

# Top 10 Office 365 Security Fails

*Assess Risks and Remediate Threats*

Joe Kuster – Director, Security/Compliance Solutions

Ed Higgins – Director, Solution Sales – Spyglass

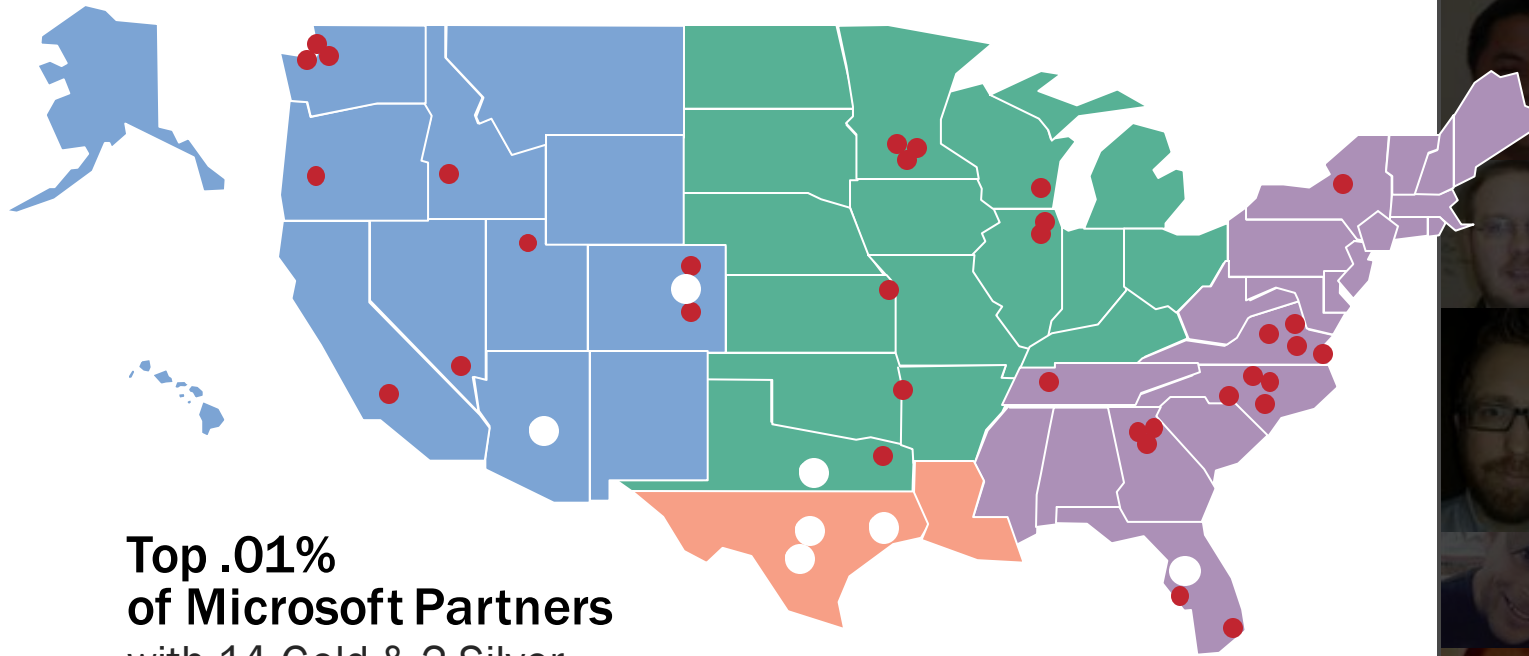


2019 Partner of the Year Winner  
PowerApps Award  
2019 Partner of the Year Finalist  
Modern Desktop Award  
Power BI Award

2019 MSUS Partner  
Award Winner  
Modern Workplace –  
Security and Compliance

# Introducing Catapult

Serving all 50 states, Mexico,  
Canada and the Caribbean



**Top .01%**  
of Microsoft Partners  
with 14 Gold & 2 Silver  
Competencies

**15,000** projects  
completed over **25** years



Transforming  
organizations for  
today's modern  
world

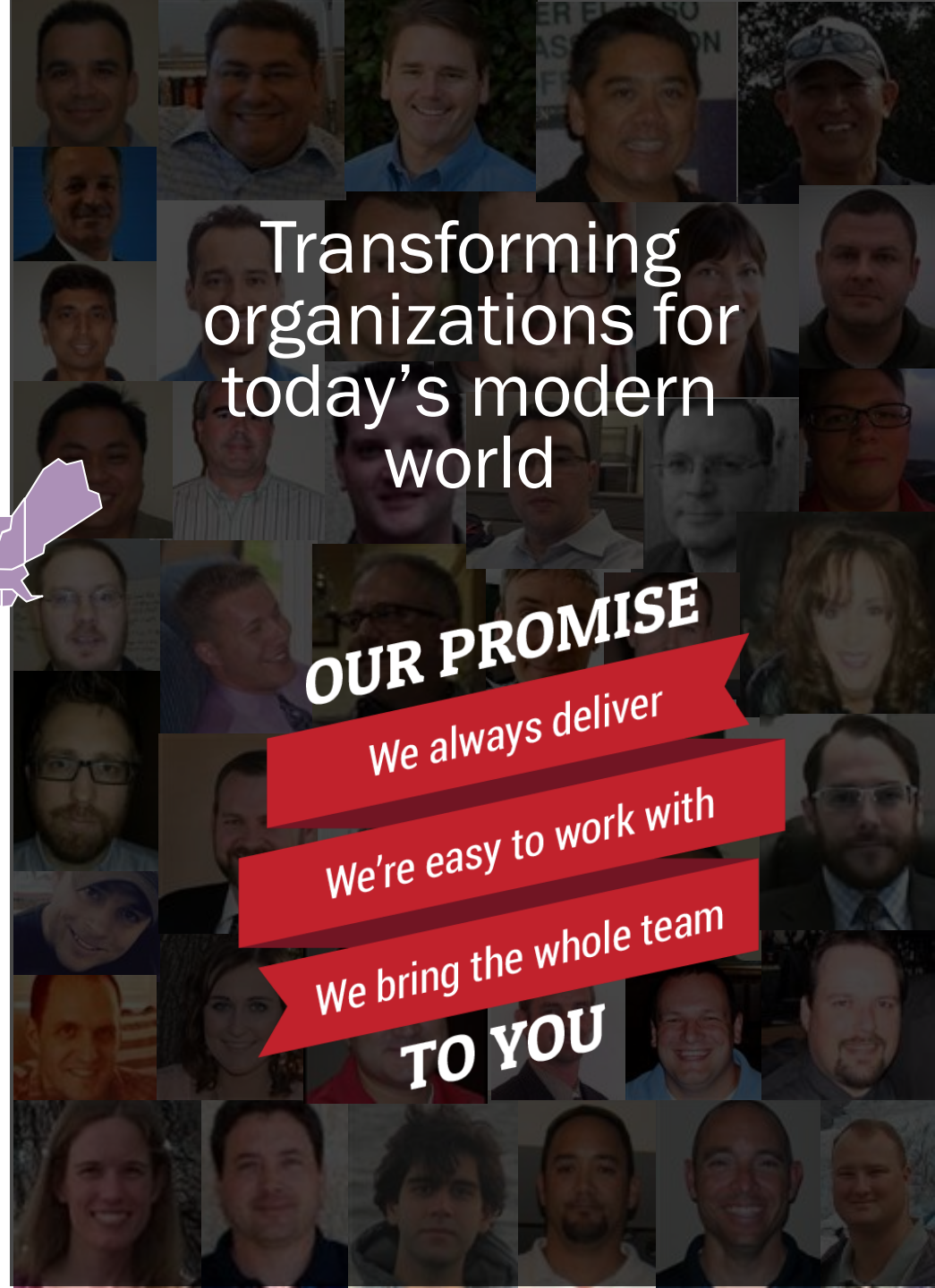
**OUR PROMISE**

We always deliver

We're easy to work with

We bring the whole team

**TO YOU**



# Security and Compliance Challenges

80%

of security incidents occur from within

62%

of cloud adopters nervous about cloud security

63%

of businesses are understaffed in security expertise

50%

of business cloud adoption is led by Shadow IT

51%

can't find and keep the needed skillsets

93%

of cyber attacks target user identity

\$3.9M

average cost of a successful security breach

# How does Catapult determine the top 10?



Office 365 Security assessments



Clients using our continuous security improvement program (Spyglass)



Microsoft insights









3<sup>rd</sup> party security researchers



What do we look at?

# Agenda

-  Active Users and Sign-in behavior
-  Privileged User Risks
-  Risky User and Device Behavior
-  Data Types and Flow  
Types of sensitive data stored in O365  
How it's being shared  
Data Governance and Classification
-  Organizational Threats  
Phishing threats and Security practices
-  Secure Score & Quick Wins
-  Next Steps: Planning Tactical and Strategic

# Executive Summary

## What do we usually find?



Business processes/users are sharing sensitive information in unsecured manners (credit cards, ssn, bank info).



Infected devices accessing company content.



Haven't deployed owned security tools.



Not sufficiently protecting administrator accounts.



Security controls (like MFA) are incorrectly setup.



External sharing & access needs governed.



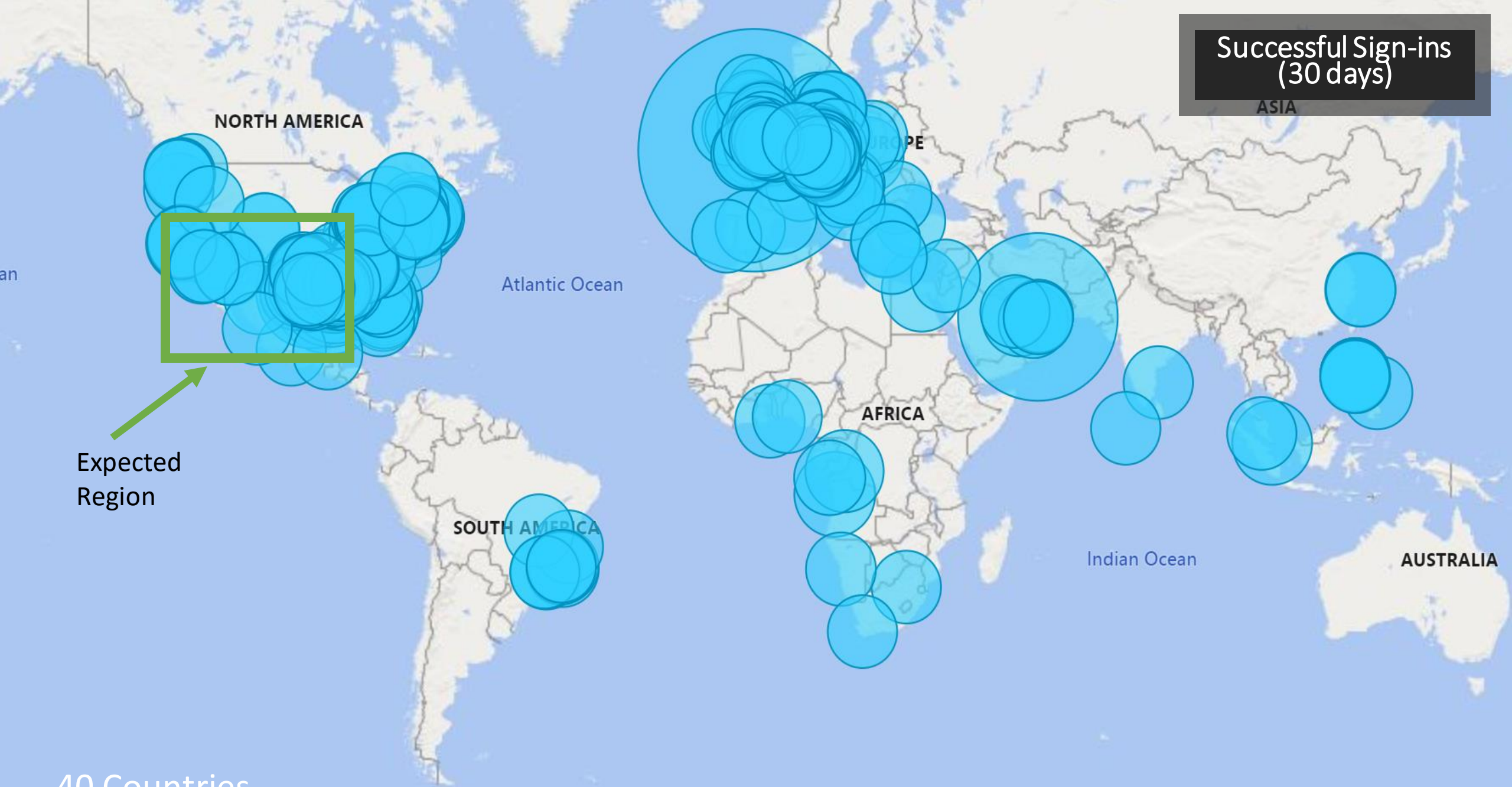
User trusted apps have unlimited access to their data.



# Fail #1 Not Knowing Where Your Users Are



Successful Sign-ins  
(30 days)

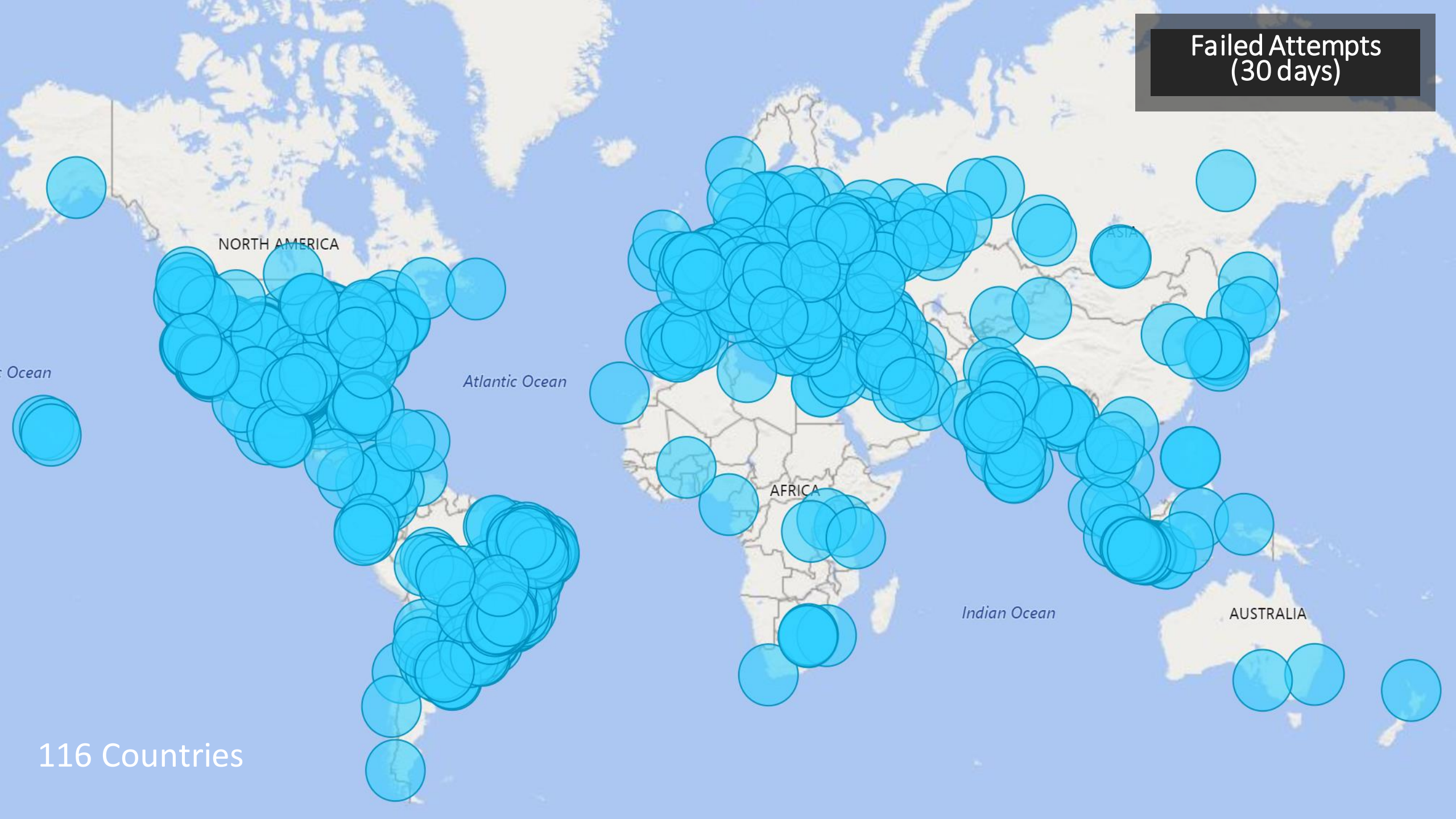


Expected  
Region

40 Countries



Failed Attempts  
(30 days)



NORTH AMERICA

Atlantic Ocean

AFRICA

ASIA

Indian Ocean

AUSTRALIA

116 Countries

Home > JoeKuster.com > Conditional Access - Policies > New > Conditions > Locations > Select

### New

Info

Name: Block Non-US Auth ✓

Assignments

- Users and groups: 0 users and groups selected
- Cloud apps or actions: No cloud apps or actions selected
- Conditions: 0 conditions selected **1**

### Conditions

Info

- Sign-in risk: Not configured
- Device platforms: Not configured
- Locations: Not configured **2**
- Client apps (preview): Not configured
- Device state (preview): Not configured

### Locations

Control user access based on their physical location. [Learn more](#)

Configure **3**

Yes  No

Include  Exclude **4**

Select the locations to exempt from the policy

All trusted locations

Selected locations **5**

Select None **5**

### Select

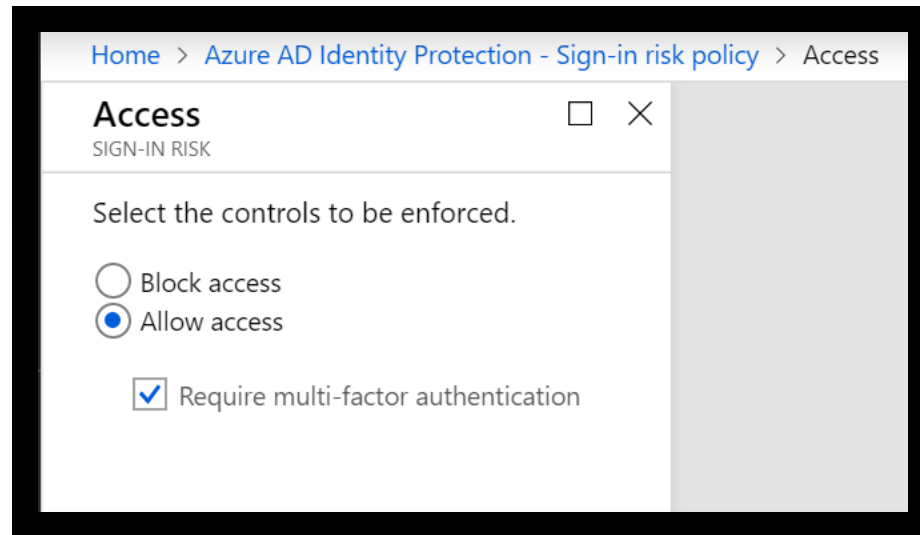
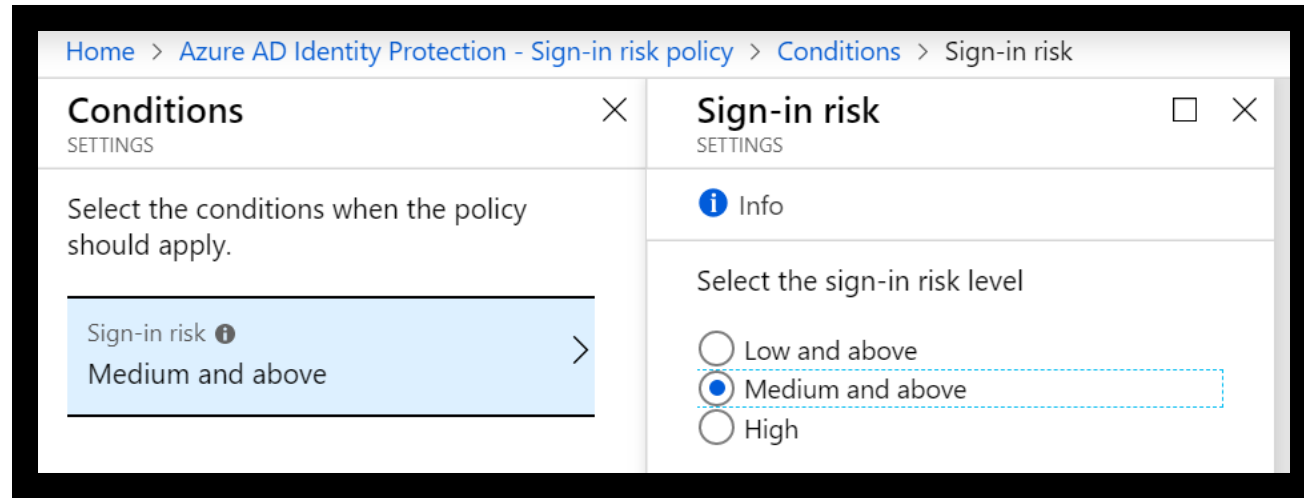
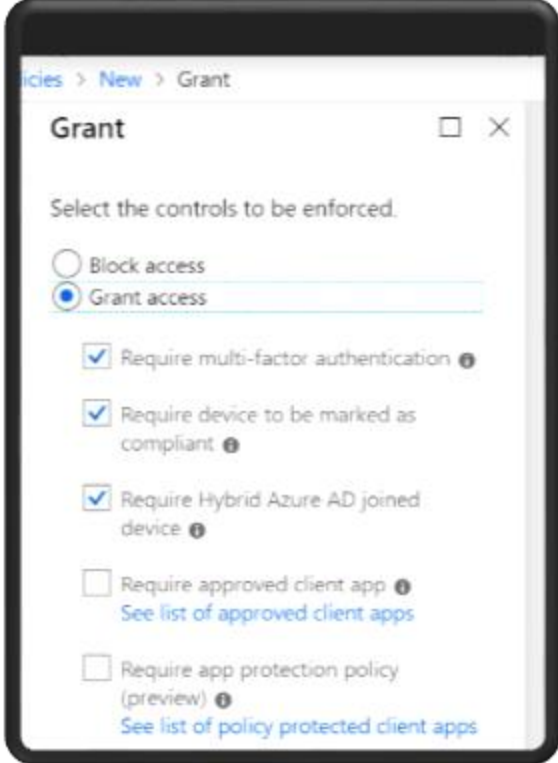
Locations

Search Locations...

NAME	TRUSTED
Home Lab IP	✓
MFA Trusted IPs	✓
Nigeria	
<input checked="" type="checkbox"/> US	


**6**

Geo-Fence?  
(not usually effective)



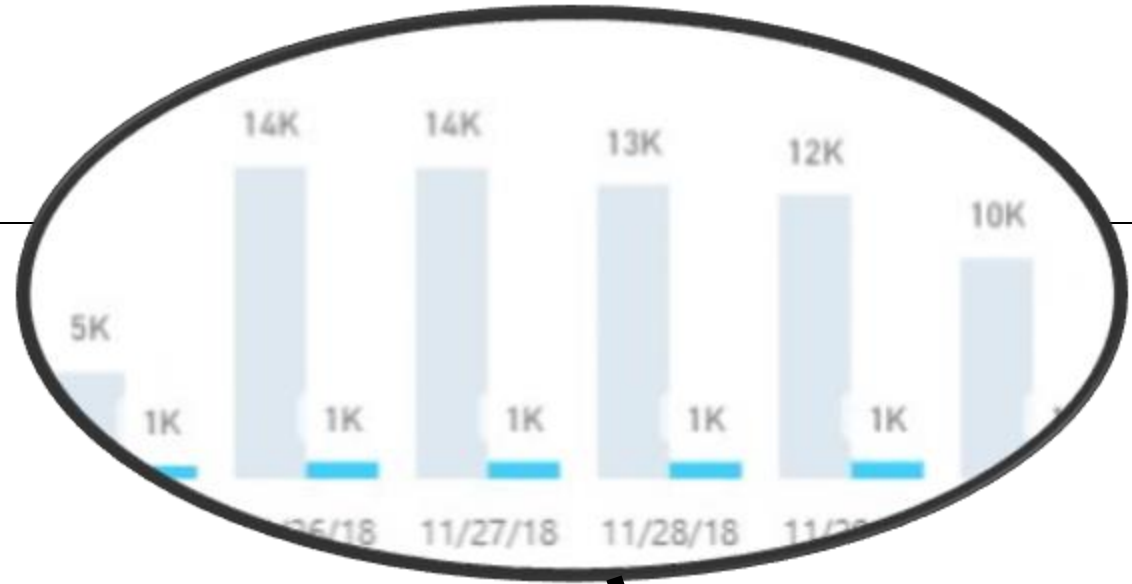
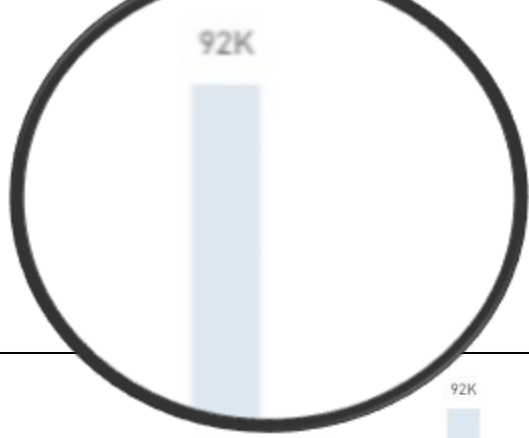
MFA/Device Compliance + Risk Analysis  
(Very Effective)



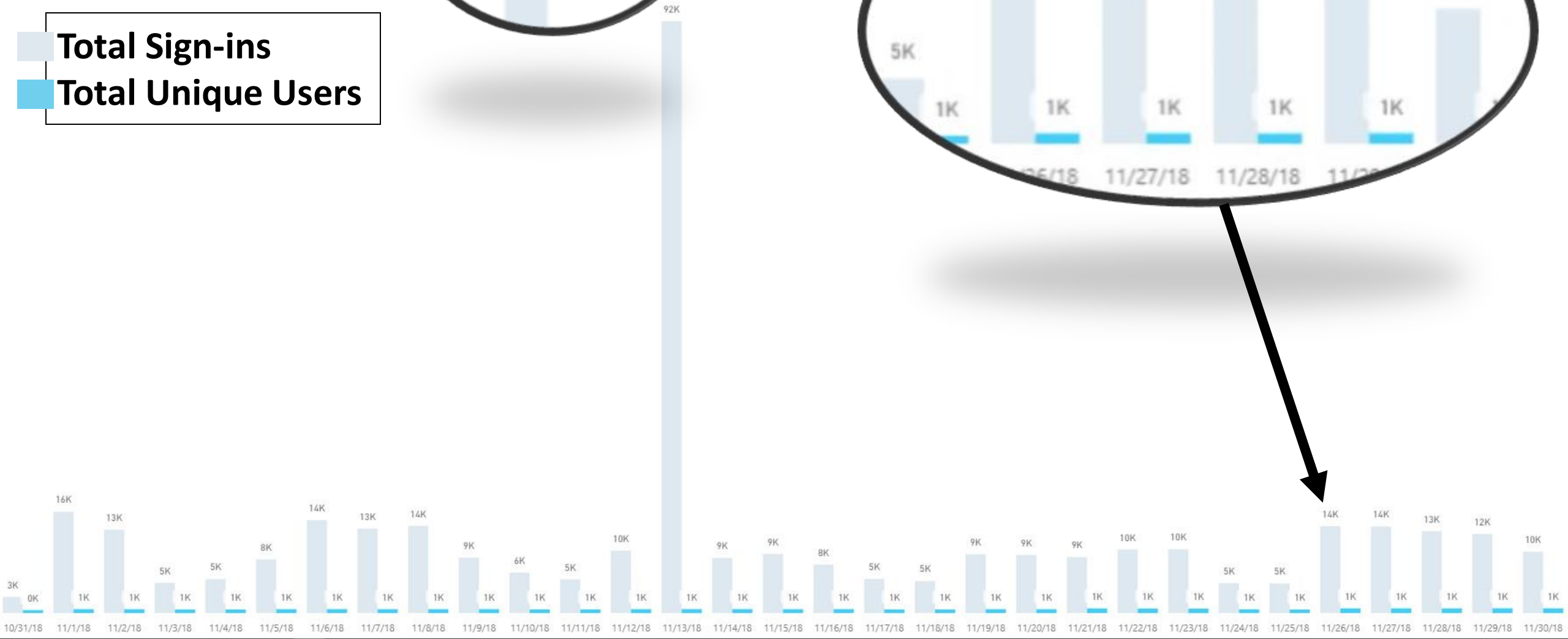


# Fail #2 Botching Multi-Factor Auth

# Sign-ins By Date



■ Total Sign-ins  
■ Total Unique Users





76

Total Apps

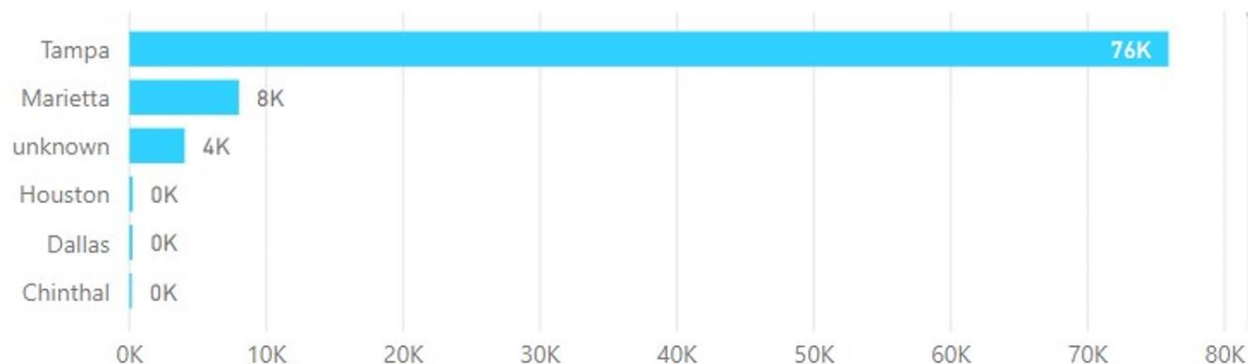
### Applications

Skype for Busin...	90.31%
Office 365 Exch...	8.14%
Office365 Shell ...	0.79%
Skype Web Exp...	0.21%
Incidentservice-...	0.09%
O365 Suite UX	0.09%
Bing	0.08%
Microsoft Office...	0.05%
Microsoft Office...	0.05%
Office 365 Shar...	0.04%
Azure Portal	0.02%
Azure Data Fact...	0.02%
Windows Azure...	0.02%
Call Quality Das...	0.01%
vlicient	0.01%
ACOM Azure W...	0.01%
Microsoft Team...	0.01%
Microsoft Team...	0.01%
Office.com	0.01%
Roaming	0.01%
Microsoft Office	0.00%

### Application Usage



### Application Sign-ins by Location



### Sign In Details

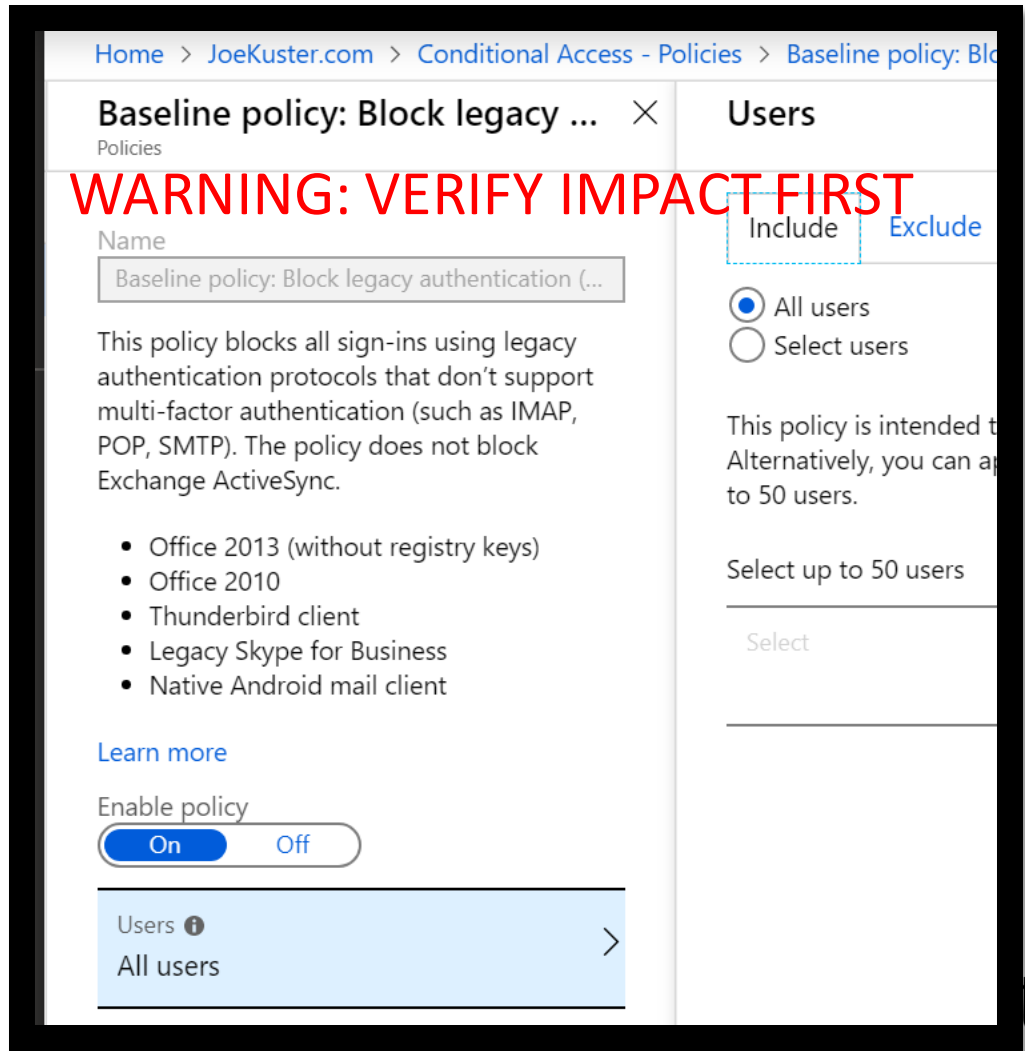
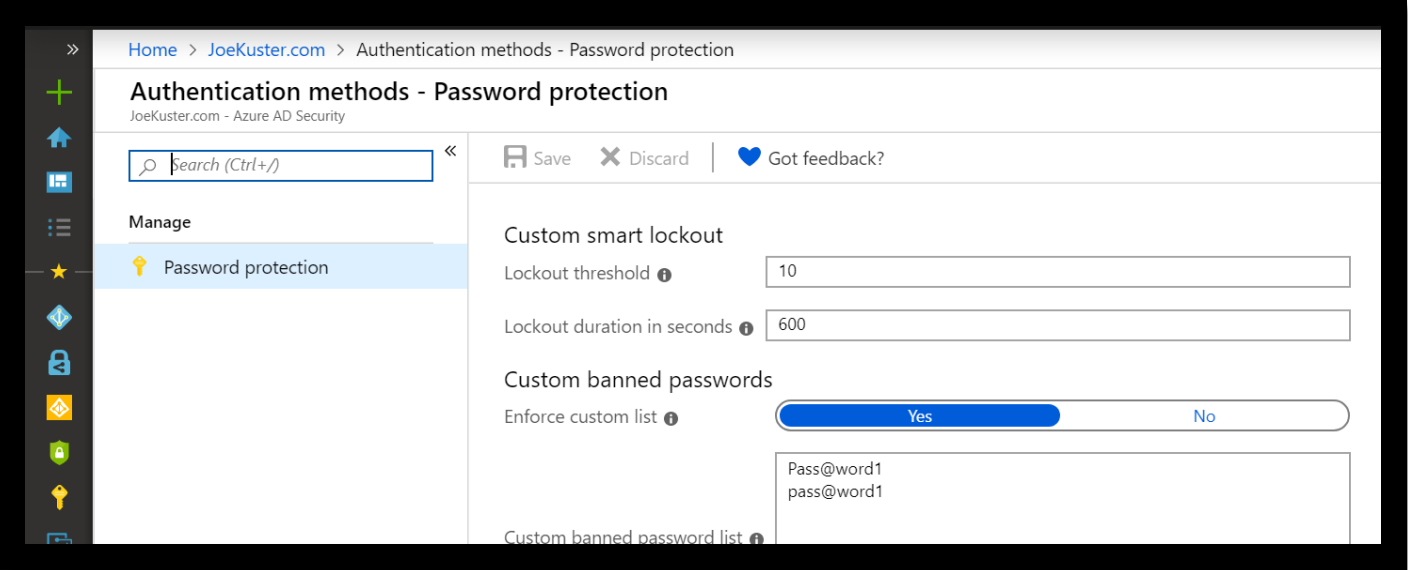
Application Name	Sign-in Date	IP Address	User Name	Sign-in Status	User Principal Na...
Bing	11/13/18	173.16.199.142	Zechariah Ward	Success	zechariah.ward@...
Microsoft Applicat...	11/7/18	64.237.29.27	Zechariah Ward	Success	zechariah.ward@...
Microsoft Authent...	11/7/18	64.237.29.27	Zechariah Ward	Success	zechariah.ward@...
Office 365 Exchan...	11/2/18	107.77.208.21	Zechariah Ward	Success	zechariah.ward@...



12/2/18, Office 365 Exchange Online, Eric Green, 222.168.6.250, , Jingyuezheng, Jilin, CN, Failure, Account is locked because user tried to sign in too many times with an incorrect user ID or password., 50053
12/2/18, Office 365 Exchange Online, Eric Green, 222.169.186.24, m, Minjiazhen, Jilin, CN, Failure, Account is locked because user tried to sign in too many times with an incorrect user ID or password., 50053
12/2/18, Office 365 Exchange Online, Eric Green, 222.191.233.23, m, Chong'an Qu, Jiangsu, CN, Failure, Account is locked because user tried to sign in too many times with an incorrect user ID or password., 50053
12/2/18, Office 365 Exchange Online, Eric Green, 222.216.37.3, , , Liangqingzhen, Guangxi, CN, Failure, Account is locked because user tried to sign in too many times with an incorrect user ID or password., 50053
12/2/18, Office 365 Exchange Online, Eric Green, 60.172.64.229, , , Huichengzhen, Anhui, CN, Failure, Account is locked because user tried to sign in too many times with an incorrect user ID or password., 50053
12/2/18, Office 365 Exchange Online, Eric Green, 61.134.36.117, , , Hujiaoyingzhen, Shaanxi, CN, Failure, Account is locked because user tried to sign in too many times with an incorrect user ID or password., 50053
12/2/18, Office 365 Exchange Online, Eric Green, 71.127.32.21, , , e.com, Bowie, Maryland, US, Success, , 0
12/2/18, Office 365 Exchange Online, Eric Leonard, 109.170.184.2, om, Durley, Hampshire, GB, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 111.26.198.30, n, Erdao Qu, Jilin, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 118.163.135.7, m, Sanchong, New Taipei, TW, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 118.163.58.11, m, Sanchong, New Taipei, TW, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 125.77.72.197, n, Cangshanzhen, Fujian, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 171.108.228.1, m, Qingxiu Qu, Guangxi, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 183.220.53.39, n, Qingyang Qu, Sichuan, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 202.107.34.25, m, Heping Qu, Liaoning, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 218.104.201.7, om, Qingyang Qu, Sichuan, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 218.64.57.12, ., Taohuazhen, Jiangxi, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 220.164.2.112, n, Lufeng Xian, Yunnan, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 27.189.251.86, n, Beiwangxiang, Hebei, CN, Failure, Sign-in was blocked because it came from an IP address with malicious activity., 50053
12/2/18, Office 365 Exchange Online, Eric Leonard, 27.189.251.86, n, Beiwangxiang, Hebei, CN, Failure, Invalid username or password or Invalid on-premise username or password., 50126

## Brute Force Attacks

- Reused compromised password from prior attack to gain intel (user changed PW back after 6 months).
- 92,000+ authentication attempts in a single day.
- Pattern of continued attacks.
- Successfully broke 4 accounts. 1 GA account.
- MFA was enabled, but Legacy Auth wasn't turned off.
- No one knew of the attack.



Smart Lockout +  
Disable Legacy Auth




How did we pull that?

# Security Graph API + Power BI

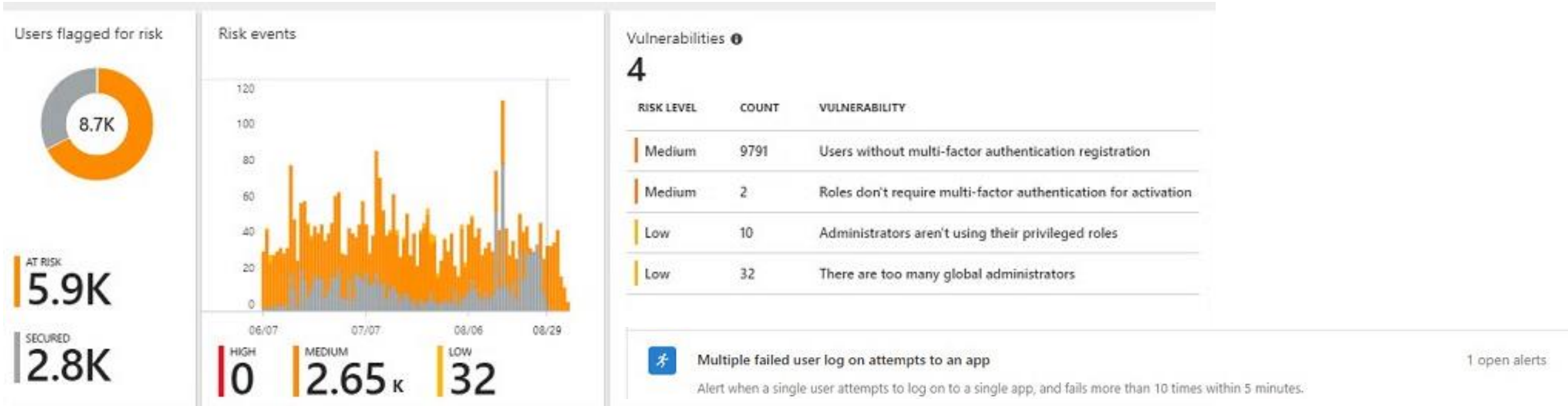




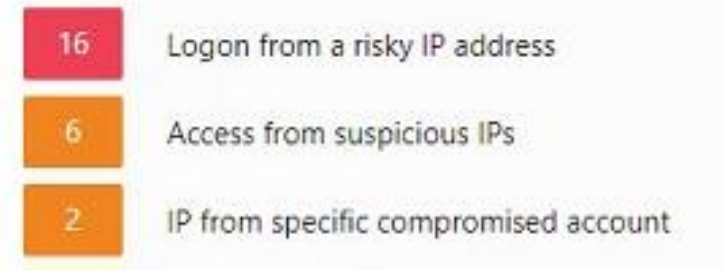


Fail #3 Not  
Tracking Risky  
Activity / Users

# Risky User Sign-ins



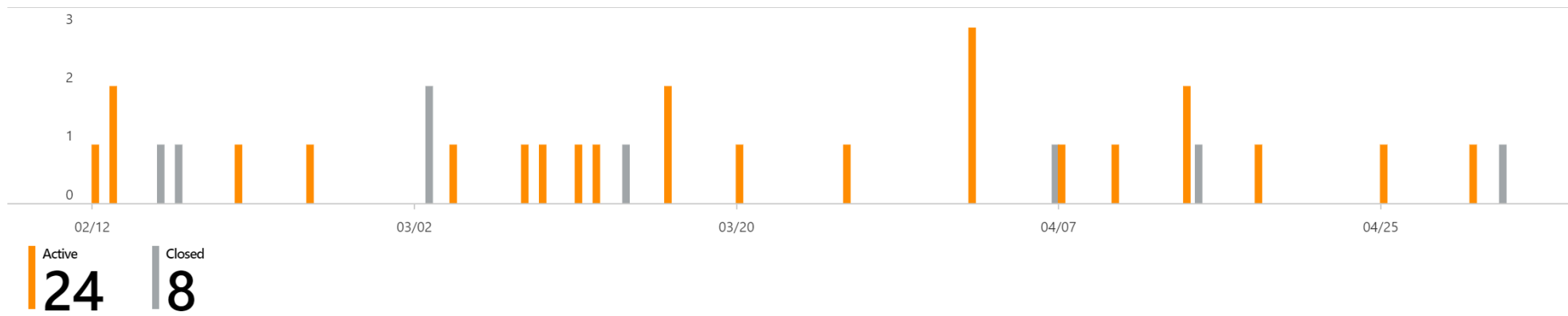
RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials <span>📘</span>	3 of 5	9/5/2019, 1:22 PM
Medium	Real-time	Sign-ins from anonymous IP addresses <span>📘</span>	532 of 623	9/17/2019, 8:16 PM
Medium	Offline	Impossible travels to atypical locations <span>📘</span>	0 of 6	9/5/2019, 1:22 PM
Medium	Real-time	Sign-ins from unfamiliar locations <span>📘</span>	33 of 66	9/16/2019, 4:13 PM
Low	Offline	Sign-ins from infected devices <span>📘</span>	0 of 4	8/8/2019, 8:04 AM



# Leaked Credentials

	USER	DISCOVERED (UTC)	STATUS	
	Claudia Powell	9/5/2019 13:22	Active	...
	Claudia Powell	9/3/2019 19:10	Active	...
	Ken Fuhrman	9/5/2019 06:53	Closed (password...)	...
	Ken Fuhrman	9/4/2019 20:13	Closed (password...)	...
	Ken Fuhrman	9/3/2019 19:04	Closed (password...)	...

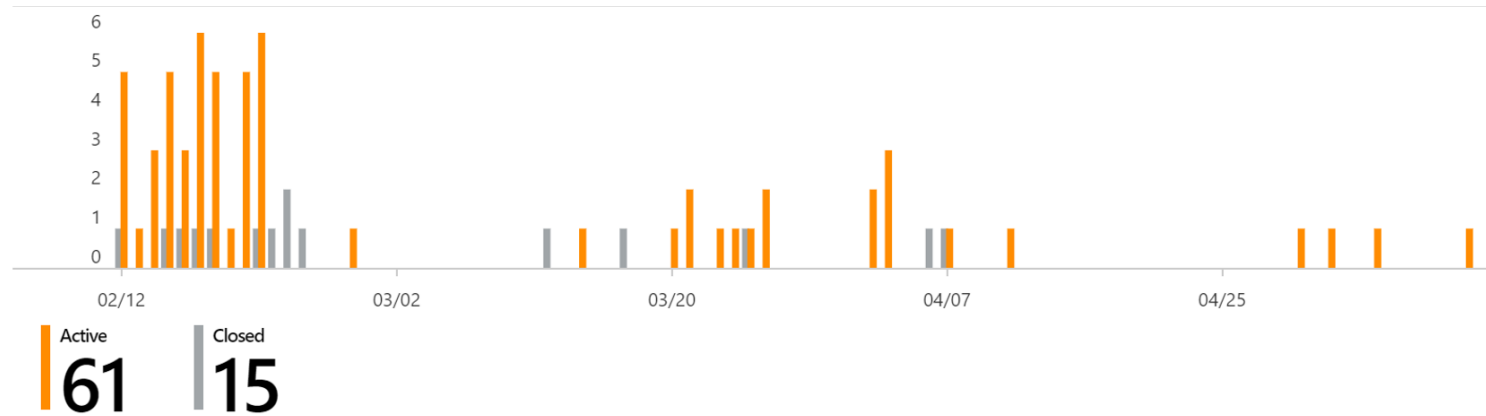




Ali, Ahmed	Alphington, Devon, GB	Brazzaville, Brazzaville, CG	91.84.193.114	102.141.12.26	2019-04-11 12:29:35Z	2019-04-11 12:07:56Z
Lynda Jeffrey	Alamo Heights, Texas, US	Ashorne, Warwickshire, GB	13.85.17.245	91.84.193.114	2019-04-03 06:22:52Z	2019-04-03 05:56:44Z
Riyaz Mohamed	Balotesti, Ilfov, RO	Dubayy, Dubayy, AE	89.35.228.199	94.200.253.242	2019-04-03 15:54:17Z	2019-04-03 15:43:37Z
Beard, Jack	Balotesti, Ilfov, RO	Ar Riya, Ar Riyad, SA	89.35.228.199	178.80.113.80	2019-04-08 11:41:24Z	2019-04-08 10:11:46Z
Doric, Sige	Balotesti, Ilfov, RO	NG, NG	89.35.228.199	102.176.247.107	2019-04-19 20:22:55Z	2019-04-19 20:15:56Z
Riyaz Mohamed	Ikorodu, Lagos, NG	Dubayy, Dubayy, AE	41.203.78.62	94.200.253.242	2019-04-03 16:09:29Z	2019-04-03 15:43:37Z
Clifton, Peter	Alphington, Devon, GB	Windhoek, Khomas, NA	91.84.193.114	164.160.109.15	2019-04-15 11:36:01Z	2019-04-15 10:52:05Z
Windcaid	Astoria, New York, US	Bad Nauheim, Hessen, DE	104.37.31.159	82.82.64.204	2019-04-15 17:46:30Z	2019-04-15 16:56:37Z
Sousa, Sebastian	Alphington, Devon, GB	Luanda, Luanda, AO	91.84.193.114	105.172.204.104	2019-05-01 07:16:33Z	2019-05-01 07:03:49Z
Tay, Sze Sze	Abington, Massachusetts, US	SG, SG	104.156.206.138	115.66.18.98	2019-04-26 15:41:53Z	2019-04-26 15:11:32Z
Sze Sze Tay	Ikorodu, Lagos, NG	SG, SG	169.239.195.57	203.125.146.174	2019-02-14 00:46:22Z	2019-02-14 00:46:22Z
Tommy Bourner	Ikorodu, Lagos, NG	Abbeville, Louisiana, US	105.112.98.255	68.70.237.178	2019-03-13 14:39:01Z	2019-03-13 13:41:54Z

# Impossible Travels

# Anonymous IP's



	USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS	
	Anthony <small>Walter</small>	43.249.36.105	Tsuen Wan, Hong Kong,...	2 instances	Active	...
	Anthony <small>Walter</small>	207.89.22.76	Dubai, Dubai, United Ar...	3/27/2019 08:03	Active	...
	Anthony <small>Walter</small>	94.46.13.169	Lisbon, Lisbon, Portugal	2 instances	Active	...
	Anthony <small>Walter</small>	94.126.172.26	Lisbon, Lisbon, Portugal	2 instances	Active	...
	Anthony <small>Walter</small>	43.249.36.100	Tsuen Wan, Hong Kong,...	2/13/2019 03:57	Active	...
	Bryan By <small>...</small>	104.37.31.70	New York, NY, United St...	2/18/2019 19:17	Active	...
	Bywalec, <small>Walter</small>	146.88.193.77	North Capitol Hill, CO, U...	5/3/2019 21:07	Active	...
	Deans, St <small>...</small>	196.52.84.26	Southampton, England, ...	5/1/2019 11:40	Active	...

How did we pull that?

# Azure AD Identity Protection

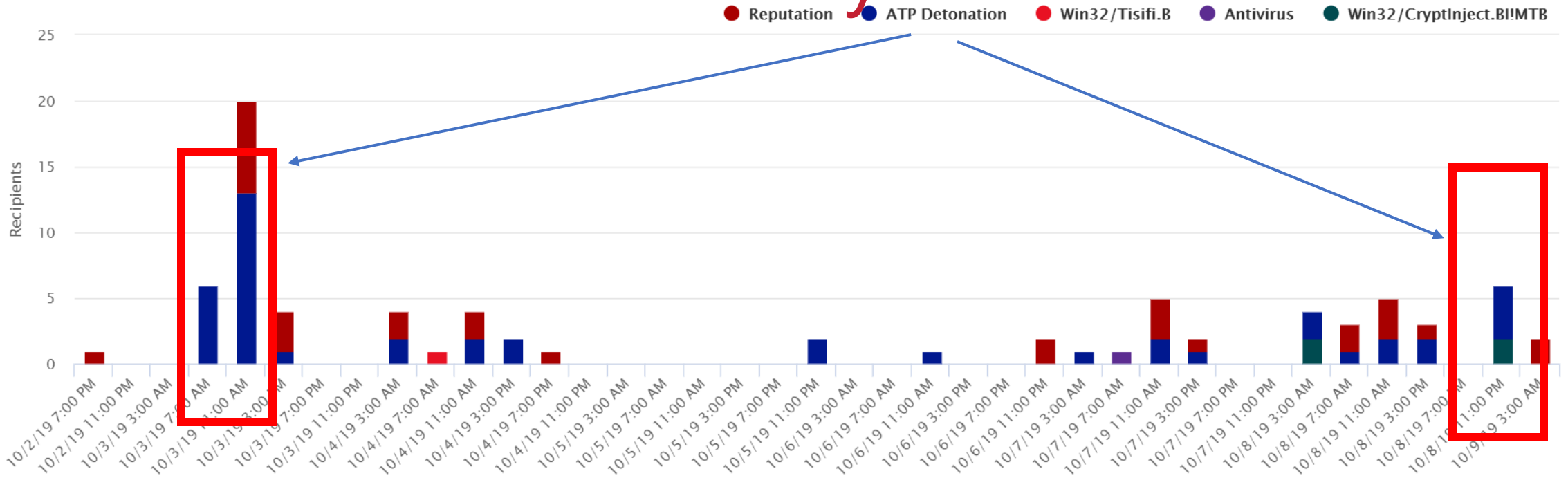






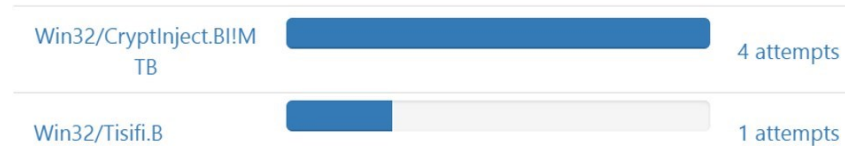
# Fail #4 Not Using Advanced Malware Tools

# Advanced Malware Activity

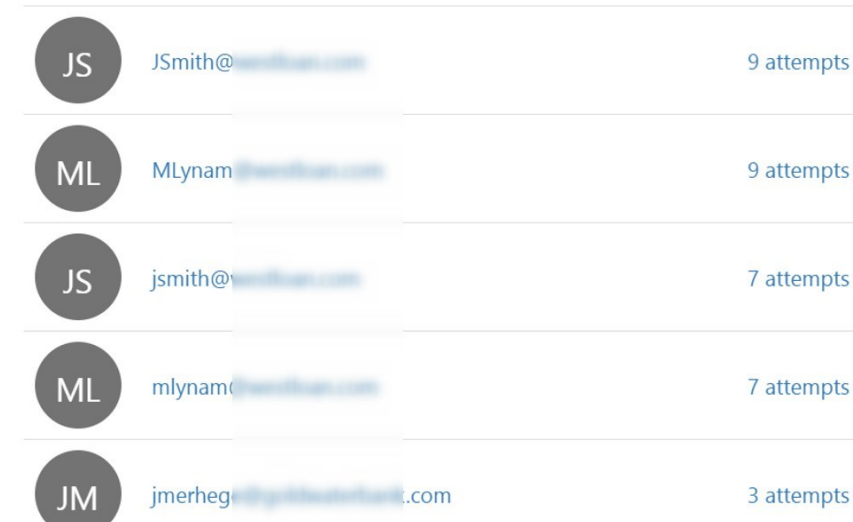


- Pattern of Advanced Attacks Detected
- No definition-based tools will detect/defend

## Top malware families



## Top targeted users



# ATP Malware Detection (SharePoint / OneDrive / Teams)

1 - 7 of 7 files

File name	Malware	Detection type	Confidence	Owner	App	Private	Status	Detection date
Docum...	Win32/...	Threat intellige...	High	Phillip	Microsoft...		Infe...	May 3, 2019
doc021...	Win32/...	Threat intellige...	High	Phillip	Microsoft...		Infe...	May 3, 2019
Refund...	JS/Phis...	Threat intellige...	High	Phillip				
Boston ...	O97M/...	Threat intellige...	High	Phillip				
Copy66...	Win32/...	Threat intellige...	High	Phillip				
Attache...	O97M/...	Threat intellige...	High	Phillip				
docum...	Win32/...	Threat intellige...	High	Phillip				

**Private**  
Only the file owner has access.

Home > Safe attachments

## Safe attachments

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams

### Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, ATP will prevent it from being opened. For more information, see [ATP for SharePoint and Microsoft Teams](#).

Turn on ATP for SharePoint, OneDrive, and Microsoft Teams


### Protect email attachments

Set up an ATP safe attachments policy for specific users or groups to help prevent people from opening malicious attachments. For more information, see [ATP safe attachments for email](#).



How did we pull that?


Threat Explorer / Cloud  
App Security / Office ATP



Fail #5 Not  
Tuning Phishing  
Protection

# Phishing Activity: Email

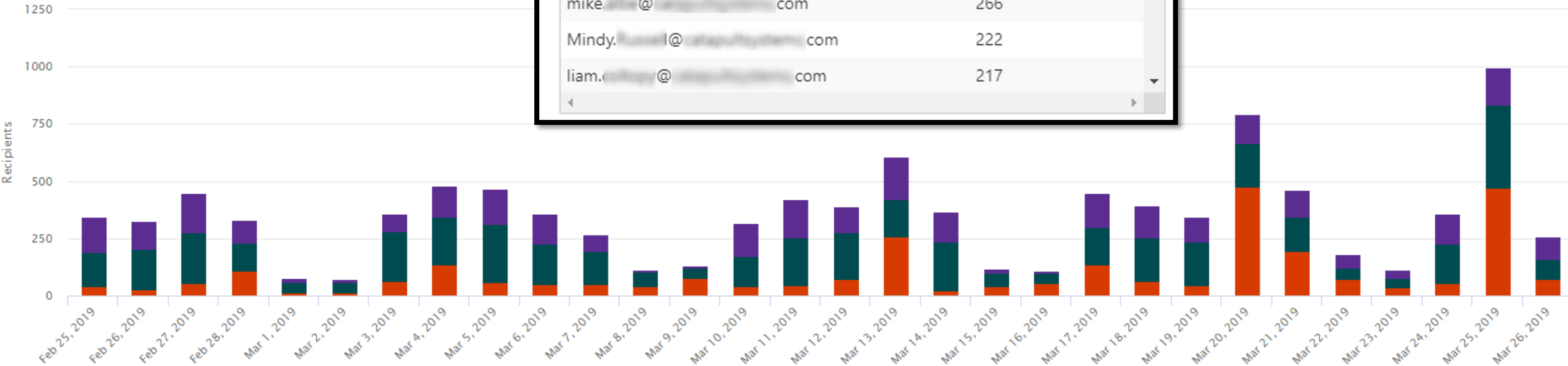
Blocked	Delivered	Delivered to junk
4501	2888	3055

 **Users targeted by phish campaign**

Review the list of users who have been targeted the most by phish campaigns.

This insight occurred 29 times in the last 29 day(s).

Name	Count
david.f...@stapupsystems.com	368
melody.berhart@stapupsystems.com	300
mike.ill@stapupsystems.com	266
Mindy.Russell@stapupsystems.com	222
liam.e...@stapupsystems.com	217






How did we pull that?

# Threat Explorer





Fail #6  
Blindly Trusting  
the Endpoint

# Check Endpoint Security Before Granting Access



Devices - All devices  
Microsoft Intune

Search (Ctrl+/)

Filter Columns Export Refresh

Search by IMEI, Serial number, Email, UPN, Device name or Management name

DEVICE NAME	MANAGED BY	OWNERSHIP	COMPLIANCE	OS	OS VERSION
HPEB	MDM	Corporate	Compliant	Windows	10.0.17134.112
OFFICEADMIN	MDM	Corporate	Not Compliant	Windows	10.0.17134.137
OFFICE-PC01	MDM	Corporate	Compliant	Windows	10.0.17134.112
OFFICE-PC02	MDM	Corporate	Compliant	Windows	10.0.17134.137

Intune

App Services

Virtual machines (class...)

Virtual machines



[Redacted]



[Redacted]

Actions ▾

Domain: Workgroup  
OS: Windows10 64-bit (Build 16299)

### Logged on users (last 30 days)

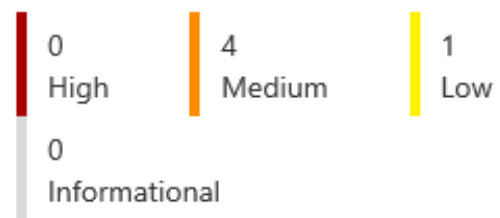
1 >

Interactive [1]  
RemoteInteractive [0]  
Other [0]

[Redacted] \pinpisher2

### No known risk ⓘ

Active alerts: ⓘ



Azure ATA Integration unavailable. [Check settings](#)

## Alerts related to this machine

✓ Last activity ↓	Title	User	Severity
01.20.2018   02:11:10	Unexpected behavior observed by a process run with no command line arguments Installation	[Redacted] nt authority\system	Medium
01.20.2018   02:08:46	A process was injected with potentially malicious code Installation	[Redacted] nt authority\system	Medium
01.20.2018   02:08:42	A process was injected with potentially malicious code Installation	[Redacted] nt authority\system	Medium
01.20.2018   02:08:37	Windows Defender AV detected a 'Finfish' backdoor Backdoor	[Redacted] \pinpisher2	Low



# Edit your policy Standard Policy (Lab)

Delete policy Increase Priority Decrease Priority

Customize the impersonation, spoofing, and advanced settings for the default policy. The default policy applies to all users within the organization, with additional domain scoped policies controlled by custom anti-phishing policies. [Learn more about these settings](#)

Priority: 0  
Status: On  
Last modified: June 6, 2019

Policy setting	Policy name	Description
	Standard Policy (Lab)	Applied to If the recipient domain is: joekuster.com joekuster.onmicrosoft.com joekuster.mail.onmicrosoft.com lab.joekuster.com www.joekuster.com home.joekuster.com

Impersonation	Users to protect	Action
	Protect all domains I own	Off
	Protect specific domains	Off
	Action > User impersonation	Move message to the recipients' Junk Email folders
	Action > Domain impersonation	Move message to the recipients' Junk Email folders
	Safety tips > User impersonation	On
	Safety tips > Domain impersonation	On
	Safety tips > Junk email character	On
	Mailbox intelligence	On
	Mailbox intelligence > Protection	On

Ransomware activity	0 open alerts	Jun 10, 2019	Settings
Malware detection [Disabled]	0 matches	Jun 10, 2019	Settings
Activity performed by terminated user	0 open alerts	Jun 10, 2019	Settings
Publicly accessible S3 buckets (AWS)	0 matches	Dec 2, 2018	Settings

- Edit policy
- View all matches
- View all alerts
- Enable...

# Most tenants do not have adequate Malware Detection or Compliance Policies

## Microsoft Defender Security Center

### Settings

#### General

- Data retention
- Alert notifications
- Power BI reports
- Secure score
- Advanced features

#### Permissions

- Roles
- Machine group

Select operating system to start onboarding process:

Windows 10

### 1. Onboard a machine

First machine onboarded: Completed

Onboard machines to Microsoft Defender ATP using the preparation instructions, read [Onboard and set up](#).

#### Deployment method

System Center Configuration Manager ...

You can use System Center Configuration Manager's deployment versions:

- System Center Configuration Manager
- System Center Configuration Manager R2
- System Center Configuration Manager (current build)

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams

Protect files in SharePoint, OneDrive, and Microsoft Teams  
If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, ATP will prevent it from being opened. [Learn more about safe attachments and Microsoft Teams](#)

Turn on ATP for SharePoint, OneDrive, and Microsoft Teams

#### Protect email attachments

Set up an ATP safe attachments policy for specific users or groups to help prevent people from opening malicious attachments for email

How did we pull that?

Office 365 ATP, Cloud  
App Security,  
Defender ATP



Fail #7 Not  
Monitoring /  
Protecting  
Content

# Types of Sensitive Data Stored in O365

- **Data Types**

- PCI, PII, Account Information, SSN, Financial Data

- **No governance controls**

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

▼ Alert when a file containing personally identifiable information (PII) is detected by in a sanctioned cloud app.

nualized Salary Projected Current Year Gross Comp # of Months ##### Westcot  
##,###.## ##,###.## #.# ##### Fertman, Eduardo Wolf XXX-XX-XXXX #/##/##

Match in content

cott, Christopher Michael XXX-XX-XXXX #/##/## ##,###.## ##,###.## #.# #####  
#/##/## ##,###.## ##,###.## #.# ##### Breaux, Eric J. XXX-XX-XXXX #/##/## ##,###.## ##,###.## #.

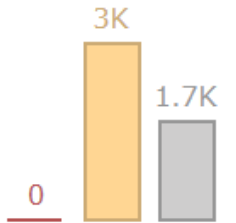
Match in content

##### Fertman, Eduardo Wolf XXX-XX-XXXX #/##/## ##,###.## ##,###.## #.# ##### Breaux, Eric J. XXX-XX-XXXX  
#/##/## ##,###.## ##,###.## #.# ##### Vanoveren, Jeremie S XXX-XX-XXXX #/##/## ##,###.## ##,###.##

4,672

Content matches

New over the last 6 months ▾



1,411

File containing PII detected in the cloud (built-...

1,411

File containing PHI detected in the cloud (built...

154

Externally shared source code

31

File containing PCI detected in the cloud (built...

7

Malware detection



# Exchange DLP Review

## DLP policy matches

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive information. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people.



FileName	SensitiveInformation
FW: FW: DP Induction (Basic) Course Azureus Offshore Training Center	U.S. Bank Account Number
FW: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
PAYMENTS UP OFFSHORE - WEEK 19.xlsx	U.S. Bank Account Number
New Bank details - SE00007531 Nugroho, Ashri Agung	U.S. Bank Account Number
RE: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
FW: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
FW: tt	U.S. Bank Account Number
FW: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
RE: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
FW: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
UK Cash Balances	U.S. Bank Account Number
PAYMENTS UP OFFSHORE - WEEK 19.xlsx	U.S. Bank Account Number
FW: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
RE: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
RE: UK Cash Balances	U.S. Bank Account Number
FW: FW: DP Induction (Basic) Course Azureus Offshore Training Center	U.S. Bank Account Number
FW: ORDER dispatched : 716185 // STIM STAR ANGOLA - 731-E Document	U.S. Bank Account Number
RE: Incumbency Certificate	U.S. Bank Account Number
RE: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
FW: Ecolab Products	U.S. Bank Account Number
RE: Sunarto Bin Karto - Chief Engineer	U.S. Bank Account Number
Scanned from a Xerox Multifunction Printer	U.S. Bank Account Number
RE: DAMEN wire payment	U.S. Bank Account Number
Dingbro Invoice	U.S. Bank Account Number
RE: Windcat Bank Balances	U.S. Bank Account Number

FileName	SensitiveInformation
MARLBROUGH_MATTHEW_WPS145368832.pdf	U.S. Social Security Number (SSN)
FG Employee Separation	U.S. Social Security Number (SSN)
Your 2018 W2	U.S. Social Security Number (SSN)
Re: Documentação Consolidação_jan/19	U.S. Social Security Number (SSN)
Documentação Consolidação_jan/19	U.S. Social Security Number (SSN)

FileName	SensitiveInformation
Update ABS	Credit Card Number
FW: Met Office Weather Forecast - PAWP	Credit Card Number
Paul, looking for a staycation this summer?	Credit Card Number
Approved: Approval of Invoice 042919NCR12139 from HANCOCK WHITNEY BAN	Credit Card Number
Ramadan Kareem Mark, exclusive offers for a Blessed Month	Credit Card Number
It's all about you: look after yourself and Pullman will help	Credit Card Number
Approved: Approval of Invoice 042919N2588559 from HANCOCK WHITNEY BAN	Credit Card Number
Met Office Weather Forecast - Arklow Bank	Credit Card Number
Action Required: Approval of Invoice 042919N2588559 from HANCOCK WHITNE	Credit Card Number
Production Support Requests 1129 and 723	Credit Card Number
Summer's coming and it's bringing incredible savings!	Credit Card Number
Action Required: Approval of Invoice 042919NCR12139 from HANCOCK WHITNE	Credit Card Number
FW: Met Office Weather Forecast - Luchterduinen	Credit Card Number
FW: Production Support Requests 1129 and 723	Credit Card Number
Dispatch - 21108770 - 74890	Credit Card Number
	Credit Card Number
FW: Production Support Requests 1129 and 723	Credit Card Number
FW: Production Support Requests 1129 and 723	Credit Card Number

How did we pull that?

O365 DLP, Cloud App Security (or Unified Audit Log)





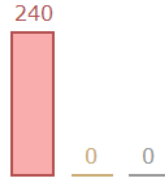
# Fail #8 Not Threat Hunting



240

Activity matches

New over the last 6 months ▾



# Abnormal User Activity

240

Multiple failed user logon attempts to a service

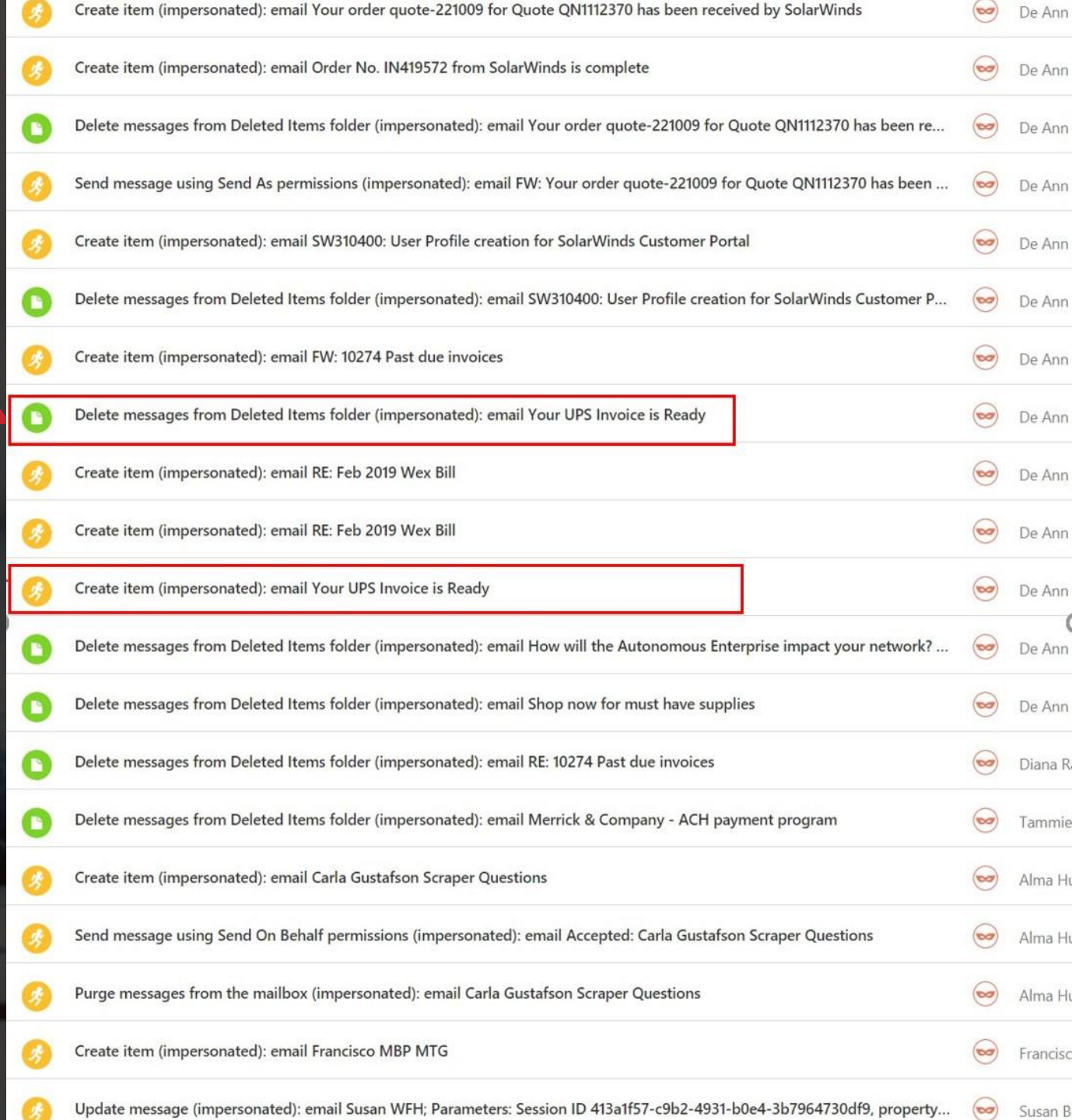
1 - 20 of 240 activities

New policy from search

Activity	User	App	IP address	Location	Device	Date
Failed log on (Failure messag...	Der Melkonian, Setrak	Office 365	86.97.143.60	United ...	PC, Windows	May 11, 2019,...
SHOW SIMILAR						
General User IP address Send us feedback...						
Description: Failed log on (Failure message: Invalid password, entered expired password)						
Type: Failed log on	User: Der Melkonian, Setrak	Date: May 11, 2019, 7:41 AM	IP address: 86.97.143.60			
Type (in app): OrgIdWsTrust2:process	User organizational unit: —	Device type: PC, Windows	IP category: —			
Source: App Connector <a href="#">View raw data</a>	User groups: —	User agent tags: —	Tags: —			
ID: 1588db233c24cf2c4bdd5c673b...	Activity objects:  Office 365, Request ID, s...	App: Office 365	Location: United Arab Emirates, Ab...			
Matched policies: <a href="#">Multiple failed user logon...</a>			ISP: Emirates Telecommunications Cor...			
Failed log on (Failure messag...	Der Melkonian, Setrak	Office 365	86.97.143.60	United ...	PC, Windows	May 11, 2019,...
Failed log on (Failure messag...	Der Melkonian, Setrak	Office 365	86.97.143.60	United ...	PC, Windows	May 11, 2019,...

Do not rely on automated tools to highlight all threats.

Expert analysis is sometimes required, but the tools make it easier.




How did we pull that?

# Cloud App Security (or Unified Audit Log)





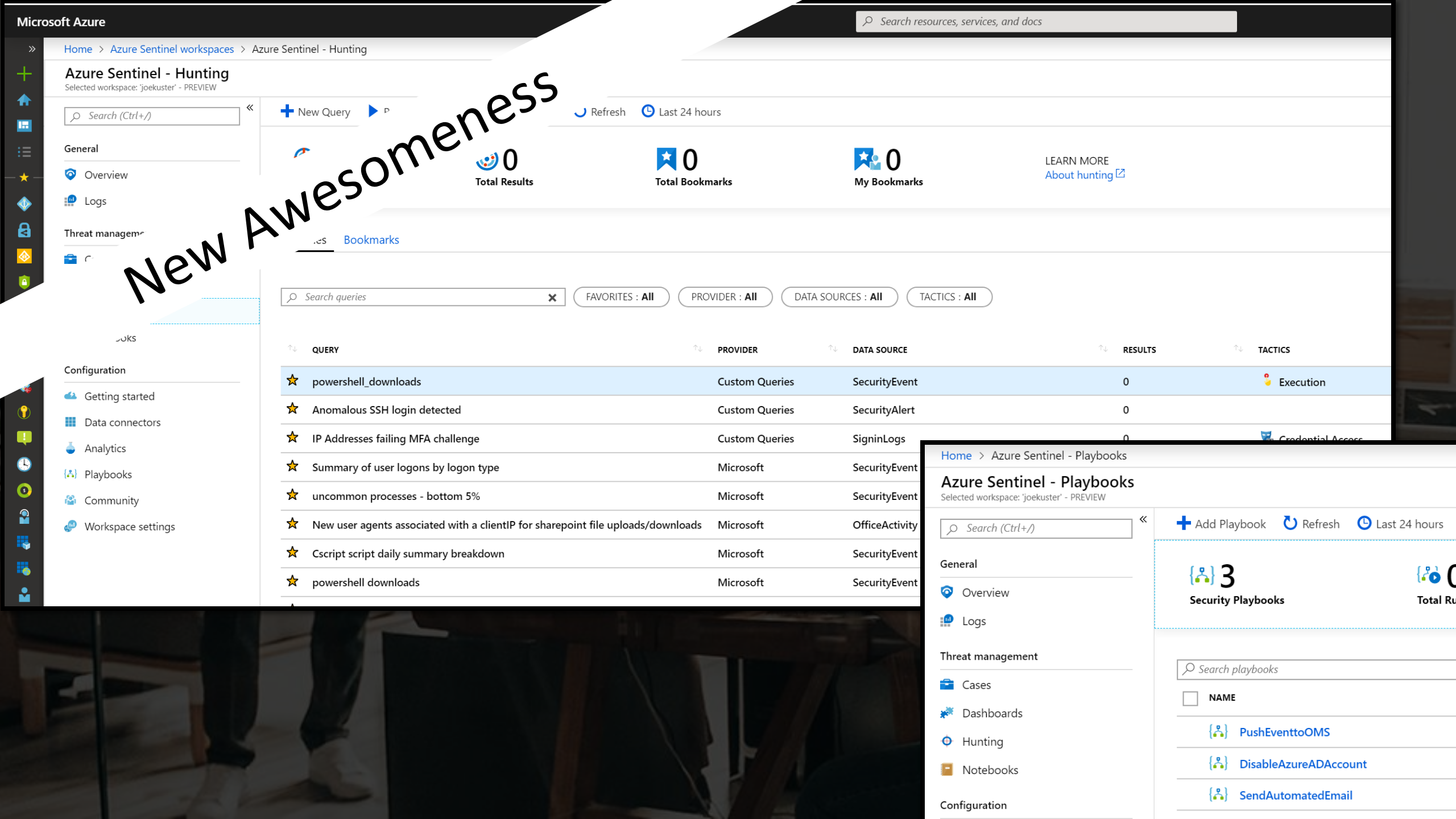


Fail #9 Not  
Enforcing /  
Automating  
Responses



# Don't let this happen to you!

- Forever stuck in Auditing & Alert Overload
  - Data Loss Prevention Reporting Only.
  - Risky Sign In – Alert, but no Proactive Protection.
  - Legacy Authentication Left Open to Support Old Client Apps.
  - MFA stalls due to service/shared/external accounts or lack of creativity in methods.
  - Business is still figuring out Data Classification (infinite loop of policy meetings).
  - IT Policies need updated before tech can be rolled out.
  - Can't deploy modern protection due to old OS's, Apps, or Practices.



### Azure Sentinel - Hunting

Selected workspace: 'joekuster' - PREVIEW

Search (Ctrl+/)

+ New Query

Refresh Last 24 hours

#### General

Overview

Logs

#### Threat management

Cases

Dashboards

Hunting

Notebooks

#### Configuration

Getting started

Data connectors

Analytics

Playbooks

Community

Workspace settings



0  
Total Results

0  
Total Bookmarks

0  
My Bookmarks

LEARN MORE  
About hunting

New Awesomeness

Search queries

FAVORITES : All

PROVIDER : All

DATA SOURCES : All

TACTICS : All

QUERY	PROVIDER	DATA SOURCE	RESULTS	TACTICS
★ powershell_downloads	Custom Queries	SecurityEvent	0	Execution
★ Anomalous SSH login detected	Custom Queries	SecurityAlert	0	
★ IP Addresses failing MFA challenge	Custom Queries	SigninLogs	0	Credential Access
★ Summary of user logons by logon type	Microsoft	SecurityEvent		
★ uncommon processes - bottom 5%	Microsoft	SecurityEvent		
★ New user agents associated with a clientIP for sharepoint file uploads/downloads	Microsoft	OfficeActivity		
★ Cscript script daily summary breakdown	Microsoft	SecurityEvent		
★ powershell downloads	Microsoft	SecurityEvent		

### Azure Sentinel - Playbooks

Selected workspace: 'joekuster' - PREVIEW

Search (Ctrl+/)

+ Add Playbook Refresh Last 24 hours

#### General

Overview

Logs

#### Threat management

Cases

Dashboards

Hunting

Notebooks

#### Configuration

3  
Security Playbooks

0  
Total Results

Search playbooks

NAME

PushEventtoOMS

DisableAzureADAccount

SendAutomatedEmail



Fail #10 Not  
Having an  
Ongoing Security  
Improvement  
Plan



# Key Recommendations

## Quick Wins 0-3 Months

- Low user impact
- Low to moderate implementation cost

Refresh or implement company policies for IT Security, Data Handling, Mobile Devices, Retention & Classification  
Fix Gaps in Incident Response (Office ATP, ATA, Monitoring)  
Security Continuous Improvement Program (Security Coaching)  
Phishing Education & Assessment Program (Attack Simulator)  
Clean up Global Admins and complete MFA and Privileged Identity Management  
Review security reports weekly  
Perform Security Score recommended steps to reach at least 240  
Implement short term Data Loss Prevention stop gaps until Azure AIP deployment  
Develop end-user data handling training for email content  
Validate applicability of GDPR & California Privacy Act for organization

## 3-6 Months

- Low to moderate user impact
- Moderate implementation cost

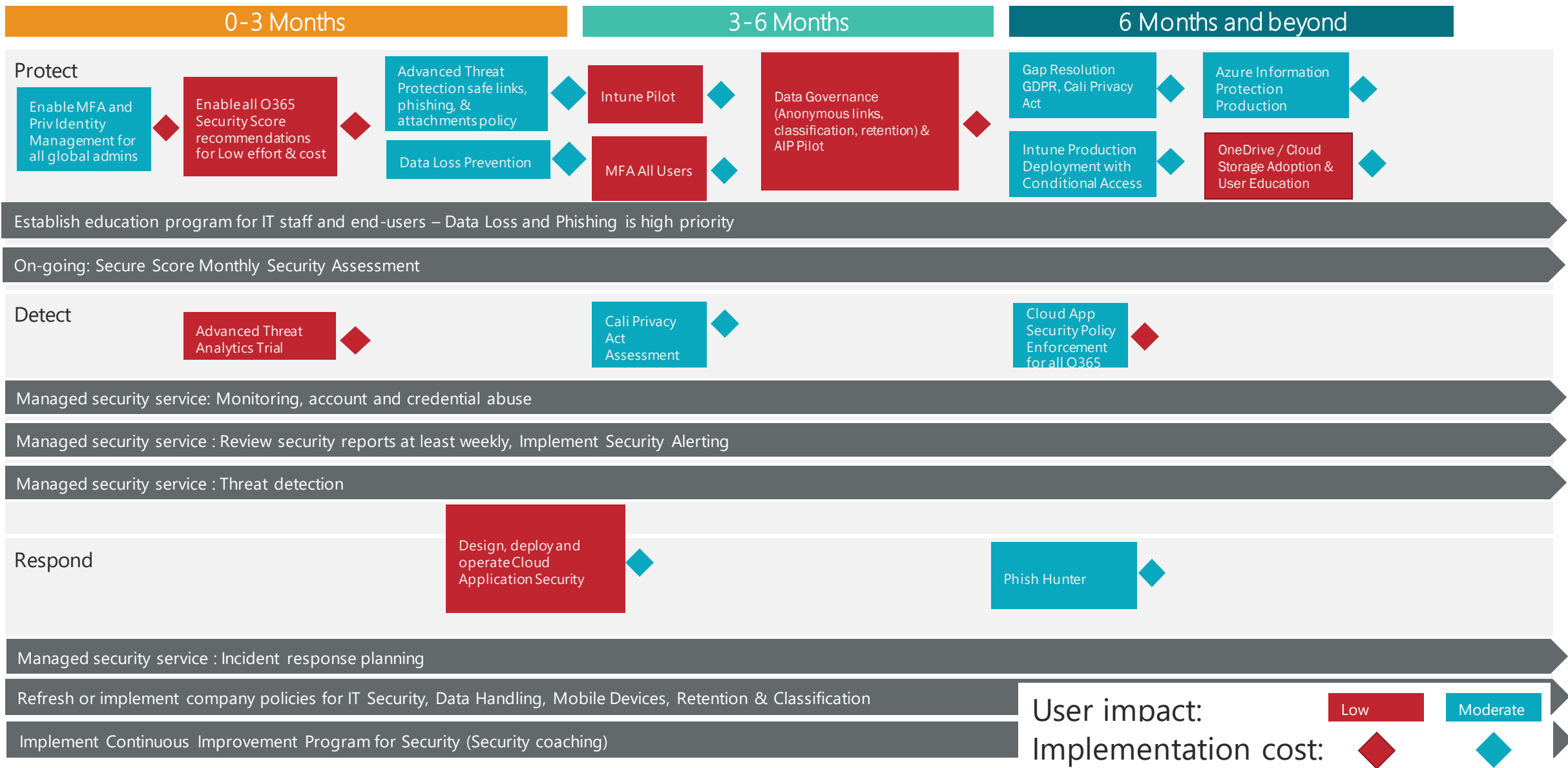
Compliance Assessments for GDPR, California Privacy Act  
Resolve non-compliant mobile devices and enable conditional controls for all users with sensitive data access  
Conditional Access policy enforcement to prevent anomalous access, impossible travel, reduce MFA prompts on trusted scenarios  
MFA for all users  
Data Governance (Anonymous links, classification, retention, data loss prevention)  
Azure Information Protection Pilot

## 6 Months and beyond

- Moderate user impact
- Low and moderate implementation cost

Complete gap resolution for GDPR, California Privacy Act  
Enforce Cloud App Security Policy + remediation for all end users  
OneDrive / Cloud Storage Adoption & User Education  
Azure Information Protection production deployment  
Leverage Graph API for threat hunting and issue automation (Spyglass, Phish Hunter, etc)

# Security Roadmap



A dark, blurred background of a laptop screen showing HTML code. A red L-shaped graphic element is positioned on the left side of the screen, framing the text. The text is white and centered on the screen.

Bonus Tip:  
Attack Your Users Before  
Hackers Do



# Simulate attacks



## Simulate attacks to test your defenses

Run realistic phishing attempts, such as spear phishing and password attacks, to identify vulnerable users within your organization.

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](#)

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.

[Launch Attack](#)

[Attack Details](#)

# Q&A



**Joe Kuster** (CISSP, MCPS, MCITP)  
Director, Security & Compliance Solutions  
Catapult Systems  
[Joe.Kuster@catapultsystems.com](mailto:Joe.Kuster@catapultsystems.com)



**Ed Higgins** (CISSP, CISM, CGEIT)  
Director, Solution Sales - Spyglass  
Catapult Systems  
[Ed.Higgins@catapultsystems.com](mailto:Ed.Higgins@catapultsystems.com)

Want an Office 365 Security Assessment?  
Need Azure Sentinel Deployed?



Thank you.

