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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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
“The cloud is more secure since ______ spends millions every year on cloud security”
Internal Network

Intranet (LAN)

Router (WAN)

DMZ
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

Source: Microsoft Ignite Conference 2018

Sean Metcalf | @PyroTek3 | TrimarcSecurity.com

<table>
<thead>
<tr>
<th>Common Passwords Attempted in Password Spray Attacks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Spring</td>
</tr>
<tr>
<td>Summer</td>
<td>September</td>
</tr>
<tr>
<td>Winter</td>
<td>Football</td>
</tr>
</tbody>
</table>

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

300% increase in identity attacks over the past year.

Source: Microsoft Ignite Conference 2018

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

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Alert (TA18-086A)
Brute Force Attacks Conducted by Cyber Actors

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

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

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 different password. This type of brute-force attack can consume many accounts before being detected, and can be very successful if the password is weak.
Cloud Attack Timeline

**1. Compromised Credential**
Day 1 – 11: Attacker compromises privileged user’s non MFA-enabled account.

**2. Compromise**

**3. Exfiltrate Data**
Day 137 – 143: Attackers create rules on Contoso’s SharePoint and email to automate data exfiltration to a cloud storage solution.

**4. Connection to On-Prem**
Day 16 – 163: Attacker uses stolen credentials to VPN into corporate network.

**5. Move Laterally**
Day 163 – 243: Attacker moves laterally throughout organization’s network, compromising privileged credentials.

Source: Microsoft Ignite Conference 2018

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

https://myignite.techcommunity.microsoft.com/sessions/64523?source=sessions
Attacking the Cloud: Password Spraying

Password Spraying the OWA portal at https://outlook.office365.com/owa/. Sit tight...

5 threads remaining

[*] Now spraying the OWA portal at https://outlook.office365.com/owa/

[*] Current date and time: 11/04/2018 09:59:26
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
[ ]

```bash
>> -userlist 'C:\Temp\0365\UserList.txt' -OutFile 'c:\temp\0365\ews-sprayed-creds.txt' -password 'Password99'
[*] Now spraying the EWS portal at https://outlook.office365.com/EWS/Exchange.asmx
[*] Current date and time: 11/04/2018 09:56:01
[*] Trying Exchange version Exchange2010
```
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
Now spraying the EWS portal at https://outlook.office365.com/EWS/Ex
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

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Name</th>
<th>Service</th>
<th>Result</th>
</tr>
</thead>
</table>
## Attacking the Cloud: Password Spraying

<table>
<thead>
<tr>
<th>Basic info</th>
<th>Device info</th>
<th>MFA info</th>
<th>Conditional Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Id</td>
<td>b6c4fd5c-a7b0-4d75-ba65-5ba429789700</td>
<td>IP address 137.135.</td>
<td></td>
</tr>
<tr>
<td>Correlation Id</td>
<td>c8dec77b-2c4c-4071-8a7c-4bed95359c01</td>
<td>Location Washington, Virginia, US</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Leia</td>
<td>Date 11/4/2018, 10:31:29 AM</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:leia@trimarcrd.com">leia@trimarcrd.com</a></td>
<td>Status Success</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>2a8165e3-296c-4168-aa52-968bce5f1ef0</td>
<td>Client App Other clients; Older Office clients</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Office 365 Exchange Online</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application ID</td>
<td>000000002-0000-0ff1-ce00-0000000000000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Attacking the Cloud: Password Spraying

<table>
<thead>
<tr>
<th>Basic info</th>
<th>Device info</th>
<th>MFA info</th>
<th>Conditional Access</th>
<th>Troubleshooting and support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Id</td>
<td>b6c4fd5c-a7b0-4d75-ba65-5ba475769700</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correlation Id</td>
<td>8603d100-6135-45d1-956b-e8f360d99e6f</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Leia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:leia@trimarcrd.com">leia@trimarcrd.com</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>2a8165e3-296c-4168-aa52-968bce5f1ef0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Office 365 Exchange Online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application ID</td>
<td>00000002-0000-0ff1-ce00-000000000000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>137.135.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Washington, Virginia, US</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>11/4/2018, 10:31:11 AM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sign-in error code</td>
<td>50126</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure reason</td>
<td>Invalid username or password or invalid on-premise username or password.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client App</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IP Geolocation Information**

- **ISP:** Microsoft Corporation
- **Continent:** North America (NA)
- **Country:** United States (US)
- **Cty:** Washington
Microsoft Cloud Security Controls

YOUR SECURITY ACCESS CONTROLS...

GRATEFULLY ACCEPTED

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
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
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

<table>
<thead>
<tr>
<th>Policy name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-in risk remediation policy</td>
</tr>
</tbody>
</table>

**Assignments**

- Users
  - All users

**Conditions**

- Sign-in risk

**Controls**

- Access
  - Require multi-factor authentication

**Review**

- Estimated impact
  - Number of sign-ins impacted

**Sign-in risk**

**SETTINGS**

- Info

**Select the sign-in risk level**

- Low and above
- Medium and above
- High

Is this a “risky sign-in”?

- Anonymous IP
- Unfamiliar location
Enable User Risk Remediation Policy

What’s the chance the account is compromised?
- Some detected in real-time
- ~14 day learning period

Sign-in risk
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:


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.

Auditing
# Microsoft Cloud Auditing

<table>
<thead>
<tr>
<th>Audit Item</th>
<th>Category</th>
<th>Enabled by Default</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Activity</td>
<td>Office 365 Security &amp; Compliance Center</td>
<td>No</td>
<td>90 days</td>
</tr>
<tr>
<td>Admin Activity</td>
<td>Office 365 Security &amp; Compliance Center</td>
<td>No</td>
<td>90 days</td>
</tr>
<tr>
<td>Mailbox Auditing</td>
<td>Exchange Online</td>
<td>No*</td>
<td>90 days</td>
</tr>
<tr>
<td>Sign-in Activity</td>
<td>Azure AD (P1)</td>
<td>Yes</td>
<td>30 days</td>
</tr>
<tr>
<td>Users at Risk</td>
<td>Azure AD</td>
<td>Yes</td>
<td>7 days</td>
</tr>
<tr>
<td>Risky Sign-ins</td>
<td>Azure AD</td>
<td>Yes</td>
<td>7 days</td>
</tr>
<tr>
<td>Azure MFA Usage</td>
<td>Azure AD</td>
<td>Yes</td>
<td>30 days</td>
</tr>
<tr>
<td>Directory Audit</td>
<td>Azure AD</td>
<td>Yes</td>
<td>7 days</td>
</tr>
</tbody>
</table>

* Microsoft is gradually enabling mailbox auditing for tenants.

---

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]
Enable User & Admin Activity Auditing

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.

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.

Run a search to view results
Enable User & Admin Activity Auditing

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

Results

<table>
<thead>
<tr>
<th>Date</th>
<th>IP address</th>
<th>User</th>
<th>Activity</th>
<th>Item</th>
<th>Detail</th>
</tr>
</thead>
</table>

Run a search to view results

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Get Mailbox Auditing

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

<table>
<thead>
<tr>
<th>Name</th>
<th>AuditEnabled</th>
<th>AuditLogAgeLimit</th>
<th>AuditAdmin</th>
<th>AuditDelegate</th>
<th>AuditOwner</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeanMetcalf</td>
<td>False</td>
<td>90.00:00:00</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete...}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete...}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete...}</td>
</tr>
<tr>
<td>Name</td>
<td>AuditEnabled</td>
<td>AuditLogAgeLimit</td>
<td>AuditAdmin</td>
<td>AuditDelegate</td>
<td>AuditOwner</td>
</tr>
<tr>
<td>hailey</td>
<td>False</td>
<td>90.00:00:00</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete...}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete...}</td>
<td>{Update, MoveToDeletedItems, SoftDelete, HardDelete...}</td>
</tr>
</tbody>
</table>
```
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}
```
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
Protecting Administration
Cloud Administration Protection

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

```powershell
$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.)
**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
Introductions

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

Provide feedback

Tell us what you think about Azure Privileged Identity Management
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
Controlling Access
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
Conditional Access

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

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
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

Source: Microsoft Ignite Conference 2018
Disable Legacy Auth
Disable Service Access

- Outlook on the Web (OWA)
- Outlook desktop (MAPI)
- Exchange Web Services (EWS)
- Mobile (Exchange ActiveSync)
- IMAP
- POP
### Azure AD Connect Health - ADFS

#### Monitor your ADFS sign-in activity using Azure AD Connect Health

![Image of Azure AD Connect Health dashboard]

#### Risky IP Preview

<table>
<thead>
<tr>
<th>TIMESTAMP</th>
<th>TRIGGER TYPE</th>
<th>IP ADDRESS</th>
<th>BAD PASSWORD ERROR COUNT</th>
<th>EXTRANET LOCKOUT ERROR COUNT</th>
<th>UNIQUE USERS ATTEMPTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/26/2018 6:00 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>1728</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 5:30 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>1728</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 4:00 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>1728</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 3:00 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>2939</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 2:00 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>2243</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 1:00 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>1728</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 12:00 PM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>2090</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 11:00 AM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>3668</td>
<td>3</td>
</tr>
<tr>
<td>9/26/2018 10:00 AM</td>
<td>hour</td>
<td>12.17.77.98</td>
<td>0</td>
<td>1754</td>
<td>3</td>
</tr>
</tbody>
</table>

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]

Gaining Password Insight
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).

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)

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

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Azure AD Premium Password Protection

Authentication methods (Preview) - Password protection (Preview)

Manage

Password protection (Preview)

Custom smart lockout
- Lockout threshold: 10
- Lockout duration in seconds: 60

Custom banned passwords
- Enforce custom list: Yes

Custom banned password list:
- Trimarc
- Washington
- DCUnited

Password protection for Windows Server Active Directory
- Enable password protection on Windows Server Active Directory: Yes
- Mode: Enforced

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Microsoft Cloud Security “Tune Up”

MUCH IMPROVE

VERY BETTER
Secure Score

Your Secure Score is:

248

of 483

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 quickly 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 admin 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.

Threats
- Password Cracking
- Account Breach
- Elevation of Privilege

Compliance Controls
- ISO 27018:2014; Control C.9.4.2, A.10.8
- CSA CCM301: Control DS1-02
- GDPR; Control 6.8.5

Compliance Controls

Compare your score

<table>
<thead>
<tr>
<th>Secure Score</th>
<th>Seat Size Average Score</th>
<th>Please Select Industry Type</th>
<th>Average Secure Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>37</td>
<td>0</td>
<td>31</td>
</tr>
</tbody>
</table>

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 external mail forwarding for a user.

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.

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]
## Secure Score – Highest Priority Items

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

**Improvement actions**

<table>
<thead>
<tr>
<th>NAME</th>
<th>SCORE IMPACT</th>
<th>USER IMPACT</th>
<th>IMPLEMENTATION COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MFA for Azure AD privileged roles</td>
<td>50</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Enable MFA for users</td>
<td>30</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Enable sign-in risk policy</td>
<td>30</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Enable user risk policy</td>
<td>30</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Ensure all users are registered for multi-factor authentication</td>
<td>20</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Do not allow users to grant consent to unmanaged applications</td>
<td>10</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Enable policy to block legacy authentication</td>
<td>10</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Policy</th>
<th>Count</th>
<th>Severity</th>
<th>Category</th>
<th>Action</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unusual file share activity (by user)</td>
<td>0</td>
<td>[ ]</td>
<td>[ ] Threat detection</td>
<td>[ ]</td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Unusual file download (by user)</td>
<td>0</td>
<td>[ ]</td>
<td>[ ] Threat detection</td>
<td>[ ]</td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Multiple failed login attempts</td>
<td>0</td>
<td>[ ]</td>
<td>[ ] Threat detection</td>
<td>[ ]</td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Unusual file deletion activity (by user)</td>
<td>0</td>
<td>[ ]</td>
<td>[ ] Threat detection</td>
<td>[ ]</td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Activity from suspicious IP addresses</td>
<td>0</td>
<td>[ ]</td>
<td>[ ] Threat detection</td>
<td>[ ]</td>
<td>Oct 24, 2018</td>
</tr>
<tr>
<td>Activity from anonymous IP addresses</td>
<td>0</td>
<td>[ ]</td>
<td>[ ] Threat detection</td>
<td>[ ]</td>
<td>Oct 24, 2018</td>
</tr>
</tbody>
</table>
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 to proceed with your password attack?

[ Back | Finish | Cancel ]
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

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

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

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

TrimarcRO Password Attack

Terminate Attack
Simulate the Attack: Password Attack

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
Simulate the Attack: Phishing Attack

Configure Phishing Attack

Provide a name to the campaign

Name
Prize Giveaway

Target recipients

Configure email details

Compose email

Confirm

Security & Compliance

Threat management

Attack simulator

Start

Use Template

Please select a template in the list...

Prize Giveaway
Payroll Update
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
If you 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

Email body

$(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” button.

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]
Simulate the Attack: Phishing Attack

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.
Simulate the Attack: Phishing Attack

**TrimarcRD Payroll Update**

**Urgent - Update Your Payroll Details**

Joe User, Your payroll details need update.

---

Security & Compliance

- Threat management
- Attack simulator

---

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]

---

Hybrid Identity Protection Conference 2018
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 an 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.
Sign in

Email, phone, or Skype

Next

No account? Create one!

Can’t access your account?
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?
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.

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Report: Payroll Update


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.

<table>
<thead>
<tr>
<th>Total users targeted</th>
<th>Fastest Click</th>
<th>Fastest Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>5 minutes 31 seconds</td>
<td>11 minutes 38 seconds</td>
</tr>
<tr>
<td>Successful attempts</td>
<td>Average Click</td>
<td>Average Credentials</td>
</tr>
<tr>
<td>1</td>
<td>8 minutes 14 seconds</td>
<td>11 minutes 38 seconds</td>
</tr>
<tr>
<td>Overall Success Rate</td>
<td>Click Success Rate</td>
<td>Credential Success Rate</td>
</tr>
<tr>
<td>11%</td>
<td>22%</td>
<td>11%</td>
</tr>
</tbody>
</table>

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

Compromised Users

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

JoeUser@TrimarcID.com  
Link clicked: 11/3/2018, 8:43:00 PM
Office 365 Subscriptions (Capability & Cost)
<table>
<thead>
<tr>
<th>Office 365 Enterprise Tiers</th>
<th>Enterprise 1 (E1) - $8 user/month</th>
<th>Enterprise 3 (E3) - $20 user/month</th>
<th>Enterprise 5 (E5) - $35 user/month</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50 GB mailbox</td>
<td>50 GB mailbox</td>
<td>100 GB mailbox</td>
</tr>
<tr>
<td></td>
<td>File storage and sharing with 1 TB OneDrive storage</td>
<td>Unlimited personal cloud storage</td>
<td>Unlimited personal cloud storage</td>
</tr>
<tr>
<td></td>
<td>No Office installed apps</td>
<td>Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user )</td>
<td>Desktop versions of Office applications (One license covers 5 phones, 5 tablets, and 5 PCs or Macs per user )</td>
</tr>
<tr>
<td></td>
<td>eDiscovery with in-place search, hold, and export</td>
<td>eDiscovery with in-place search, hold, and export</td>
<td>Customer Lockbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Office ATP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Auto classification, smart import, and more with Advanced Data Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Office 365 Cloud App Security</td>
</tr>
</tbody>
</table>

[ Sean Metcalf | @PyroTek3 | TrimarcSecurity.com ]
Azure Active Directory Options

- 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

<table>
<thead>
<tr>
<th>Plan</th>
<th>Features</th>
<th>Office 365 E3 Price</th>
<th>Office 365 E5 Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD P1: $6</td>
<td>Azure Active Directory Premium P1, Intune, Azure Information Protection P1, Advanced Threat Analytics</td>
<td>$8.74** (per user per month)</td>
<td></td>
</tr>
</tbody>
</table>

---

[Sean Metcalf | @PyroTek3 | TrimarcSecurity.com]
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.
• 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.