

The logo features a stylized shield icon on the left, composed of white lines. To its right, the text "Hybrid Identity Protection" is written in a bold, white, sans-serif font, with "Hybrid" on the first line, "Identity" on the second, and "Protection" on the third. Below this, "Conference 2018" is written in a smaller, white, sans-serif font. The background is dark blue with orange horizontal bars at the top and bottom, and faint gear icons on the right side.

**Hybrid
Identity
Protection**
Conference 2018

Renaissance Midtown Hotel
New York, NY

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Securing the Microsoft Cloud (Office 365 & Azure AD)



Sean Metcalf
Founder, Trimarc



Presenter bio



Sean Metcalf

Founder & CTO, Trimarc

One of ~100 people globally who holds the Microsoft Certified Master Directory Services (MCM) certification.

Presented on Active Directory attack and defense at Black Hat, BSides, DEF CON, DerbyCon, Shakacon and Sp4rkCon security conferences.

Posts info on ADSecurity.org



Agenda

- The “Cloud”
- Attacking the Cloud
- Cloud Security Controls
- Auditing
- Administration
- Controlling Access
- Password Insight
- Cloud Security “Tune Up”
- Testing Defenses
- Office 365 Subscriptions & Capability
- Best Practices & Wrap-up

Azure Active Directory in the Marketplace

Every Office 365 and Microsoft Azure customer uses Azure Active Directory

17.5M

organizations



1.1B

identities



634k

3rd party apps
in Azure AD



90k

paid Azure AD /
EMS customers



450B

monthly
authentications



90%

of Fortune 500
companies



Source: Microsoft Ignite Conference 2018

<https://myignite.techcommunity.microsoft.com/sessions/64565?source=sessions>

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Sep 2018

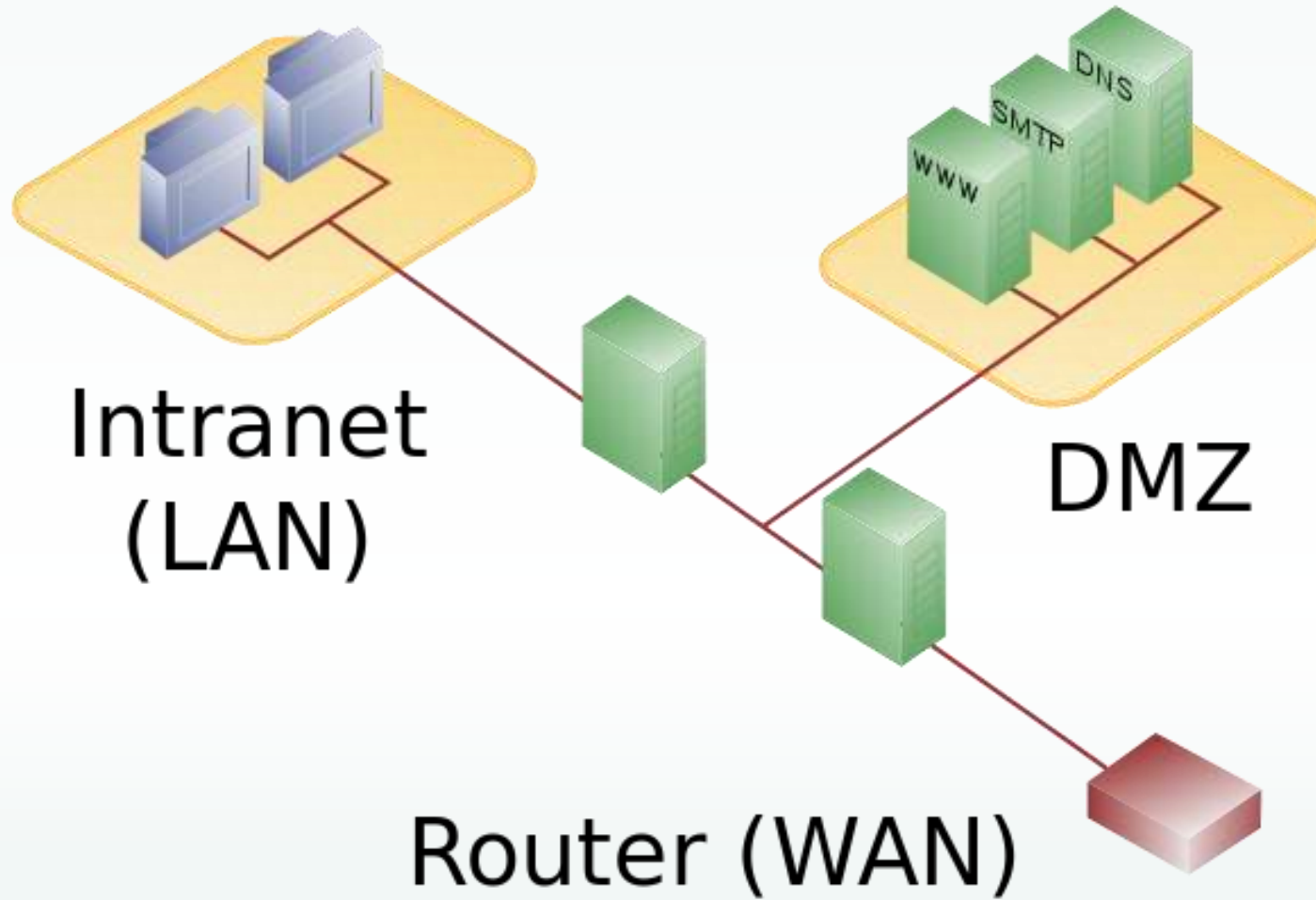


Internal Network

“The cloud is more secure since _____ spends millions every year on cloud security”



Internal Network



Anywhere Cloud Access

SaaS Applications

Office Portal



portal.office.com

Exchange Online
Multi-Tenant



outlook.office365.com
outlook.office.com

Yammer



Yammer.com

Azure AD (eSTS)



login.microsoftonline.com



Attackers Love the Cloud

Common Passwords Attempted in Password Spray Attacks

Password	Spring	2018
Summer	September	1234
Winter	Football	Your Company Name

The threats are real, global, and target all of us

1.29 Billion

Authentications blocked in August 2018

81%

 of data breaches involved weak, default, or stolen passwords

Source: Microsoft Ignite Conference 2018

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Attacks on the Cloud

Source: Microsoft Ignite Conference 2018

300% increase in identity attacks over the past year.



Phishing

23M

high risk enterprise sign-in attempts detected in **March 2018**



Password Spray

350K

compromised accounts detected in **April 2018**



Breach Replay

4.6B

attacker-driven sign-ins detected in **May 2018**

<https://myignite.techcommunity.microsoft.com/sessions/64523?source=sessions>

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

[HOME](#)[ABOUT US](#)[CAREERS](#)[PUBLICATIONS](#)[ALERTS AND TIPS](#)[RELATED RESOURCES](#)[C³ VP](#)

Alert (TA18-086A)

[More Alerts](#)

Brute Force Attacks Conducted by Cyber Actors

Original release date: March 27, 2018 | Last revised: March 28, 2018

[Print](#)[Tweet](#)[Send](#)[Share](#)

Systems Affected

Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals, who were associated with the Mabna Institute, for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are releasing this Alert to provide further information on this activity.

Description

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the attacks remain undetected by avoiding single account lockout.

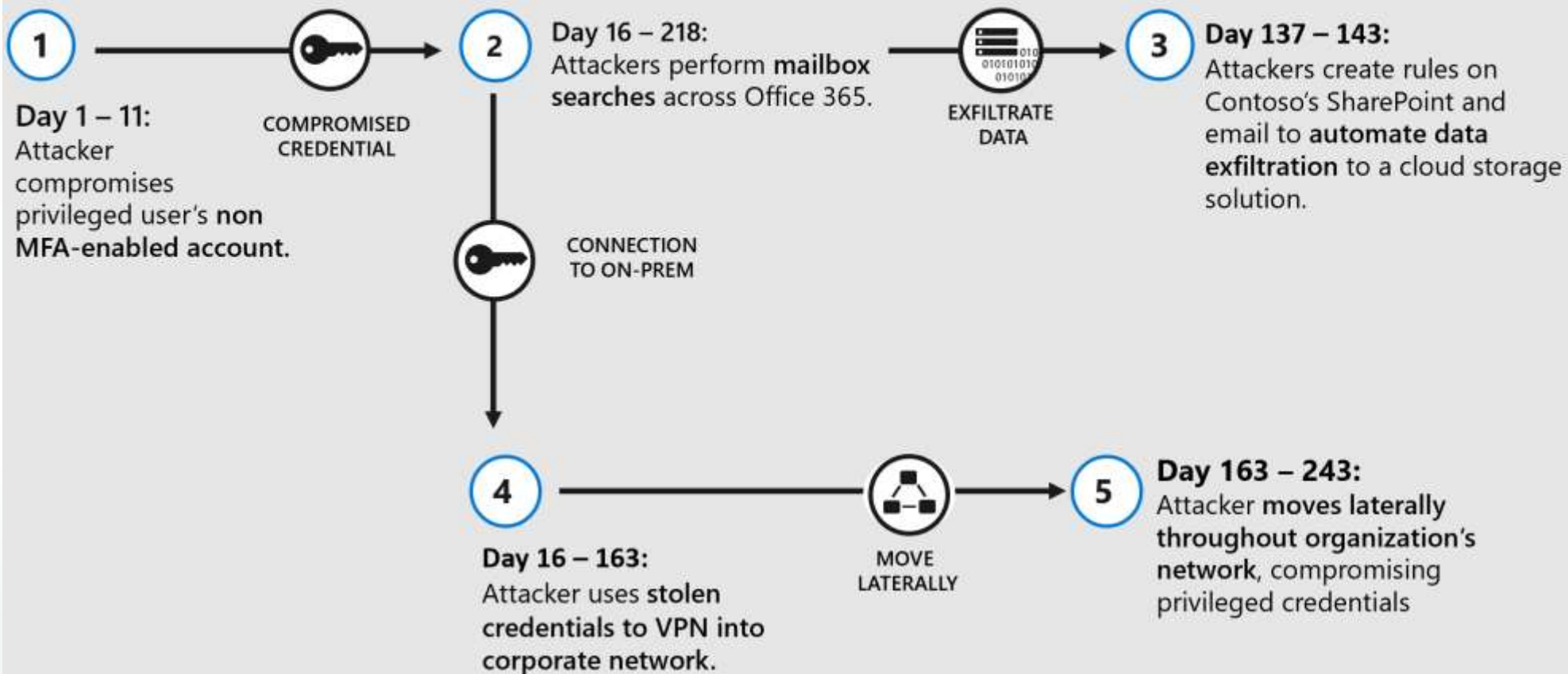




Cloud Attack Timeline

Source: Microsoft Ignite Conference 2018

Attack timeline



<https://myignite.techcommunity.microsoft.com/sessions/64523?source=sessions>

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



EWS Capability

- Availability
- Bulk Transfer
- Conversations Delegate Management
- Exchange Store Search
- Exchange Search
- Federated Sharing Folder
- Inbox Rules Item
- Mail Tips Messaging
- Records Management
- Message Tracking Notification
- Service Configuration Synchronization
- Unified Messaging User Configuration Utility

Attacking the Cloud: Password Spraying

Password Spraying the EWS portal at <https://outlook.office365.com/EWS/Exchange.asmx>. Sit tight....
5 threads remaining.

```
[*] A total of 1 credentials were obtained.  
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.  
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx  
[*] Current date and time: 11/04/2018 10:30:20  
[*] Trying Exchange version Exchange2010  
[*] SUCCESS! User:TrimarcRD.com\DarthVader@TrimarcRD.com Password:Summer2018!  
[*] A total of 1 credentials were obtained.  
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.  
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx  
[*] Current date and time: 11/04/2018 10:30:34  
[*] Trying Exchange version Exchange2010  
[*] SUCCESS! User:TrimarcRD.com\HanSolo@TrimarcRD.com Password>Password99!  
[*] A total of 1 credentials were obtained.  
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.  
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx  
[*] Current date and time: 11/04/2018 10:30:48  
[*] Trying Exchange version Exchange2010  
[*] SUCCESS! User:TrimarcRD.com\JangoFett@TrimarcRD.com Password>Password#99  
[*] A total of 1 credentials were obtained.  
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.  
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx  
[*] Current date and time: 11/04/2018 10:31:01  
[*] Trying Exchange version Exchange2010
```





Attacking the Cloud: Password Spraying

```
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange
[*] Current date and time: 11/04/2018 10:31:16
[*] Trying Exchange version Exchange2010
[*] SUCCESS! User:TrimarcRD.com\Leia@TrimarcRD.com Password>Password99
[*] A total of 1 credentials were obtained.
Results have been written to c:\temp\0365\ews-sprayed-creds.txt.
```



Attacking the Cloud: Password Spraying

11/4/2018, 10:31:29 AM	Leia	Office 365 Exchange Online	Success
11/4/2018, 10:31:29 AM	Yoda	Office 365 Exchange Online	Failure
11/4/2018, 10:31:29 AM	ObiWan Kenobi	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Han Solo	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Bailey	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Boba Fett	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Jango Fett	Office 365 Exchange Online	Failure
11/4/2018, 10:31:23 AM	Darth Vader	Office 365 Exchange Online	Failure
11/4/2018, 10:31:11 AM	ObiWan Kenobi	Office 365 Exchange Online	Failure
11/4/2018, 10:31:11 AM	Yoda	Office 365 Exchange Online	Failure
11/4/2018, 10:31:11 AM	Leia	Office 365 Exchange Online	Failure



Attacking the Cloud: Password Spraying

<u>Basic info</u>	Device info	MFA info	Conditional Access
Request Id	b6c4fd5c-a7b0-4d75-ba65-5ba429789700	IP address	137.135.1
Correlation Id	c8dec77b-2c4c-4071-8a7c-4bed95359c01	Location	Washington, Virginia, US
User	Leia	Date	11/4/2018, 10:31:29 AM
Username	leia@trimarc.com	Status	Success
User ID	2a8165e3-296c-4168-aa52-968bce5f1ef0	Client App	Other clients; Older Office clients
Application	Office 365 Exchange Online		
Application ID	00000002-0000-0ff1-ce00-000000000000		





Attacking the Cloud: Password Spraying

Basic info [Device info](#) [MFA info](#) [Conditional Access](#) [Troubleshooting and support](#)

Request Id	b6c4fd5c-a7b0-4d75-ba65-5ba475769700	IP address	137.135.
Correlation Id	8603d100-6135-45d1-956b-e8f360d99e6f	Location	Washington, Virginia, US
User	Leia	Date	11/4/2018, 10:31:11 AM
Username	leia@trimarcrd.com	Status	Failure
User ID	2a8165e3-296c-4168-aa52-968bce5f1ef0	Sign-in error code	50126
Application	Office 365 Exchange Online	Failure reason	Invalid username or password or Invalid on-premise username or password.
Application ID	00000002-0000-0ff1-ce00-000000000000	Client App	

ISP: Microsoft Corporation

IP Geolocation Information

Continent: North America (NA)
Country: United States (US)
City: Washington





Microsoft Cloud Security Controls



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Trimarc - Overview

Azure Active Directory

Search (Ctrl+/)

- Password reset
- Company branding
- User settings
- Properties
- Notifications settings

Security

- Identity Secure Score (Previe...
- Conditional access
- MFA Server
- Users flagged for risk
- Risky sign-ins
- Authentication methods

Monitoring

- Sign-ins
- Audit logs
- Logs
- Diagnostic settings

Troubleshooting + Support

- Troubleshoot

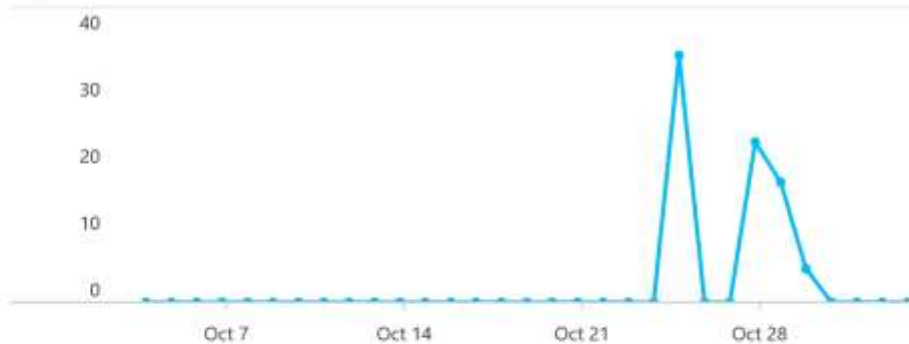
Switch directory Delete directory

trimarcrd.com

Trimarc

Azure AD for Office 365

Sign-ins



What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

34 entries since July 15, 2018. [View archive](#)

<input checked="" type="checkbox"/>	All services	(34)	Fixed
<input type="checkbox"/>	Collaboration	(2)	Group Management - Collaboration
<input type="checkbox"/>	SSO	(4)	

<input type="checkbox"/>	User Authentication	(8)	
<input type="checkbox"/>	3rd Party Integration	(4)	
<input type="checkbox"/>	Platform	(1)	New feature

Your role

Global administrator and 2 other roles

[More info](#)

Find

Users ▼

Search

Azure AD Connect sync

Status: Not enabled
 Last sync: Sync has never run

Create

- User
- Guest user
- Group
- Enterprise application
- App registration

Other capabilities

- Identity Protection
- Privileged Identity Management
- Tenant restrictions
- Azure AD Domain Services
- Access reviews





Azure Identity Protection

- Included with Azure AD Premium
- Have to “install” via the Azure Marketplace (portal.azure.com)
- Dashboard covering identity risk.
- Provides automatic remediation of “risky” sign-ins



Azure Information Protection

Microsoft

Identity



Search (Ctrl+/)

GENERAL

Overview

Getting started

INVESTIGATE

Users flagged for risk

Risk events

Vulnerabilities

CONFIGURE

Multi-factor authentication regis...

User risk policy

Sign-in risk policy

SETTINGS

Alerts

Weekly Digest

Pin to dashboard

4 users have a high risk level. →

Users flagged for risk
7.85% OF 433 USERS



AT RISK
19
SECURED
15

Risk events



HIGH **2** MEDIUM **36** LOW **0** CLOSED **89**

Vulnerabilities

4

RISK LEVEL	COUNT	VULNERABILITY
Medium	398	Users without multi-factor authentication registration
Medium	1	Roles don't require multi-factor authentication for activation
Low	10	Administrators aren't using their privileged roles
Low	31	There are too many global administrators





Enable Risk-based Policies

- Requires Azure Identity Protection (included with Azure AD Premium)
- Assigns a risk level during sign-in
- Risk level determines action
 - Force password change
 - Require MFA registration
 - MFA for higher risk authentication



Enable Sign-in Risk Policy

Policy name
Sign-in risk remediation policy

Assignments

- Users ⓘ
All users >
- Conditions ⓘ
Sign-in risk >

Controls

- Access ⓘ
Require multi-factor authentication >

Review

- Estimated impact ⓘ
Number of sign-ins impacted >

Enforce Policy

On Off

Is this a “risky sign-in”?

- Anonymous IP
- Unfamiliar location

Sign-in risk

SETTINGS

Info

Select the sign-in risk level

- Low and above
- Medium and above
- High



Enable User Risk Remediation Policy

Policy name

User risk remediation policy

Assignments

Users ⓘ

All users



Conditions ⓘ

User risk



Controls

Access ⓘ

Require password change



Review

Estimated impact ⓘ

Number of users impacted



Enforce Policy

On

Off

What's the chance the account is compromised?

- Some detected in real-time
- ~14 day learning period

Sign-in risk

SETTINGS

Info

Select the sign-in risk level

Low and above

Medium and above

High



Enable User Risk Remediation Policy

If you want to require MFA for risky sign-ins, you should:

1. Enable the [multi-factor authentication registration policy](#) for the affected users.
2. Require the affected users to sign in to a non-risky session to perform an MFA registration.

Completing these steps ensures that multi-factor authentication is required for a risky sign-in.

The sign-in risk policy is:

- Applied to all browser traffic and sign-ins using modern authentication.
- Not applied to applications using older security protocols by disabling the WS-Trust endpoint at the federated IDP, such as ADFS.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>



Auditing





Microsoft Cloud Auditing

Audit Item	Category	Enabled by Default	Retention
User Activity	Office 365 Security & Compliance Center	No	90 days
Admin Activity	Office 365 Security & Compliance Center	No	90 days
Mailbox Auditing	Exchange Online	No*	90 days
Sign-in Activity	Azure AD (P1)	Yes	30 days
Users at Risk	Azure AD	Yes	7 days 30 days (AAD P1) 90 days (AAD P2)
Risky Sign-ins	Azure AD	Yes	7 days 30 days (AAD P1) 90 days (AAD P2)
Azure MFA Usage	Azure AD	Yes	30 days
Directory Audit	Azure AD	Yes	7 days 30 days (Azure AD P1/P2)

* Microsoft is gradually enabling mailbox auditing for tenants.





Enable User & Admin Activity Auditing

Home > Audit log search

Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Turn on auditing

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

Clear

Activities

Show results for all activities ▾

Start date

2018-10-20



00:00



End date

2018-10-28



00:00



Results

Date ▾

IP address

User

Activity

Item

Detail

Run a search to view results





Enable User & Admin Activity Auditing

Home > Audit log search

Audit log search

! We're preparing the Office 365 audit log. You'll be able to search for user and admin activity in a couple of hours.

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

Clear

Activities

Show results for all activities ▾

Start date

2018-10-20



00:00



End date

2018-10-28



00:00



Results

Date ▾

IP address

User

Activity

Item

Detail

Run a search to view results





Get Mailbox Auditing

```
PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"}  
| FL Name,Audit*
```

```
Name : SeanMetcalf
```

```
AuditEnabled : False
```

```
AuditLogAgeLimit : 90.00:00:00
```

```
AuditAdmin : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
```

```
AuditDelegate : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
```

```
AuditOwner : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
```

```
Name : bailey
```

```
AuditEnabled : False
```

```
AuditLogAgeLimit : 90.00:00:00
```

```
AuditAdmin : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
```

```
AuditDelegate : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
```

```
AuditOwner : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
```



Enable Mailbox Auditing

```
PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} |  
Set-Mailbox -AuditEnabled $true -AuditOwner MailboxLogin,HardDelete,SoftDelete
```

```
PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} |  
FL Name,Audit*
```

```
Name           : SeanMetcalf  
AuditEnabled   : True  
AuditLogAgeLimit : 90.00:00:00  
AuditAdmin     : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}  
AuditDelegate  : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}  
AuditOwner     : {SoftDelete, HardDelete, MailboxLogin}
```

```
Name           : bailey  
AuditEnabled   : True  
AuditLogAgeLimit : 90.00:00:00  
AuditAdmin     : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}  
AuditDelegate  : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}  
AuditOwner     : {SoftDelete, HardDelete, MailboxLogin}
```



Azure Log Retention: Log Analytics (Preview)

Log Analytics integration not enabled

This Azure Active Directory tenant is not currently enabled to send logs to Log Analytics. Please click the link below to learn about how to turn on this feature.



[Read about AAD integration with Log Analytics](#)

Advanced Queries with Log Analytics



- Log Analytics advanced query experience now in Azure Portal
- Central Analytics Platform across Monitoring, Management, Security
- Run ADEQL queries for investigations, statistics, and root cause + trend analyses
- Utilize ML algorithms for clustering and anomaly detection
- Setup custom alerts and actions
- Dashboard views

Home > f/128 Photography - Logs
f/128 Photography - Logs
Azure Active Directory

New Query 1* +

AzureADLogsWS [Run] Time range: Custom [Save]

```
AuditLogs  
summarize totalEvents = count( OperationName ) by Category  
sort by totalEvents desc
```

Completed. Showing results from the custom time range.

TABLE | CHART | Columns ▾

Drag a column header and drop it here to group by that column.

Category	totalEvents
Account Provisioning	170,941

Home > Log Analytics > AzureADLogsWS > Overview > Azure AD Account Provisioning Events
azureadlogs

Refresh | Analytics | Edit | Clone

8/21/18 09:27 - 9/20/18 09:27

NEW USERS PROVISIONED

Successful add operations
ACCOUNT PROVISIONING

TOTAL SUCCESSFUL ADDS
46.0

APP	COUNT
Box	24
Salesforce F128	11
Workday to Active Directory Us...	11
Salesforce Managers	1
Salesforce members	1
Z test SF	1

NEW USERS PROVISIONED

Failed add operations
ACCOUNT PROVISIONING

TOTAL FAILED ADDS
898

APP	COUNT
Workday to Active Directory Us...	784
Box	107
Self-Service App Access for Ser...	13
Self-Service App Access for Spl...	7
whatever you want	7
Self-Service App Access for Exp...	7
Self-Service App Access for Sal...	7
Salesforce F128	7

USERS UPDATED

Successful update operations
ACCOUNT PROVISIONING

TOTAL SUCCESSFUL UPDATES
45k

APP	COUNT
Workday to Active Directory Us...	45.1K
Box	313
Expense Managers	85
New Employees 2018	36
Socials	32
Photography Training	32
All Users	12
Salesforce members	11



Protecting Administration



Cloud Administration Protection

- Only cloud admin accounts are in privileged groups.
- Require all cloud admin accounts to use MFA (Microsoft Authenticator only).

```
$UserCredential = Get-Credential
Import-Module MSOnline
Connect-MsolService -Credential $UserCredential

$auth = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement
$auth.RelyingParty = "*"

$auth.State = "Enabled"

$auth.RememberDevicesNotIssuedBefore = (Get-Date)

# Enable MFA on all Users
Get-MsolUser -All | where {$_.userprincipalname -like "*admin*"} | `
  Foreach {Set-MsolUser -UserPrincipalName $_.UserPrincipalName -StrongAuthenticationRequirements $auth }
```



“Break Glass” Cloud Admin Account

- New account designated as the Microsoft Cloud Admin account.
- Has permanent membership in the most privileged groups.
- Is excluded from most security controls: MFA and Conditional Access policies.
- Has a strong password.
- Only used in emergencies.
- All other cloud admin accounts have strong security controls (MFA, etc.)



Manage

Try out PIM

Members

Description

Troubleshooting + Support

Troubleshoot

New support request



Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)



Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.



Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.



Review privileged access

With Access Reviews, you can choose delegates or have users attest for themselves if they still need access to privileged roles.



Do more with Azure AD Privileged Identity Management

- Require Multi-Factor Authentication
- Log service/ticket numbers when activating
- Schedule activations for a specific date
- Require approval workflow to activate
- Receive notifications when users are assigned
- Configure and resolve alerts for privileged roles

Privileged Identity Management - Quick start

Quick start

Consent to PIM

Tasks

My roles

My requests

Application access

Approve requests

Review access

Manage

Azure AD roles

Azure resources

Activity

My audit history

Troubleshooting + Support

Troubleshoot

New support request



Introduction

Secure your organization by managing and restricting privileged access

[Azure AD Privileged Identity Management](#)

[Azure AD Privileged Identity Management PowerShell module](#)

[Azure AD Privileged Identity Management for Azure resource roles](#)

What's new in Privileged Identity Management

- All services
- Azure Active Directory
- Azure resources

Feature update

Azure Active Directory

Wednesday, October 3, 2018

[Breaking change: AAD PIM Powershell Module updates to 2.0.0.1762](#)

New feature

Azure Active Directory, Azure resources

Monday, August 6, 2018

[Reduce potential delays with Application access \(preview\)](#)

New feature

Azure resources

Monday, August 6, 2018

[Management Group support in PIM for Azure resources](#)

[Feature update](#) [Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Azure Active Directory, Azure resources



Learn more

Browse our forums to see if your questions have been answered by others or help answer questions posted by other members of the community.

[Go to the forum](#)



Provide feedback

Tell us what you think about Azure Privileged Identity Management

[Provide feedback](#)

Privileged Identity Management - Consent to PIM



Refresh



Consent

Quick start

Consent to PIM

Tasks

My roles

My requests

Application access

Approve requests

Review access

Manage

Azure AD roles

Azure resources

Activity

My audit history

Troubleshooting + Support

Troubleshoot

New support request



Status check completed. Please click 'Consent' button to consent to Privileged Identity Management service



Azure AD Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)



Limit standing access

PIM allows you to make users eligible for roles, which means they only have access when necessary.



Discover who has access

Using the built-in wizard, you can easily discover users with permanent privileged role assignments and make them eligible.



Review privileged access

With Access Reviews, you can choose delegates or have users attest for themselves if they still need access to privileged roles.



Do more with Azure AD Privileged Identity Management

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Leverage PIM

Azure AD directory roles - Overview
international genetic technologies

Overview
Quick start

TASKS

- My roles
- Approve requests (preview)
- My requests (preview)
- Review access

MANAGE

- Roles
- Wizard
- Settings
- Sign up PIM for Azure AD Dir...

Refresh

Admin view My view

My Activation history for the past 7 days

Role	Activation Count
SECURITY AD...	1
PRIVILEGED...	1
GLOBAL AD...	2

My roles

Eligible role assignments

ROLE NAME	STATUS	ACTION
No roles found		

Active role assignments

ROLE NAME	STATUS	ACTION
Security Administrator	Permanently assigned	■
Global Administrator	Permanently assigned	■
Privileged Role Administrator	Permanently assigned	■

Approve requests

Approve Deny Refresh

REQUESTOR	ROLE	REASON	REQUEST RECEI...
-----------	------	--------	------------------

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Controlling Access



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Azure AD Conditional Access

- Enforce different rules on authentication/access based on a variety of conditions.
- Control access based on:
 - Sign-in activity (anomalies?)
 - Network location (corporate network vs internet)
 - Device (AAD Joined?)
 - Application
- Requires Azure AD P1

When this happens

Then do this

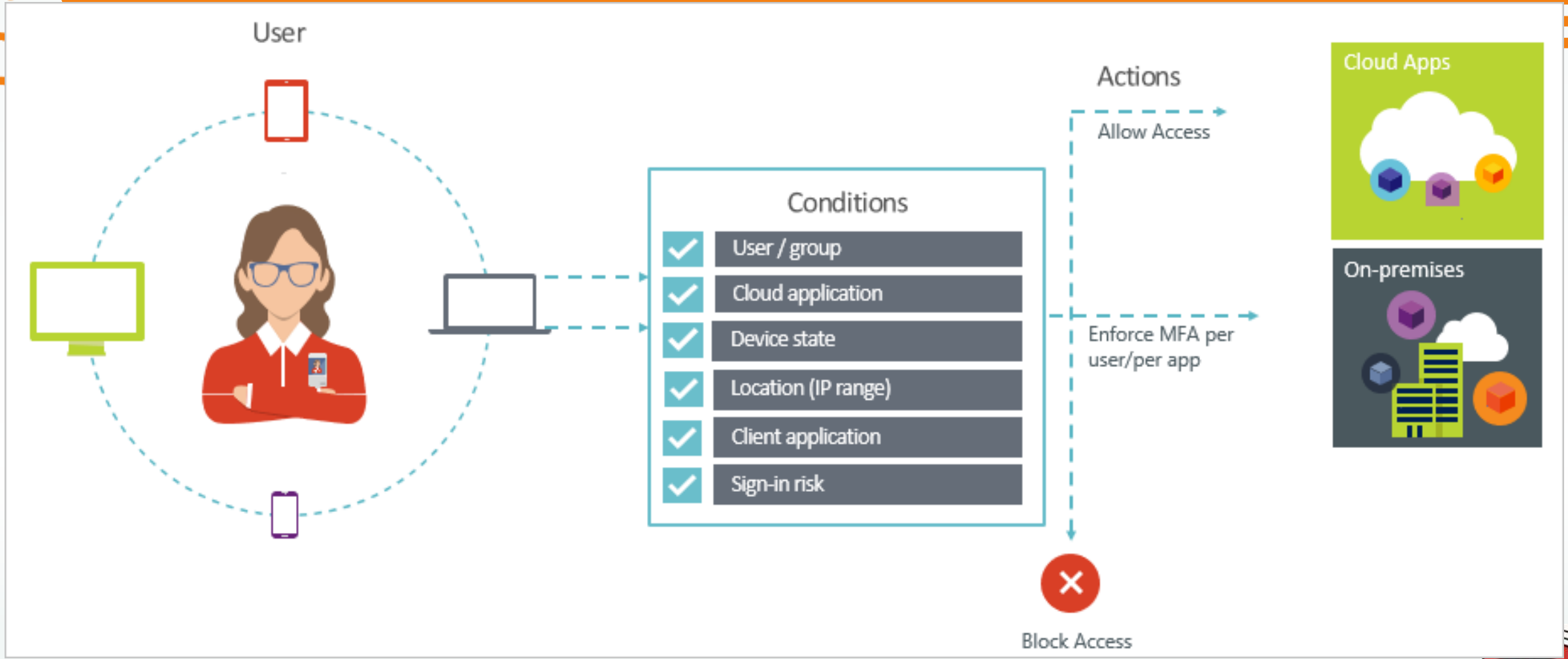
Conditional access policy

Conditions

Access controls



Conditional Access



<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>





Legacy Authentication

Why Block Legacy Authentication?

- 350K compromised accounts in April 2018 due to password spray, 200K in the last month.
- Nearly 100% of password spray attacks we see are from legacy authentication
- Blocking legacy authentication reduces compromise rate by 66%
- <https://aka.ms>PasswordSprayBestPractices>

Source: Microsoft Ignite Conference 2018



Legacy vs Modern Authentication

Legacy Auth

- Office 2010 and older
- Office 2013 (requires patch + reg key to support modern auth)
- Clients that use mail protocols such as IMAP/SMTP/POP
- Older PowerShell modules

Modern Auth

- Office 2013 (requires enabling)
- Office 2016 (PC & Mac)
- Outlook Mobile
- iOS 11 Mail app

Step 1: Understand the usage of Legacy Authentication in your organization

- Use sign in logs to examine current usage. Filter by Client App (add column if you do not see it)
- POP, IMAP, MAPI, SMTP and ActiveSync go to Exchange Online
- “Other Clients” shows SharePoint and Exchange Web Services
- You can export/download the sign in logs, sort by Client App and identify the top offenders

	USERNAME	APPLICATION	SIGN-IN STATUS	CLIENT APP	CONDITIONAL ACC...
	audrey.oliver@wingt...	Azure Portal	Success	Browser	Success
	audrey.oliver@wingt...	Azure Portal	Failure	Browser	Success
	audrey.oliver@wingt...	Azure Portal	Failure	Browser	Failure
	audrey.oliver@wingt...	Azure Portal	Failure	Unknown	Not Applied
7/17/2018, 1:15:08 AM	Hannah Han	hannahhahaha@wi...	Microsoft App Acce...	Browser	Success
7/16/2018, 11:11:35 PM	Barbara Kess	barbarak@wingtpt...	Azure Portal	Browser	Not Applied
7/16/2018, 11:11:24 PM	Barbara Kess	barbarak@wingtpt...	Azure Portal	Unknown	Not Applied
7/16/2018, 11:10:58 PM	Barbara Kess	barbarak@wingtpt...	Azure Portal	Unknown	Not Applied

Source: Microsoft Ignite Conference 2018



Disable Legacy Auth

Home > Conditional access - Policies > Block Legacy Access > Conditions > Client apps (preview)

Block Legacy Access

Info Delete

Name: Block Legacy Access

Assignments

- Users and groups: Specific users included
- Cloud apps: All cloud apps included and 1 ...
- Conditions: 2 conditions selected

Access controls

- Grant: Block access
- Session: 0 controls selected

Enable policy: On Off

Conditions

Info

- Sign-in risk: Not configured
- Device platforms: All platforms (including unsuppo...)
- Locations: Not configured
- Client apps (preview): 1 included
- Device state (preview): Not configured

Client apps (preview)

Configure: Yes No

Select the client apps this policy will apply to:

- Browser
- Mobile apps and desktop clients
- Modern authentication clients
- Exchange ActiveSync clients
- Other clients

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]





Disable Service Access

- Outlook on the Web (OWA)
- Outlook desktop (MAPI)
- Exchange Web Services (EWS)
- Mobile (Exchange ActiveSync)
- IMAP
- POP

MB Bailey
bailey@trimarc.com

Email apps

Choose the apps the user can use to access their Office 365 email.

Outlook on the web	<input checked="" type="checkbox"/>	On
Outlook desktop (MAPI)	<input checked="" type="checkbox"/>	On
Exchange web services	<input type="checkbox"/>	Off
Mobile (Exchange ActiveSync)	<input type="checkbox"/>	Off
IMAP	<input type="checkbox"/>	Off
POP	<input type="checkbox"/>	Off





Azure AD Connect Health - ADFS

Home > Azure Active Directory Connect Health - AD FS services > fs.fabidentity.com > Risky IP [Preview]

Risky IP [Preview]

fs.fabidentity.com

Download Notification Settings Threshold Settings

Learn more about this report notifications and solution recommendations →

TIMESTAMP	TRIGGER TYPE	IP ADDRESS	BAD PASSWORD ERROR CO...	EXTRANET LOCKOUT ERROR...	UNIQUE USERS ATTEMPTED
9/26/2018 6:00 PM	hour	52.231.77.95	0	1728	3
9/26/2018 5:00 PM	hour	52.231.77.95	0	1728	3
9/26/2018 4:00 PM	hour	52.231.77.95	0	1728	3
9/26/2018 3:00 PM	hour	52.231.77.95	0	2939	3
9/26/2018 2:00 PM	hour	52.231.77.95	0	2245	3
9/26/2018 1:00 PM	hour	52.231.77.95	0	1728	3
9/26/2018 12:00 PM	hour	52.231.77.95	0	2090	3
9/26/2018 11:00 AM	hour	52.231.77.95	0	3068	3
9/26/2018 10:00 AM	hour	52.231.77.95	0	1754	3

<https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Monitor-your-ADFS-sign-in-activity-using-Azure-AD-Connect-Health/ba-p/245395>





Gaining Password Insight



Azure AD Smart Lockout (Public Preview)

Smart Lockout

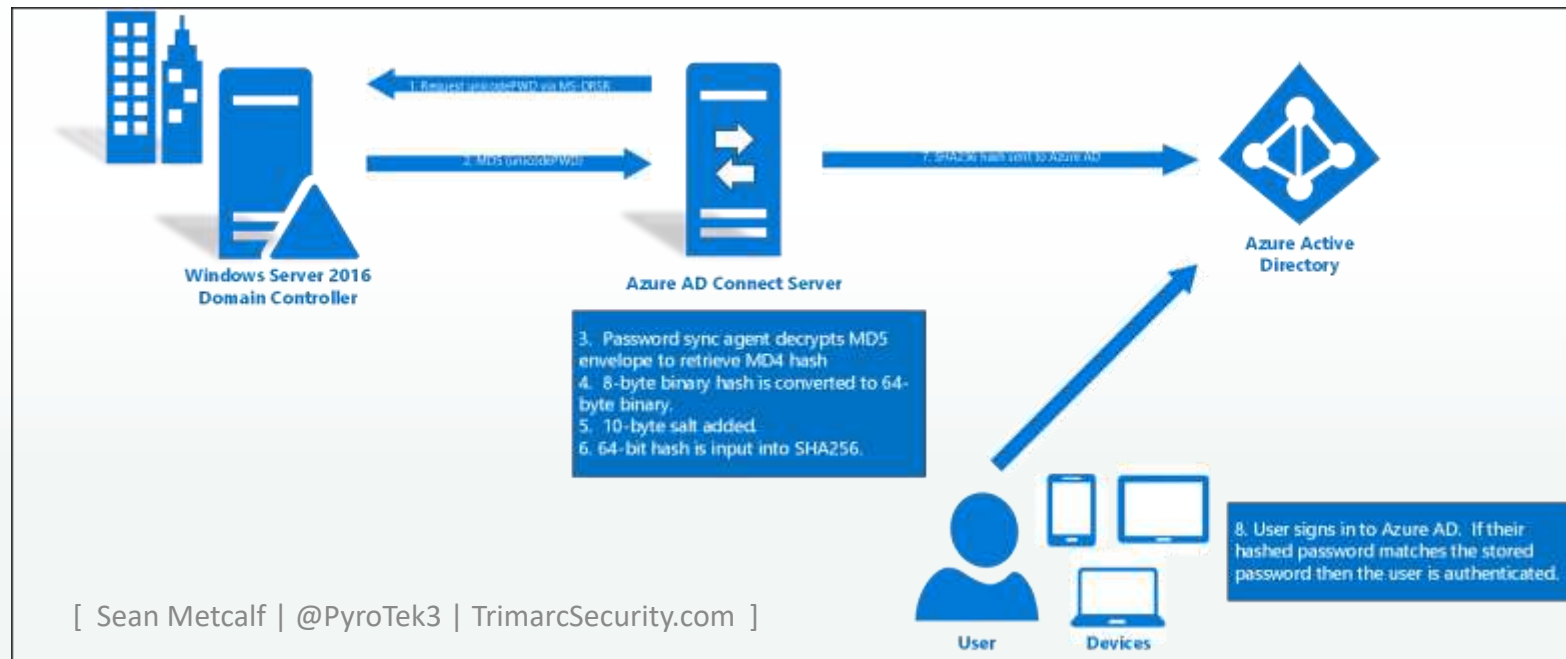
Smart lockout is our lockout system that uses cloud intelligence to lock out bad actors who are trying to guess your users' passwords. That intelligence can recognize sign-ins coming from valid users and treats those differently than ones that attackers and other unknown sources. This means smart lockout can lock out the attackers while letting your users continue to access their accounts and be productive. Smart lockout is always on for all Azure AD customers with default settings that offer the right mix of security and usability, but you can also customize those settings with the right values for your environment. With banned passwords and smart lockout together, Azure AD password protection ensures your users have hard to guess passwords and bad guys don't get enough guesses to break in. *Please note: Azure AD Smart Lockout is included in all versions of Azure AD (including those versions in Office365).*

<https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Password-Protection-and-Smart-Lockout-are-now-in-Public/ba-p/245423>



Password Hash Sync, What & Why?

- Azure AD Connect provides capability.
- Requests password hashes from Active Directory Domain Controllers on-prem.
- Hashes these hashes (MD4+salt+PBKDF2+HMAC-SHA256)
- Sends to Azure AD tenant.
- Microsoft can identify and flag Azure AD users with bad passwords.






[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Azure AD Premium Password Protection (Public Preview)

- On-prem Active Directory solution.
- Microsoft Password Filter deployed to DCs.
- 1-2 Proxy servers configured in the AD forest.
- Blocks >500 commonly used passwords (plus > 1M character substitution of the passwords).
- Audit or Enforce password restrictions.
- Usage reporting (Get-AzureADPasswordProtectionSummaryReport)

SYSVOL > trimarcresearch.com > Policies > {4A9AB66B-4365-4C2A-996C-58ED9927332D} > AzureADPasswordProtection >

Name	Date modified	Type	Size
 Azure	11/3/2018 10:57 PM	File folder	
 Configuration	11/3/2018 10:57 PM	File folder	
 PasswordPolicies	11/3/2018 10:57 PM	File folder	

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





Azure AD Premium Password Protection

Authentication methods (Preview) - Password protection (Preview)

Trimarc R&D - Azure AD Security

Search (Ctrl+/) << Save Discard

Manage

- Password protection (Preview)

Custom smart lockout

Lockout threshold ⓘ 10 ✓

Lockout duration in seconds ⓘ 60 ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

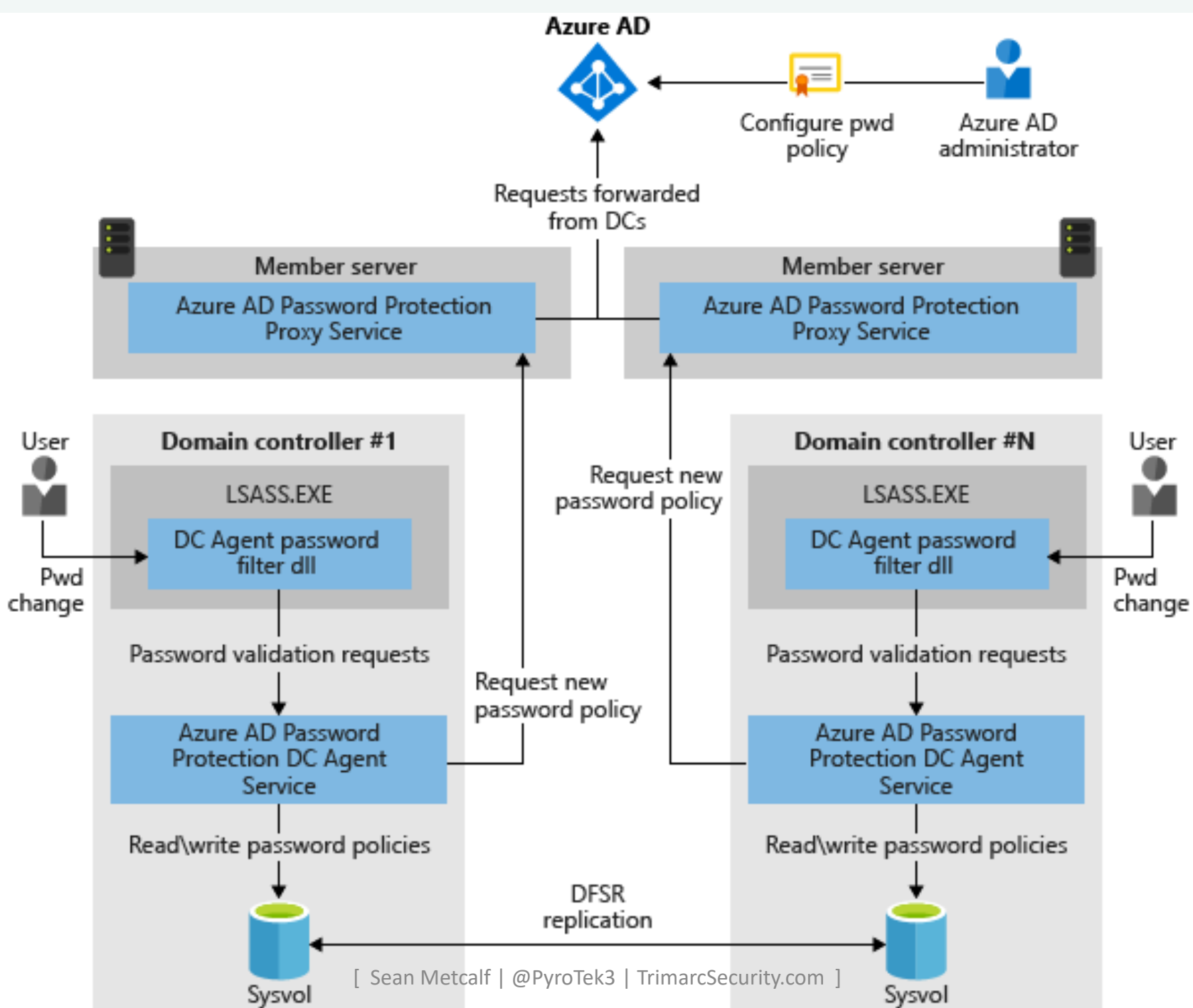
- Trimarc ✓
- Washington
- DCUnited

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit







Microsoft Cloud Security “Tune Up”



[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Secure Score



Your Secure Score

Secure Score figures out what Office 365 services you are using, then looks at your configuration and behaviors and compares it to a baseline asserted by Microsoft. If your configuration and behaviors are in line with best practices, you will get points, which you can track over time. More importantly, you will be able to quick determine what things you can do to reduce their risk





Secure Score

Enable MFA for Azure AD privileged roles

You should enable MFA for all of your Azure AD privileged roles because a breach of any of those accounts can lead to a breach of any of your data. We found that you had 1 admins out of 1 that did not have MFA enabled. If you enable MFA for those 1 admin accounts, your score will go up 50 points.

Action Category	Identity
User Impact	Low
Implementation Cost	Low
Action Score	0/50

Threats

- Password Cracking
- Account Breach
- Elevation of Privilege

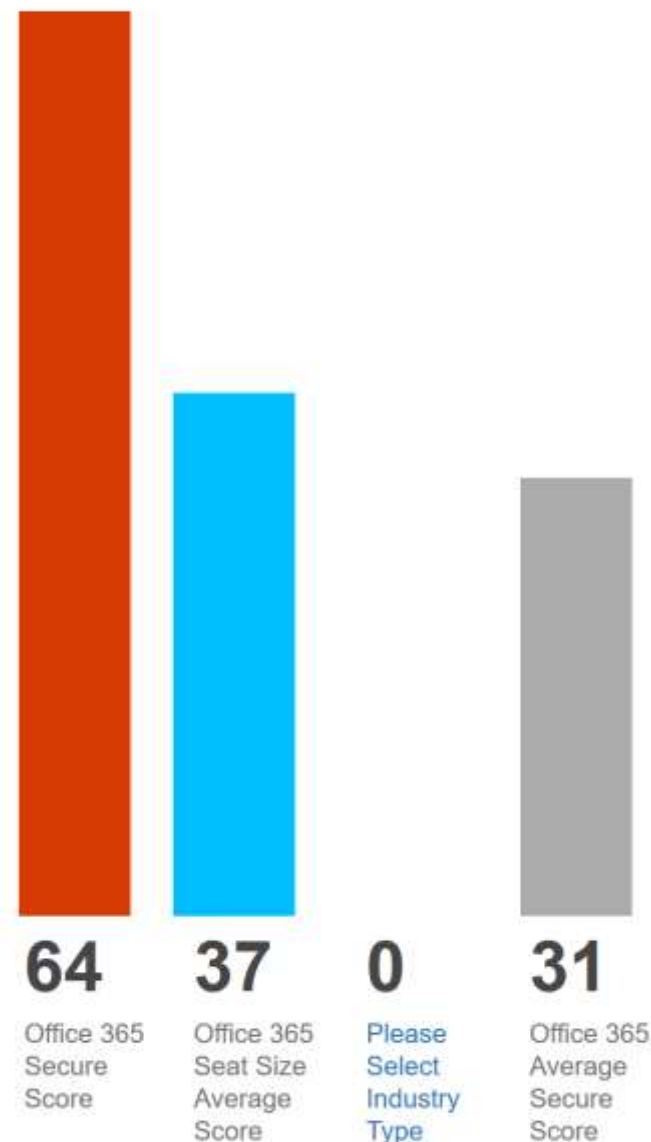
Compliance Controls

- ISO 27018:2014; Control C.9.4.2, A.10.8
- CSA CCM301; Control DSI-02
- GDPR; Control 6.6.5

Show more ▾

[Learn more](#) [Ignore](#) [Third Party](#)

Compare your score



Seat size this tenant belongs to is 6 - 99 seats



Enable Client Rules Forwarding Block



What am I about to change?

There are several ways today that a bad actor can use external mail forwarding to exfiltrate data.

1. Client created external mail forwarding Rules, such as the Outlook desktop client.
2. Admins can set up external mail forwarding for a user via setting ForwardingSmtpAddress on a user object.
3. Admins can create external transport rules to forward messages.
4. Client created ForwardingSmtpAddress via Outlook Web Access interface

This Security Control action will help mitigate Client created external mail forwarding rules.

A simple mitigation is to, on each Remote Domain, including the Default to disallow Auto-Forwarding. This is a global setting and applies to every email sent from within a Tenant, as a result it is a very broad approach, which does not allow white listing. More details can be found [here](#). RBAC roles can be used to achieve a similar result.

Using a properly configured Transport Rule we can control the impact of data exfiltration via Client created external mail forwarding rules. This approach has a couple of advantages:

1. Clients will receive a custom NDR message, useful for highlighting to end users external forwarding rules they may have not known existed (accidental exfiltration), or external forwarding rules created by a bad actor on a compromised mailbox.
2. Allows a whitelist of users or groups to be configured to allow business approved exceptions to the policy.
3. Provides some mitigation, for when an Admin account has been used to create a Remote Domain with auto-forwarding enabled to specific namespace to exfiltrate data.
4. Provides some mitigation, for when an Admin account has been used to alter the Default Remote Domain settings.

This Security Control will create a transport rule of the type AutoForward, mitigating the use of

Enable Client Rules Forwarding Block Complete



You have successfully created the transport rule that blocks the use of client-side forwarding rules. We found that you had 0 Rules out of 0 that did have blocks enabled.

Your score will increase by 20 points within 24 hours. We found that you had 0 Rules out of 0 that did have blocks enabled.

Apply

More

Cancel

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Secure Score – Highest Priority Items

Action	Score Increase
Enable MFA for Azure AD privileged roles	50
Enable MFA for users	30
<i>Enable sign-in risk policy</i>	30
<i>Enable user risk policy</i>	30
Enable Client Rules Forwarding Block	20
<i>Enable Cloud App Security Console</i>	20
<i>Enable Data Loss Prevention policies</i>	20
<i>Enable Microsoft Intune Mobile Device Management</i>	20
<i>Enable policy to block legacy authentication</i>	20
Ensure all users are registered for multi-factor authentication	20
<i>Review permissions & block risky OAuth applications connected</i>	20
<i>Set automated notification for new OAuth applications connected</i>	20
<i>Set automated notifications for new and trending cloud applications</i>	20

**Recommended
ASAP**

*Additional
subscription
required*



Last updated 11/3/2018, 12:00:00 AM ⓘ

Your Identity Secure Score

26 / 223

Your score is above the average for your company's industry.

Trimarc R&D **26** ■

Industry average **-1**

Typical 6-99 person co... **26** ■

[Change industry](#)

Show score for last

7 days

30 days

60 days

90 days



Improvement actions

☰ Column ↓ [Download](#)

🔍 *Search to filter items...*

NAME	↑↓	SCORE IMPACT	↑↓	USER IMPACT	↑↓	IMPLEMENTATION COST
Enable MFA for Azure AD privileged roles		50		Low		Low
Enable MFA for users		30		Moderate		Moderate
Enable sign-in risk policy		30		Moderate		Moderate
Enable user risk policy		30		Moderate		Moderate
Ensure all users are registered for multi-factor authentication		20		High		High
Do not allow users to grant consent to unmanaged applications		10		Moderate		Low
Enable policy to block legacy authentication		10		Moderate		Moderate

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Manage advanced alerts



Your subscription allows you to use Office 365 Cloud App Security!

Take advantage of features such as:

- > Alerts - Create alerts and investigate anomalous and suspicious behavior
- > Productivity app discovery - Gain visibility into how Office 365 and other productivity cloud services are being used
- > App permissions - View and control which apps have been granted permissions to your Office 365 environment

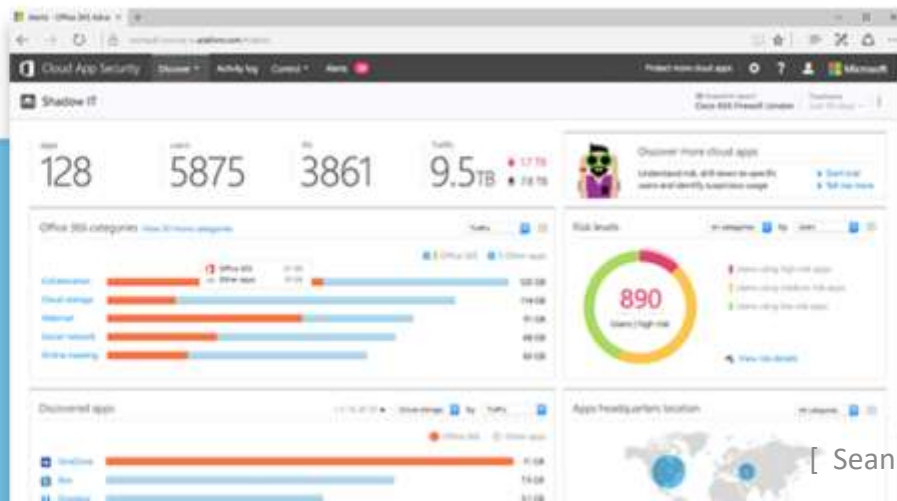
Turn on Office 365 Cloud App Security

[Go to Office 365 Cloud App Security](#)

[Learn more about Office 365 Cloud App Security](#)

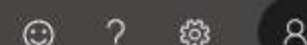
Office 365 Cloud App Security is powered by Microsoft Cloud App Security service which is a separate online service

- [Privacy & Cookies](#)
- [Terms](#)



Investigate
identity behavior across
cloud apps





Get started with Cloud App Security

[Create a Cloud Discovery report](#)

[Connect apps](#)

[Create policies](#)

[Learn more...](#)



General dashboard >

General dashboard



178 activities monitored



10 files monitored



177 accounts monitored



[Discover your cloud apps](#)
upload traffic logs



0 governance actions taken



0 user notifications sent

View dashboard for a specific app

- Office 365
- Microsoft OneDrive for Business
- Microsoft SharePoint Online
- Microsoft Azure
- Microsoft Cloud App Security
- Microsoft Exchange Online

[View all apps...](#)

View dashboard for a specific risk type

- Threat detection
- Privileged accounts



Open alerts

New over the last month ▾

RECENT ALERTS

[View all alerts...](#)

BY SEVERITY



BY ALERT TYPE



Top 3 alert types

- N/A
- N/A
- N/A



Policies

NAME:

TYPE:

STATUS: ACTIVE DISABLED

SEVERITY: ■ ■ ■ ■ ■ ■ ■ ■ ■

CATEGORY:

Advanced

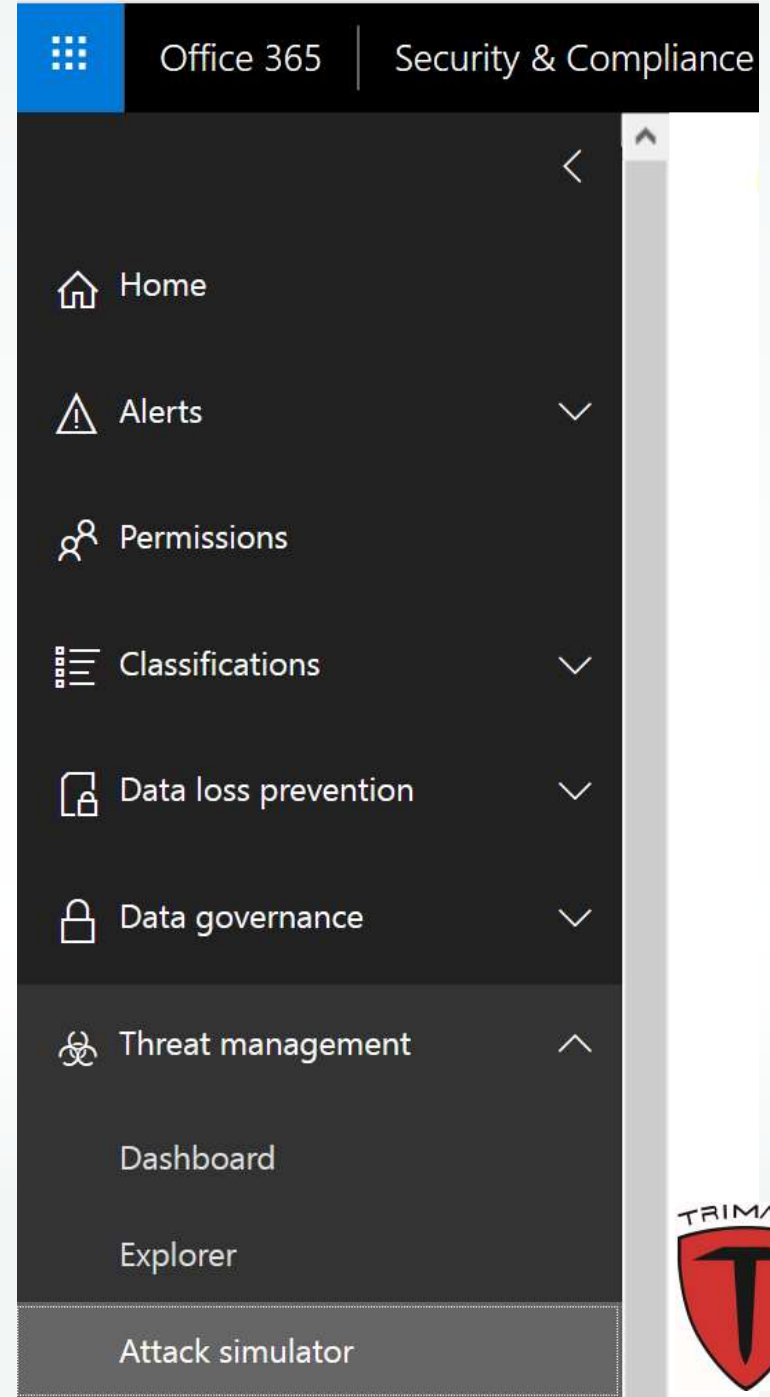
1 - 17 of 17 Policies Create policy

Policy	Count	Severity	Category	Action	Modified
Unusual file share activity (by user) <small>This policy profiles your environment and triggers alerts when users ...</small>	0 open alerts	■ ■ ■	Threat detection		Oct 24, 2018
Unusual file download (by user) <small>This policy profiles your environment and triggers alerts when users ...</small>	0 open alerts	■ ■ ■	Threat detection		Oct 24, 2018
Multiple failed login attempts <small>This policy profiles your environment and triggers alerts when users ...</small>	0 open alerts	■ ■ ■	Threat detection		Oct 24, 2018
Unusual file deletion activity (by user) <small>This policy profiles your environment and triggers alerts when users ...</small>	0 open alerts	■ ■ ■	Threat detection		Oct 24, 2018
Activity from suspicious IP addresses <small>This policy profiles your environment and triggers alerts when activit...</small>	0 open alerts	■ ■ ■	Threat detection		Oct 24, 2018

Activity from anonymous IP addresses <small>This policy profiles your environment and triggers alerts when activit...</small>	0 open alerts	■ ■ ■	Threat detection		Oct 24, 2018
---	---------------	-------	------------------	--	--------------



Testing Defenses



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



Simulate the Attack: Password Spray

Configure Password Attack

- ✓ Start
- ✓ Target users
- ✓ Choose attack settings

Confirm

Please confirm your settings: Users: bailey@trimarcrd.com BobaFett@TrimarcRD.com DarthVader@TrimarcRD.com HanSolo@TrimarcRD.com JangoFett@TrimarcRD.com JoeUser@TrimarcRD.com Leia@TrimarcRD.com ObiWanKenobi@TrimarcRD.com Yoda@TrimarcRD.com
Are you sure you want proceed with your password attack?

● Confirm





Simulate the Attack : Password Spray

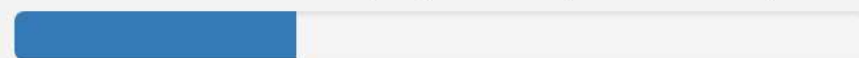
< Password Spray Attack

Attack Details

A password spray attack against an organization is typically done by running a list of commonly used passwords against a list of valid Office 365 user accounts. Typically, the attacker crafts one password to try against all of the known user accounts. If the attack is not successful, the attacker will try again using another carefully crafted password, usually with a waiting period between attempts to avoid policy-based account lockout triggers.

Current Attack Status

TrimarcRD Password Spray Attack (Winter2018!)



33% of user accounts attempted

1 of 9 users have been compromised

[Terminate Attack](#)





Simulate the Attack: Password Spray

Attack details

< Report: TrimarcRD Password Spray Attack (Winter2018!)

11/3/2018, 8:08:20 PM to 11/3/2018, 8:09:10 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

9

Successful attempts

1

Overall Success Rate

11%

For this attack, 1 of 9 users were found to be susceptible to Password Spray attacks.

Compromised Users

BobaFett@TrimarcRD.com





Simulate the Attack: Password Attack

Configure Password Attack

- ✓ Start
- ✓ Target users
- ✓ Choose attack settings

● Confirm

Confirm

Please confirm your settings: Users: bailey@trimarcrd.com BobaFett@TrimarcRD.com DarthVader@TrimarcRD.com HanSolo@TrimarcRD.com JangoFett@TrimarcRD.com JoeUser@TrimarcRD.com Leia@TrimarcRD.com ObiWanKenobi@TrimarcRD.com Yoda@TrimarcRD.com
Are you sure you want proceed with your password attack?

Back

Finish

Cancel





Simulate the Attack: Password Attack

Security & Compliance

Threat management

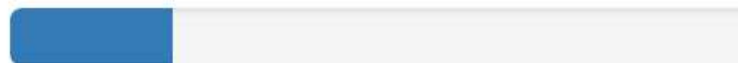


Attack simulator

Brute Force Password (Dictionary Attack) Account Breach

A brute-force attack dictionary is an automated, trial-and-error method of generating multiple passwords guesses from a dictionary file against a user's password.

TrimarcRD Password Attack



22% of user accounts attempted

1 of 9 users have been compromised

Launch Attack

Terminate Attack

Attack Details



Simulate the Attack: Password Attack

Security & Compliance

Threat management

Attack simulator

Attack details

< Brute Force Password (Dictionary Attack)

Attack Details

Password cracking techniques are used to guess a user's password by trying many variations with a computer. Once an attacker has the user name and password for a user, the attacker will generally be able to sign in to Office 365 and gain access to additional information, such as other user accounts and sensitive information. Brute-force attacks work by calculating every possible combination that could make up a password and testing to see if it is the correct password. As the password's length increases, the amount of time, on average, to find the correct password increases exponentially. This means short passwords can usually be discovered rather quickly, but longer passwords may take decades to discover. Two types of brute-force password attacks exist: a dictionary attack using a well-known list of passwords, and an exhaustive attack, where combinations are tried sequentially. Attack simulator uses a dictionary list attack, allowing modifications of frequency between attacks and the number of attempts. If a password is discovered, the password itself is not shown; only an indication that a password was discovered will be shown.

Current Attack Status

TrimarcRD Password Attack



[Terminate Attack](#)





Simulate the Attack: Password Attack

Security & Compliance

Threat management

Attack simulator

Attack details

< Report: TrimarcRD Password Attack

11/3/2018, 8:01:54 PM to 11/3/2018, 8:04:41 PM

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

Total users targeted
9
Successful attempts
6
Overall Success Rate
67%

For this attack, 6 of 9 users were found to be susceptible to Brute Force Password attacks.

Compromised Users

BobaFett@TrimarcRD.com

DarthVader@TrimarcRD.com

HanSolo@TrimarcRD.com

JangoFett@TrimarcRD.com

JoeUser@TrimarcRD.com

Leia@TrimarcRD.com

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Simulate the Attack: Phishing Attack

Security & Compliance

Threat management

Attack simulator

Configure Phishing Attack

Provide a name to the campaign

Name

Prize Giveaway

Use Template

Please select a template in the list...

Prize Giveaway

Payroll Update

Start

Target recipients

Configure email details

Compose email

Confirm



Simulate the Attack: Phishing Attack

Please provide email details ✕

From (Name)

TrimarcRD Payroll Update

From (Email)

payrollservices@payrolltooling.com

Phishing Login server Url

http://portal.payrolltooling.com

Custom Landing Page URL

To use a custom landing page for user awareness after an attack, enter your URL here.

Subject

Urgent - Update Your Payroll Details

Back

Next

Cancel



Simulate the Attack: Phishing Attack

Security & Compliance


Threat management


Attack simulator

Email body

Email body

Email Source





\$(username), Your payroll details need updating, please click below to start

UPDATE YOUR ACCOUNT DETAILS

Dear, \$(username)

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for you


Please review and enter your routing number details at the link above \$(username) - by clicking on the "Update Your Account Details" b

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Simulate the Attack: Phishing Attack

Security & Compliance

 Threat management



Attack simulator

Spear Phishing (Credentials Harvest) Account Breach

A spear-phishing attack is a targeted attempt to acquire sensitive information, such as user names, passwords, and credit card information, by masquerading as a trusted entity. This attack will use a URL to attempt to obtain user names and passwords.

Launch Attack

Attack Details

Simulate the Attack: Phishing Attack

TrimarcRD Payroll Update

Urgent - Update Your Payroll Details

Joe User, Your payroll details need up

Urgent - Update Your Payroll Details



TrimarcRD Payroll Update <payrollservices@payrolltooling.com>

Today, 8:37 PM

Joe User



Reply all

Inbox

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, [click here](#).

To always show content from this sender, [click here](#).

icon

Joe User, Your payroll details need updating, please click below to start the update.

UPDATE YOUR ACCOUNT
DETAILS

Dear, Joe User

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for your account nominated to receive your salary.

Please review and enter your routing number details at the link above Joe User - by

Security & Compliance

Threat management

Attack simulator

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Security & Compliance

Threat management



Attack simulator



Joe User, Your payroll details need updating, please click below to start the update.

UPDATE YOUR ACCOUNT
DETAILS

Dear, Joe User

We have recently upgraded our payroll system, as a security measure we need you to confirm your bank routing number details for your account nominated to receive your salary.

Please review and enter your routing number details at the link above Joe User - by clicking on the "Update Your Account Details" button above.

Failure to update your account details will result in delays with your salary being processed. Please make sure to update the details at least 5 days before the next Payroll cycle to avoid a unnecessary delay in processing.

Please let us know if you have any questions.

Thank you.

Do not share this email

This email contains a secure link to a secure site. Please do not share this link email with others.

Questions or concerns about the new Payroll Service?

If you have any questions about the site, please visit our support page support page rather than replying to this email.

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Security & Compliance

Threat management ^

Attack simulator



Sign in

Email, phone, or Skype

Next

No account? [Create one!](#)

[Can't access your account?](#)

Security & Compliance

Threat management



Attack simulator



Sign in

Email, phone, or Skype

This connection is not secure. Logins entered here could be compromised. [Learn More](#)

No account? [Create one!](#)

[Can't access your account?](#)





Security & Compliance

Threat management



Attack simulator



jangofett@trimarc.com



Enter password

Password



This connection is not secure. Logins entered here could be compromised. [Learn More](#)

[Forgot my password](#)



You have been redirected to this web page as a recent message you opened was part of a Phishing awareness test being run by your Organization. You will be contacted shortly by your Administrators for some follow up training on security best practices. In the meantime some high-level information is presented below to help you remain safe.

Why are we talking about Phishing?

Phishing happens to everybody. It's a huge problem, and it's getting bigger. In fact, a 2016 study reports that 91% of cyberattacks and the resulting data breach begin with a phishing email. These attacks are becoming more frequent and sophisticated. So much so that one online article states that 97% of people world-wide could not identify a sophisticated phishing attack. And, it's not just your work accounts at risk. These phishers will hack things like your banking, utilities, insurance information and even Facebook, Twitter, and Instagram accounts.



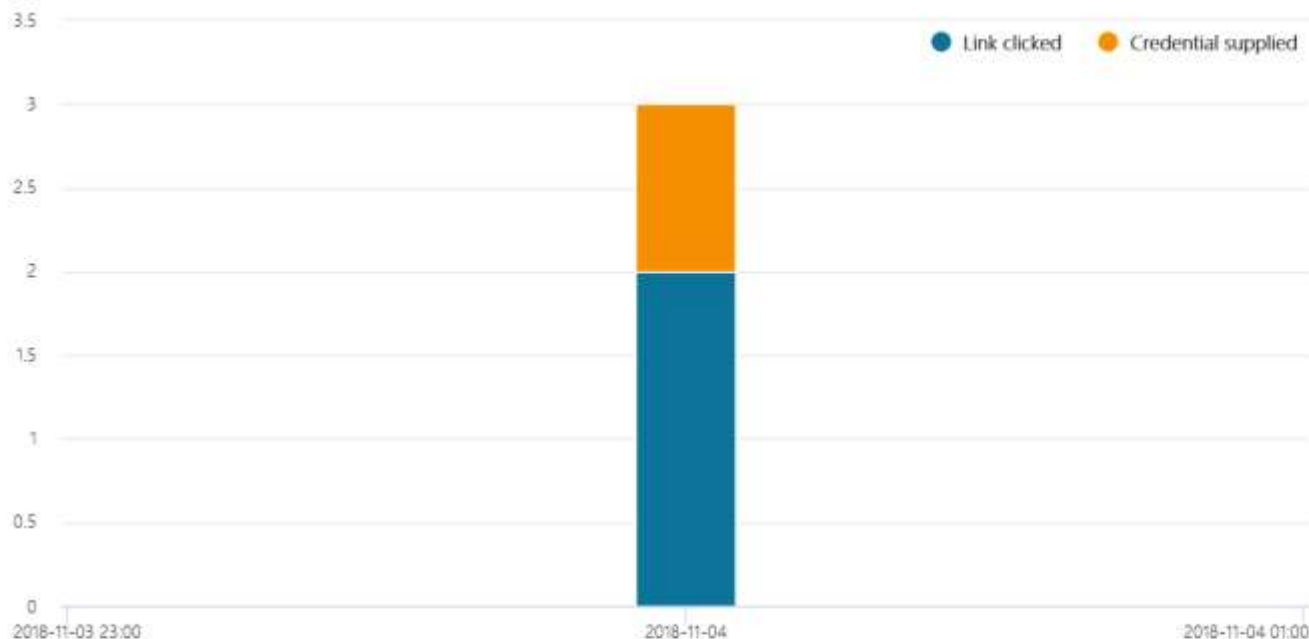
Report: Payroll Update

11/3/2018, 8:37:08 PM to 11/3/2018, 8:37:22 PM

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

Total users targeted	Fastest Click	Fastest Credentials
9	5 minutes 51 seconds	11 minutes 58 seconds
Successful attempts	Average Click	Average Credentials
1	8 minutes 14 seconds	11 minutes 58 seconds
Overall Success Rate	Click Success Rate	Credential Success Rate
11%	22%	11%

For this attack, 1 of 9 users were found to be susceptible to Spear Phishing attacks.



● Credential supplied
● Link clicked
● None



Compromised Users

JangoFett@TrimarcRD.com
Credential supplied: 11/3/2018, 8:49:07 PM
Link clicked: 11/3/2018, 8:47:46 PM
JoeUser@TrimarcRD.com
Link clicked: 11/3/2018, 8:43:00 PM

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]



Office 365 Subscriptions (Capability & Cost)

Office 365 Enterprise Tiers

Enterprise 1 (E1) - \$8 user/month	Enterprise 3 (E3) - \$20 user/month	Enterprise 5 (E5) - \$35 user/month
50 GB mailbox	50 GB mailbox	100 GB mailbox
File storage and sharing with 1 TB OneDrive storage	Unlimited personal cloud storage	Unlimited personal cloud storage
No Office installed apps	Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user)	Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user)
	eDiscovery with in-place search, hold, and export	eDiscovery with in-place search, hold, and export
		Customer Lockbox
		Office ATP Auto classification, smart import, and more with Advanced Data Governance
		Office 365 Cloud App Security



Azure Active Directory Options

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

- Free
- Basic: \$1 per user monthly
 - No object limit & Basic reports
- **P1: \$6 per user monthly**
 - Self-Service Group and app Management
 - Self Service Password Reset/Change/Unlock
 - Two-way sync between on-prem & Azure AD
 - Multi-Factor Authentication (Cloud and On-premises (MFA Server))
 - Cloud App Discovery
 - Conditional Access based on group, location, and device state
 - Connect Health
 - Microsoft Cloud App Security integration
 - MDM auto-enrollment
- **P2: \$9 per user monthly**
 - Includes P1 features
 - Identity Protection
 - Privileged Identity Management
 - Access Reviews



Enterprise Mobility + Security Options

Azure AD P1: \$6

Enterprise Mobility + Security

E3

- Azure Active Directory Premium P1
- Intune
- Azure Information Protection P1
- Advanced Threat Analytics

\$8.74**

per user per month

Enterprise Mobility + Security

E5

- Azure Active Directory Premium P2
- Intune
- Azure Information Protection P2
- Advanced Threat Analytics
- Cloud App Security
- Azure Advanced Threat Protection

\$14.80**

per user per month

Azure AD P2: \$9

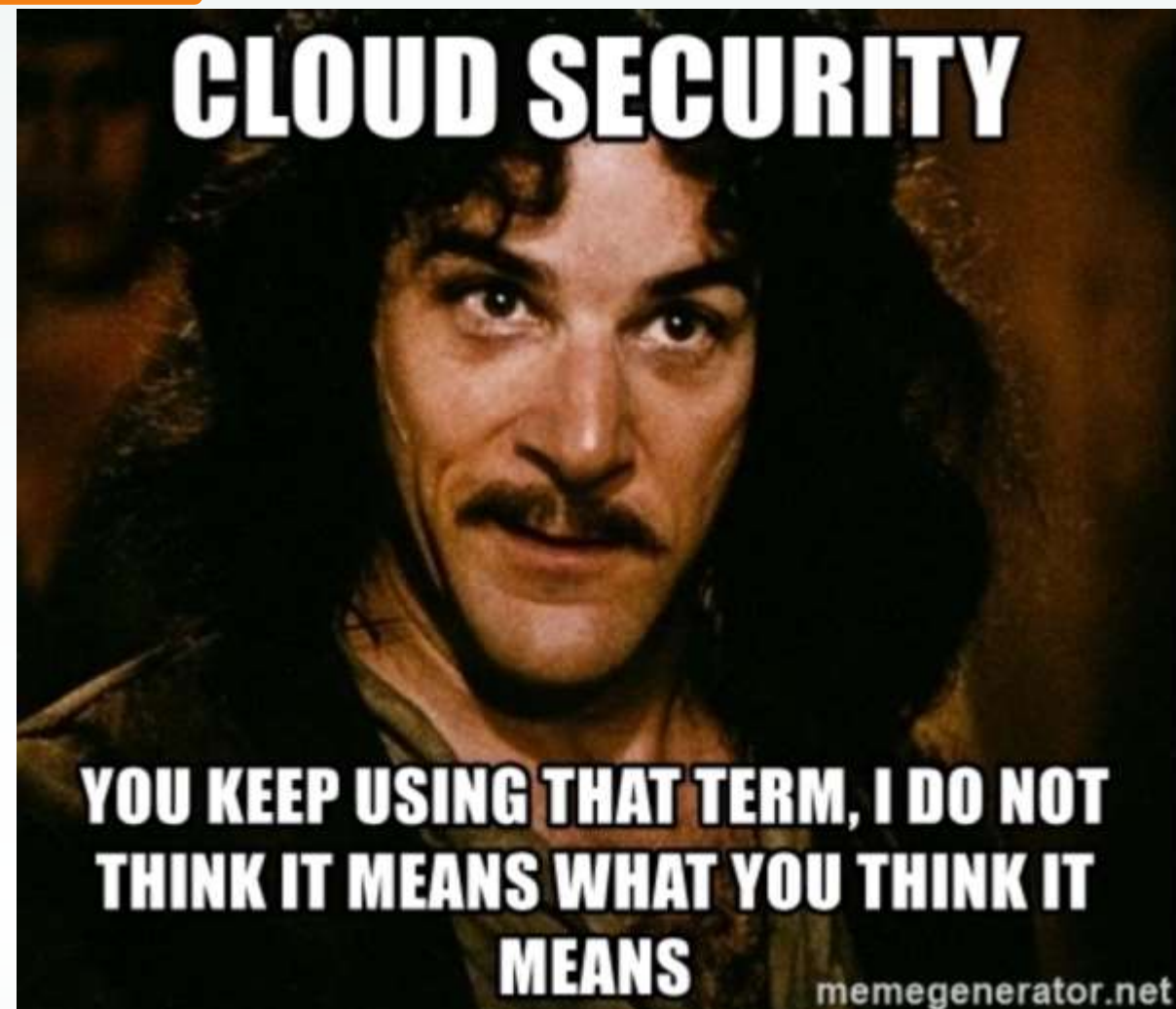




Approximate Microsoft Cloud Cost (\$26 - \$50 user/month)

- Office 365 E3 & Azure AD
 - Office 365 E3 (\$20) + Azure AD P1 (\$6) = \$26/user/month
 - Office 365 E3 (\$20) + Azure AD P2 (\$9) = \$29/user/month
- Office 365 E5 & Azure AD
 - Office 365 E5 (\$35) + Azure AD P1 (\$6) = \$41/user/month
 - Office 365 E5 (\$35) + Azure AD P2 (\$9) = \$44/user/month
- Office 365 E3 & Enterprise Mobility + Security
 - Office 365 E3 (\$20) + Enterprise Mobility + Security E3 (\$8.74) = ~\$29/user/month
 - Office 365 E3 (\$20) + Enterprise Mobility + Security E5 (\$14.80) = ~\$35/user/month
- Office 365 E5 & Enterprise Mobility + Security
 - Office 365 E5 (\$35) + Enterprise Mobility + Security E3 (\$8.74) = ~\$44/user/month
 - Office 365 E5 (\$35) + Enterprise Mobility + Security E5 (\$14.80) = ~\$50/user/month





Cloud Security Best Practices



Microsoft Cloud Recommendations Summary

- Disable user access protocols that aren't required - goal is Modern Auth with MFA.
- Enable user and admin activity logging in Office 365 (UnifiedAuditLogIngestionEnabled).
- Enable mailbox activity auditing on all O365 mailboxes.
- Review the recommendations in Office Secure Score and implement as many as possible.
- Enable “Password Hash Sync”
- Enable self-service password reset
- Ensure all users are registered for MFA
- Enable MFA for all users
- Enable sign-in & user risk policy
- Conditional Access: Block Legacy Auth (most attacks leverage legacy auth)
- Monitor App registrations.
- Audit consented permissions for apps & user access to apps



Microsoft Cloud: Protecting Admin Accounts

- Enforce MFA on all admin accounts
- Many of the basics remain the same
 - Least privilege is key and poorly understood in many cloud implementations
 - Least access, use the security features provided by the cloud
 - Cloud admin workstations – treat same as privileged users
- Limit admin role membership and monitor group membership. PIM can help.



Summary

- The cloud isn't inherently secure.
- There are many security features and controls that are available.
- Security controls need to be researched, tested, and implemented.
- Security in the cloud may cost extra.

Slides: Presentations.ADSecurity.org



Sean Metcalf (@Pyrotek3)
sean [at] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com