<br>• Certificate provisioning<br>• System Center integration | **RMS for O365+**<br>• Automated intelligent classification and labeling of data<br>• Tracking and notifications for shared documents<br>• Protection for on-premises Windows Server file shares | **Cloud App Security**<br>• Visibility and control for all cloud apps<br>**Advanced Threat Analytics**<br>• Identify advanced threats in on premises identities<br>**Azure AD Premium P2**<br>• Risk based conditional access |
| Office 365 | **Basic identity mgmt. via Azure AD for O365:**<br>• Single sign-on for O365<br>• Basic multi-factor authentication (MFA) for O365 | **Basic mobile device management via MDM for O365**<br>• Device settings management<br>• Selective wipe<br>• Built into O365 management console | **RMS protection via RMS for O365**<br>• Protection for content stored in Office (on-premises or O365)<br>• Access to RMS SDK<br>• Bring your own key | **Advanced Security Management**<br>• Insights into suspicious activity in Office 365 |

# EMS benefits for Windows 10 customers

| | Identity and access management | Managed mobile productivity | Information protection | Identity-driven security |
|---|---|---|---|---|
| Enterprise Mobility +Security | • Conditional access policies for secure single sign-on<br>• MDM auto-enrollment<br>• Self-Service Bitlocker recovery<br>• Password reset with write back to on-premises<br>• Cloud-based advanced security reports and monitoring<br>• Enterprise State-Roaming | • Mobile device management<br>• Mobile app management<br>• Secure content viewer<br>• Certificate, Wi-Fi, VPN, email profile provisioning<br>• Agent-based management of Windows devices (domain-joined via ConfigMgr and internet-based via Intune) | • Automated intelligent classification and labeling of data<br>• Tracking and notifications for shared documents<br>• Protection for content stored in Office and Office 365 & Windows Server on premises | **Cloud App Security**<br>• Visibility and control for all cloud apps<br>**Advanced Threat Analytics**<br>• Behavioral analytics for advanced threat detection<br>**Azure AD Premium**<br>• Risk based conditional access |
| Windows 10 | • Single sign-on for business cloud apps<br>• Device setup and registration for Windows devices | • Windows Store for Business<br>• Traditional domain join manageability<br>• Manageability via MDM and MAM | • Encryption for data at rest and generated on device<br>• Encryption for data included in roaming settings | **Windows Defender Advanced Threat Protection**<br>• Identify advanced threats focused on Windows 10 behavioral sensors |