

Ciérrale la puerta al cibercrimen con seguridad basada en identidades

Javier Dominguez
Senior Program Manager

81%

of data breaches
involved weak, default,
or stolen passwords

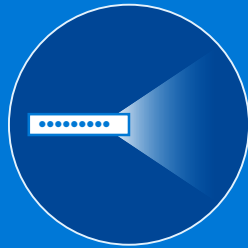
300% increase in identity attacks over the past year.



Phishing

23M

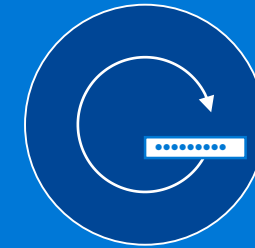
high risk enterprise sign-in attempts detected in **March 2018**



Password Spray

350K

compromised accounts detected in **April 2018**

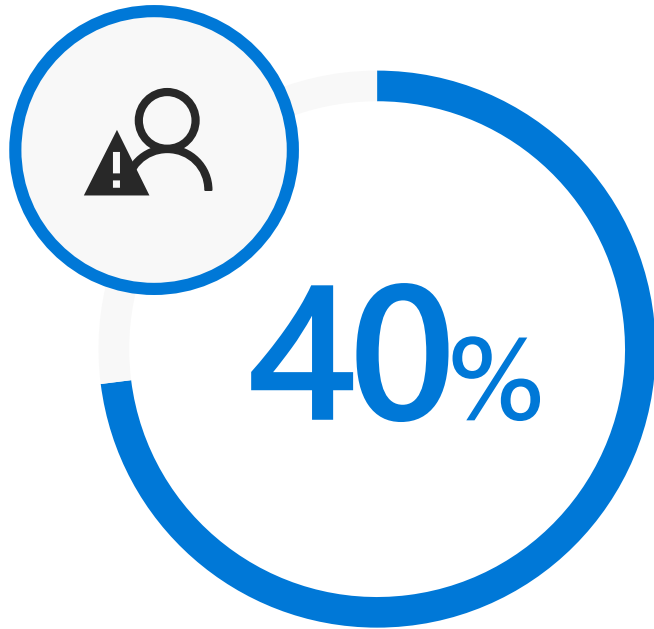


Breach Replay

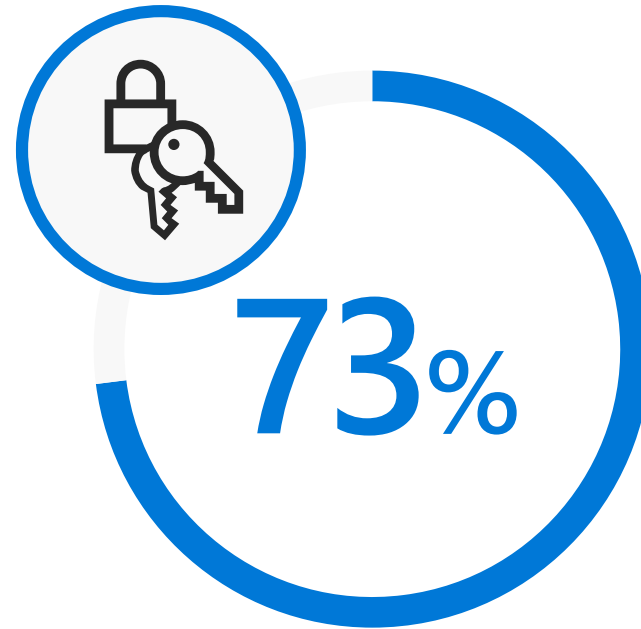
4.6B

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

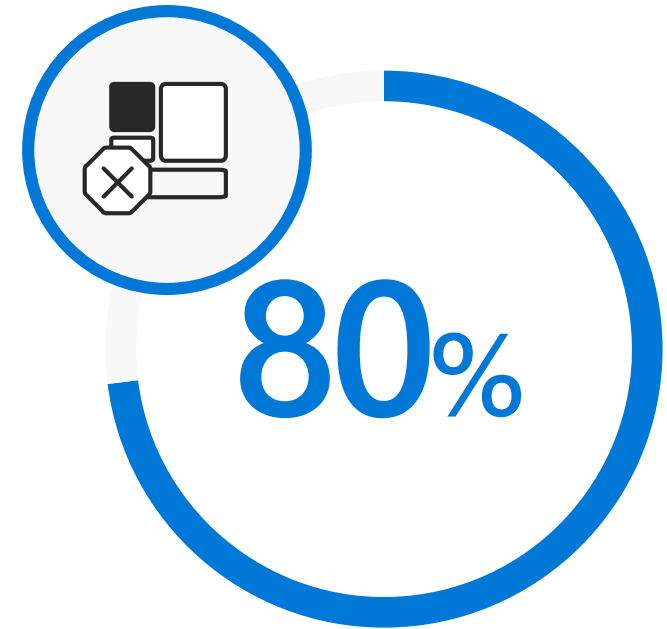
WHY **IDENTITY** IS IMPORTANT



of passwords are eventually compromised



of passwords are duplicates



of employees use non-approved apps for work

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

All organizations are at risk—every day.

167,000,000

malware
attacks

12,000,000

fraudulent sign-in
attempts

4,000

ransomware
attacks

96%

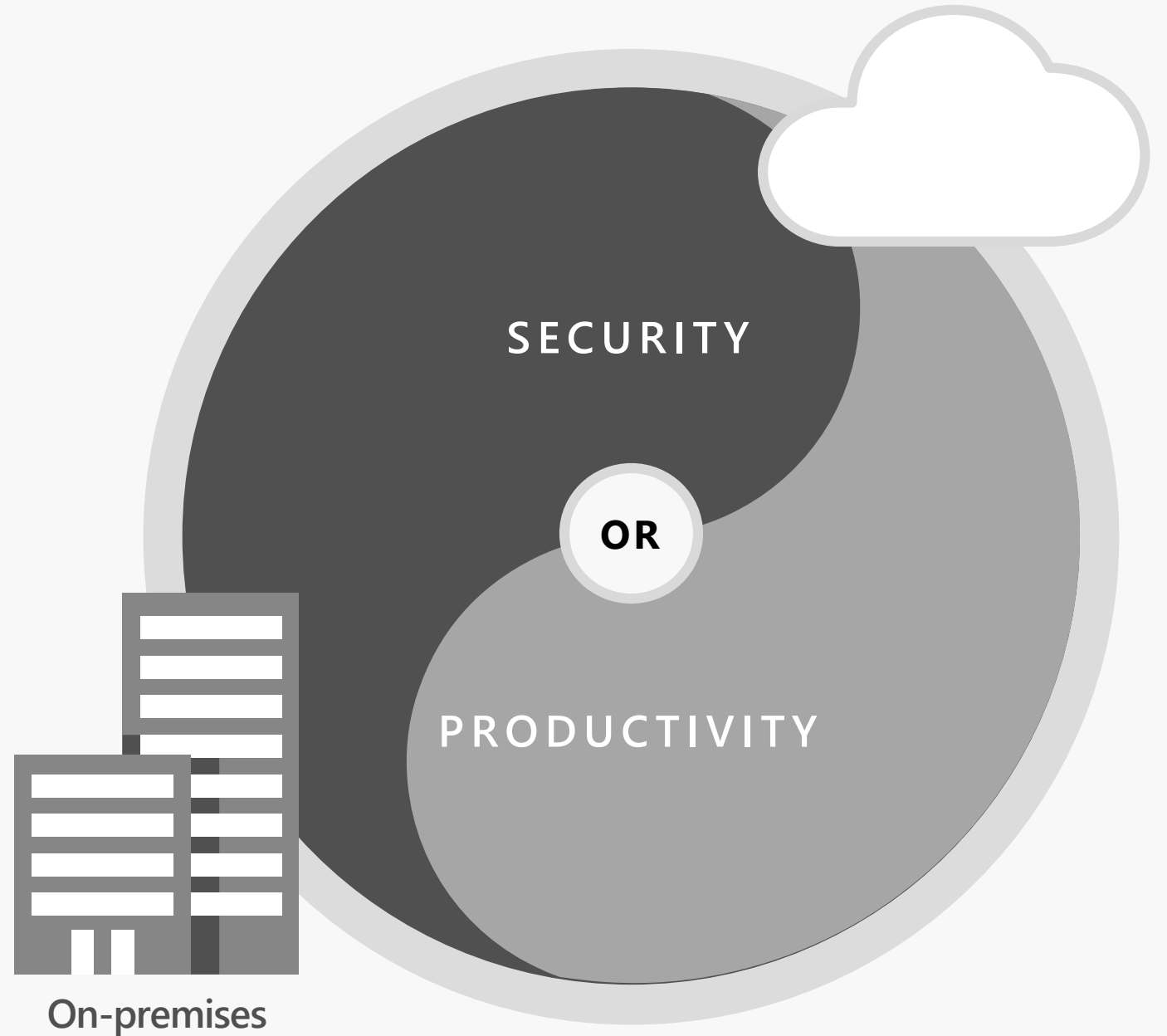
of malware is
polymorphic

Every. Single. Day.

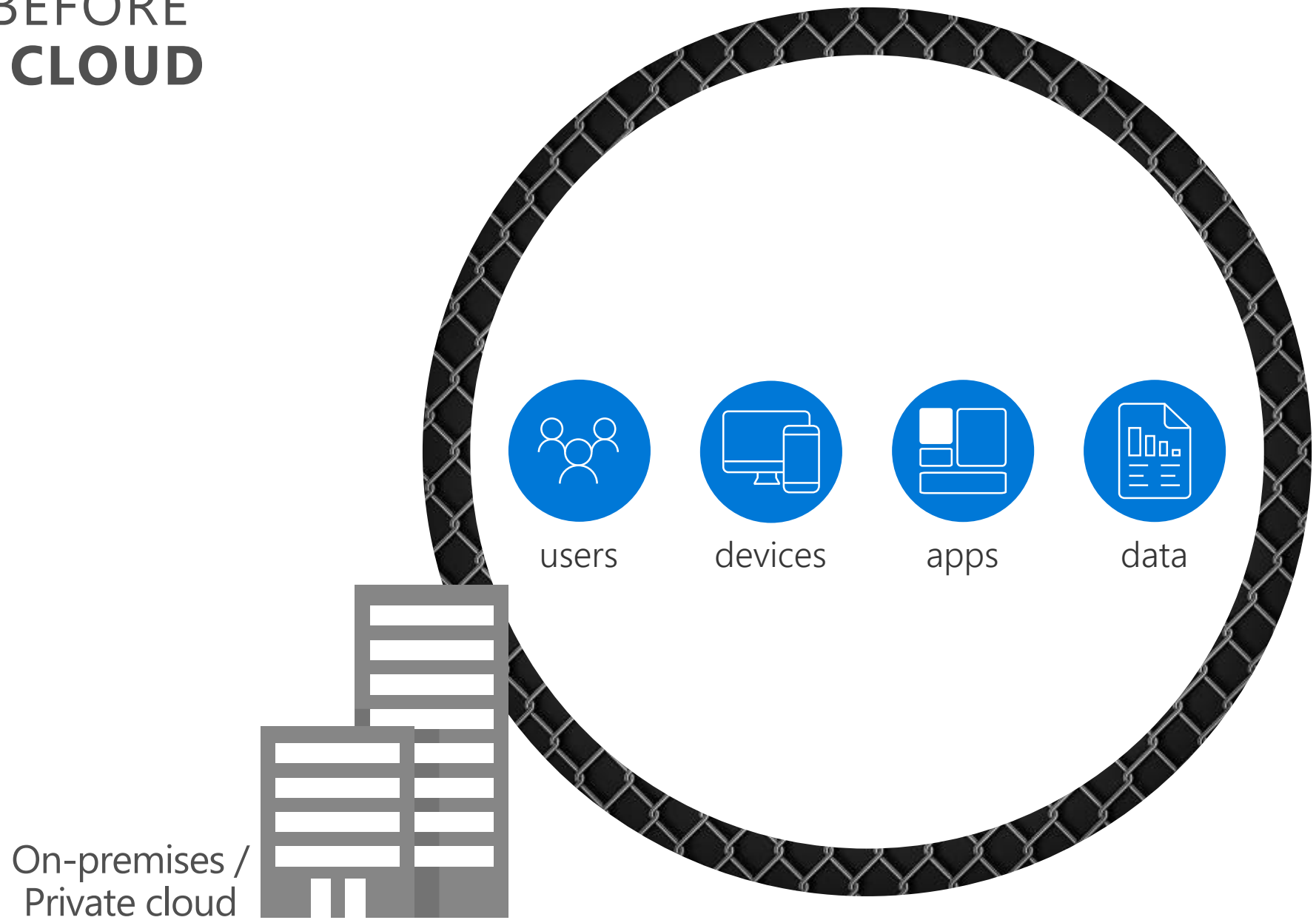


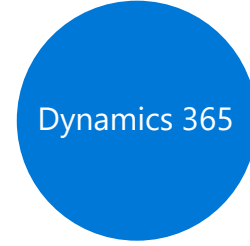
THE PROBLEM:

HOW DO WE ENABLE
PRODUCTIVITY WITHOUT
COMPROMISING SECURITY?

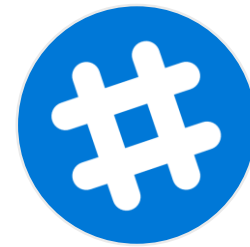


THE WORLD BEFORE **MOBILITY & CLOUD**





CLOUD APPS & SAAS SERVICES



On-premises /
Private cloud



Office 365

Dynamics 365

salesforce

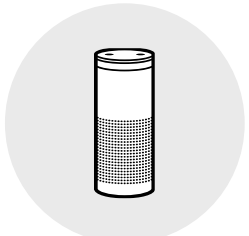
now



#

MOBILE AND PERSONAL DEVICES

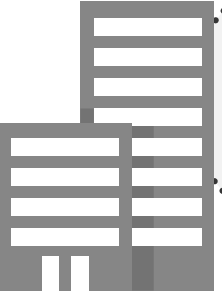
☐



W



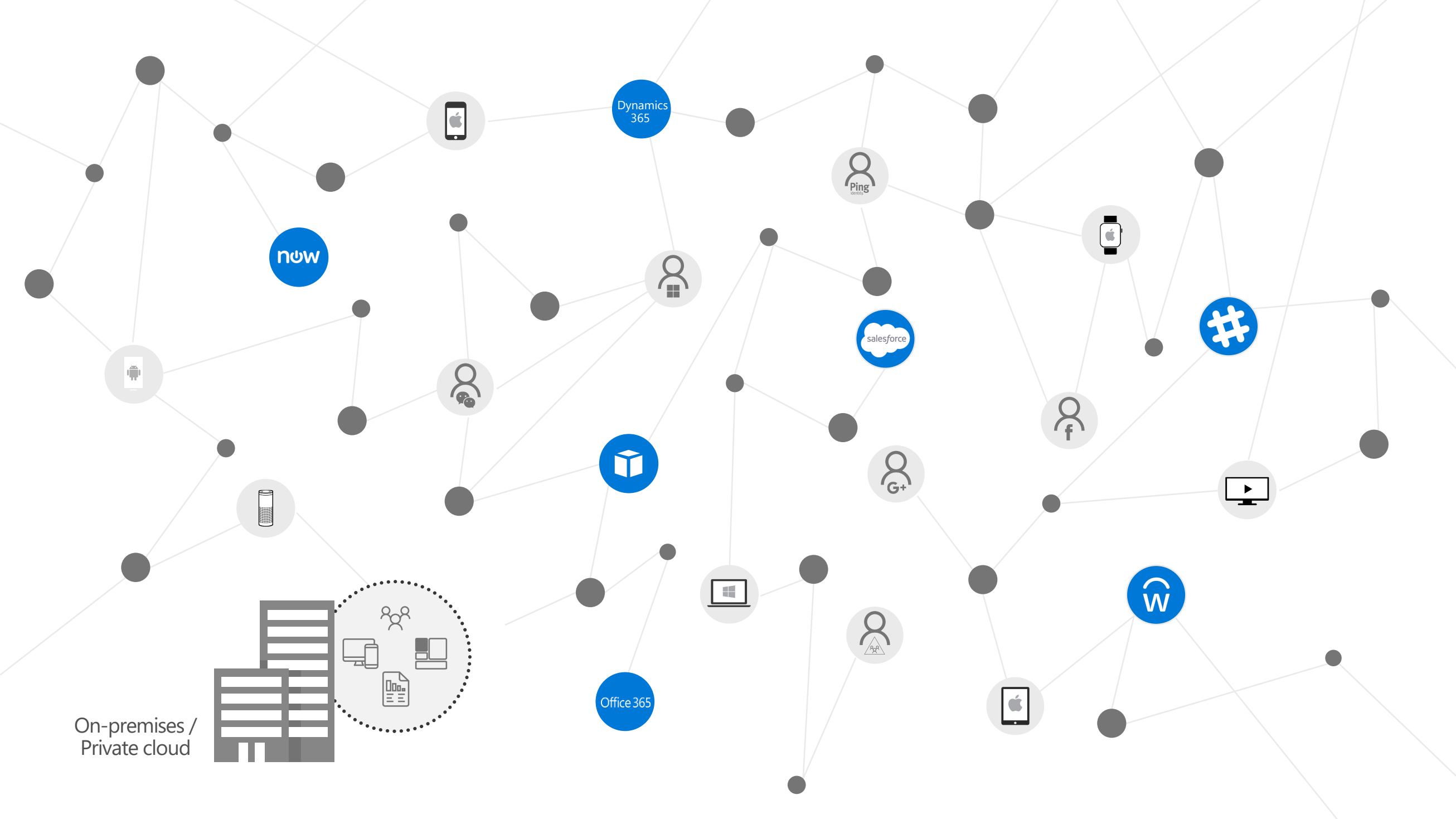
On-premises / Private cloud



ORGANIZATION & SOCIAL IDENTITIES

On-premises /
Private cloud





Dynamics 365

NOW

Ping

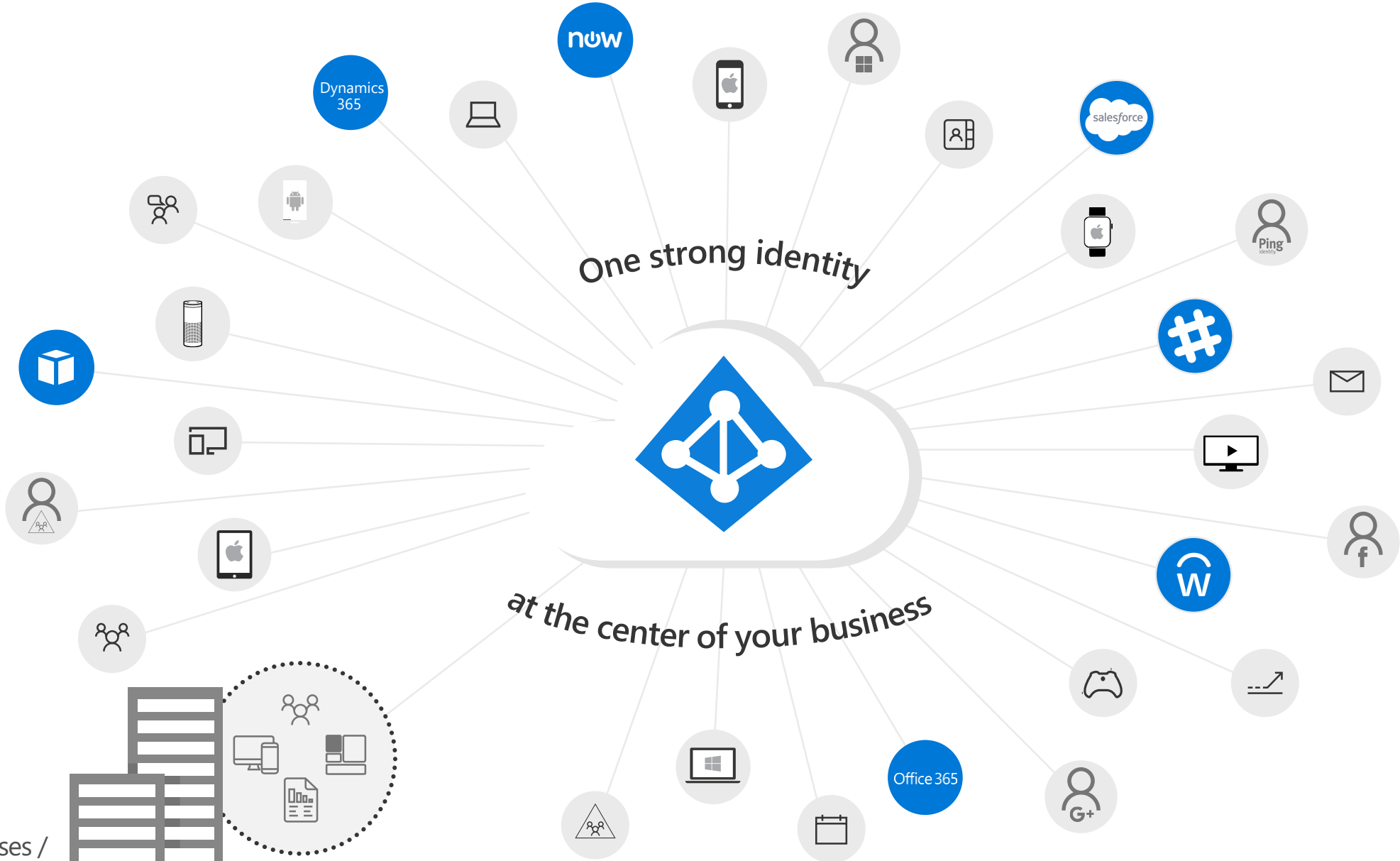
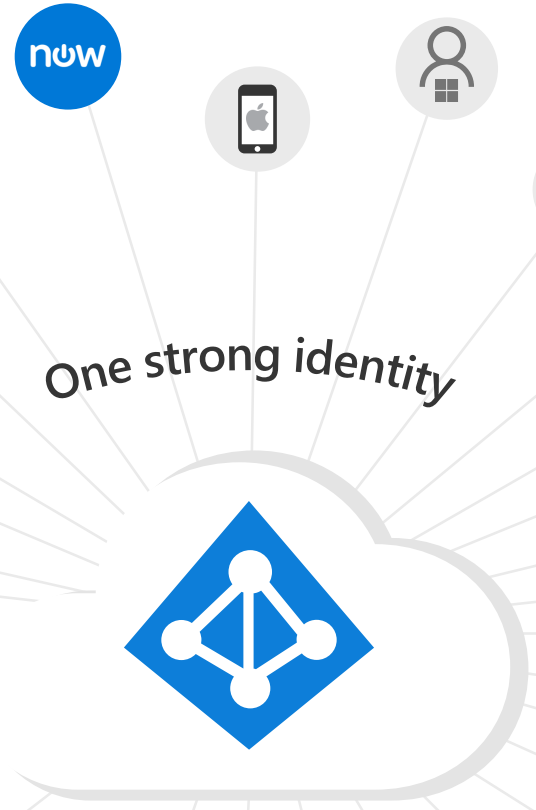
salesforce

Office 365

On-premises / Private cloud

One strong identity

at the center of your business



On-premises / Private cloud



IDENTITY & ACCESS MANAGEMENT

Prove users are authorized and secure before granting access to apps and data



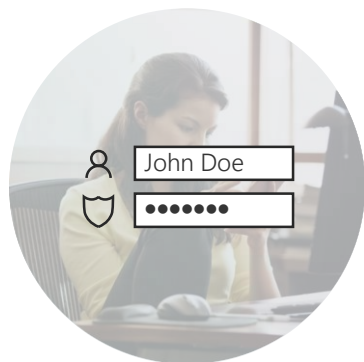
Protect at the
front door



Simplify access to
devices and apps



Safeguard customer
credentials



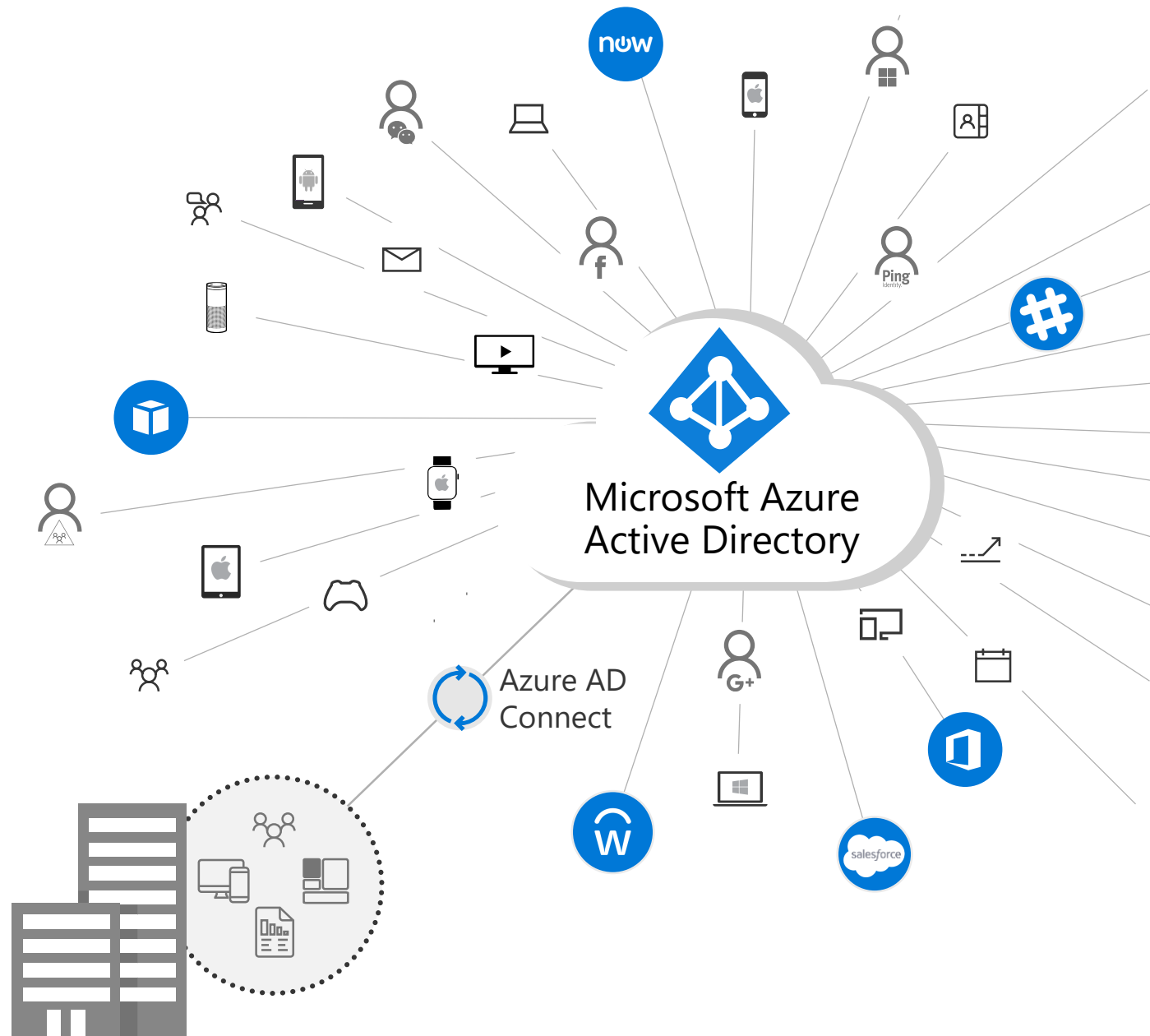
I want to provide my employees access to every app from any location and any device

Hybrid made easy

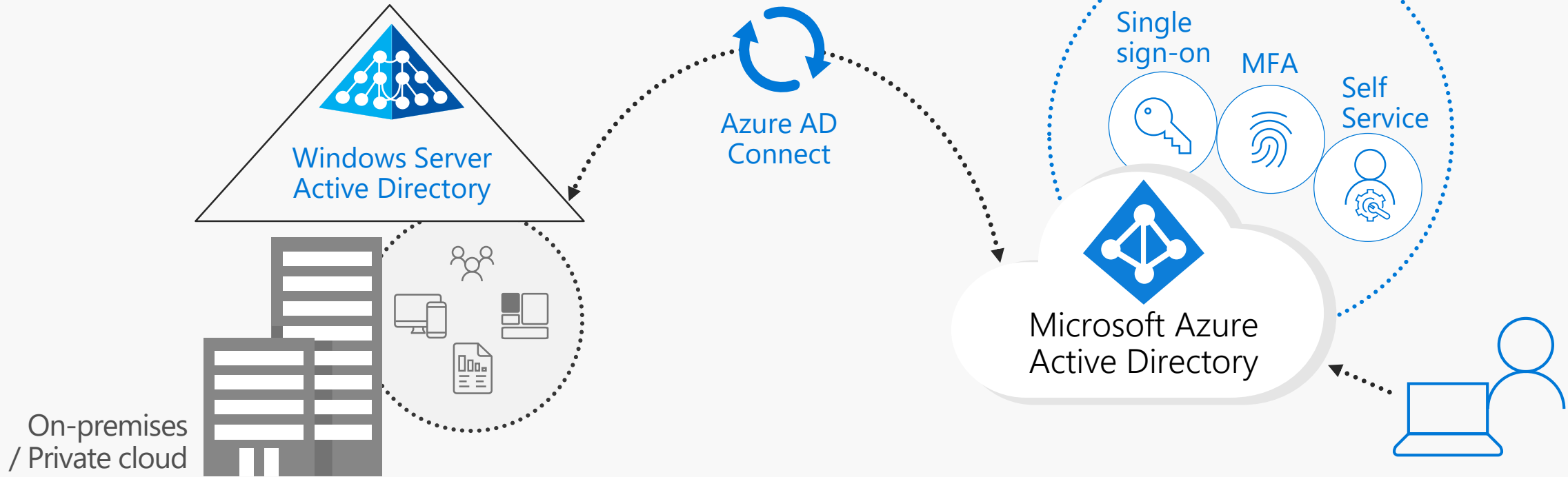
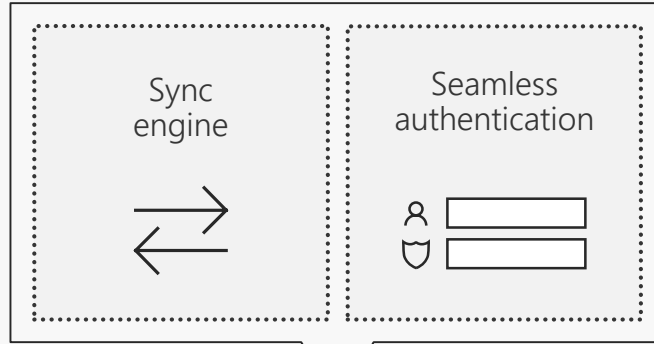
1 Identity

Thousands of apps

On-premises /
Private cloud



1 Identity



Identity and access management

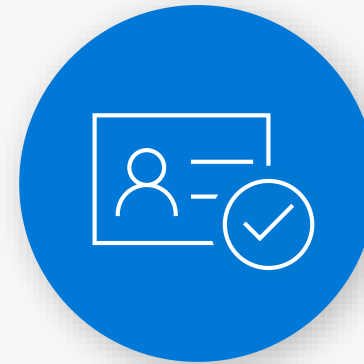
Secure identities to reach zero trust



Secure authentication



Conditional access



Identity protection

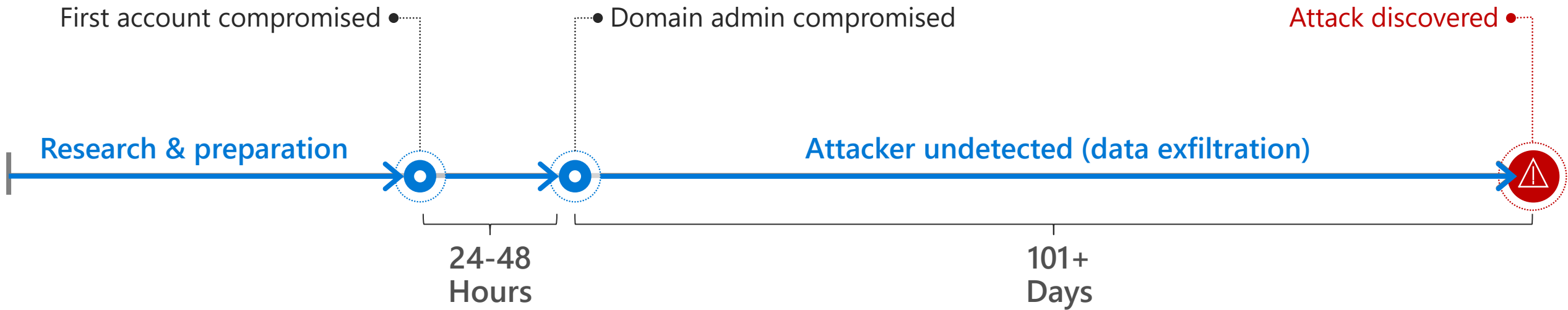


Better Insights



Identity protection

Typical advanced attack timeline & observations



| Attack sophistication | Target Active Directory (AD) & identities | Attacks not detected. Assume breach | Response and recovery |
|--|---|---|---|
| <ul style="list-style-type: none"> • Attack operators exploit any weakness • Target information on any device or service • Attacks get automated and are industrialized | <ul style="list-style-type: none"> • Active Directory controls access to business assets • Attackers commonly target AD and IT Admins | <ul style="list-style-type: none"> • Time to detect an attack is very short as attacks can occur out of nowhere and might be automated • You may be under attack (or compromised) | <ul style="list-style-type: none"> • Response requires advanced expertise and tools • Expensive and challenging to successfully recover |

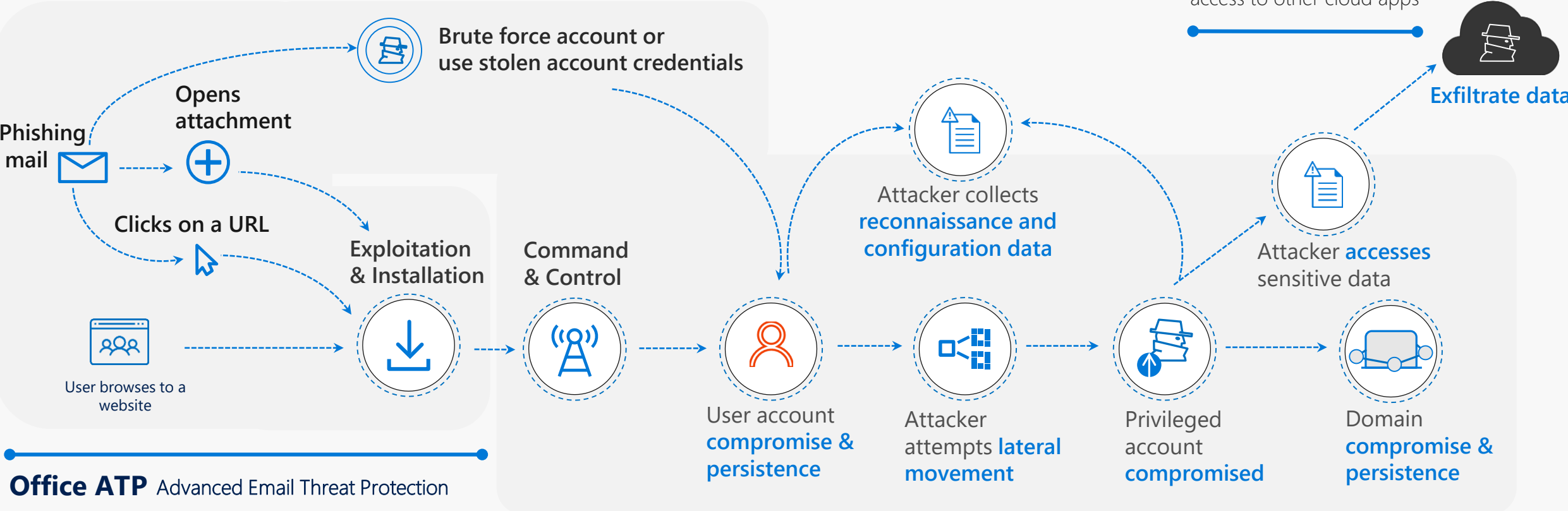
Attacker kill chains

Azure AD Identity Protection

Identity protection & conditional access

Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



Office ATP Advanced Email Threat Protection

Azure AD Privileged Identity Management

Privileged Access Management

Azure ATP Identity forensics

Applying intelligence for unified identity investigation across on-premises and cloud activities

Microsoft
Cloud App
Security

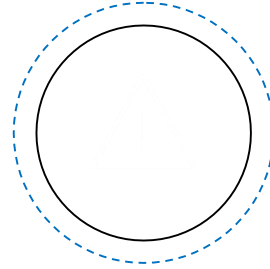
Azure
ATP



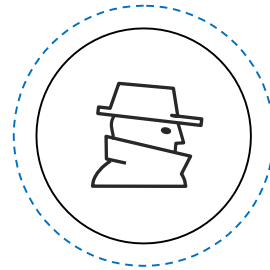
Azure AD
Identity
Protection



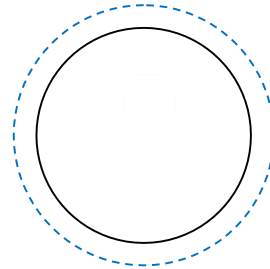
Identify attacks advanced persistent threads



Abnormal behavior

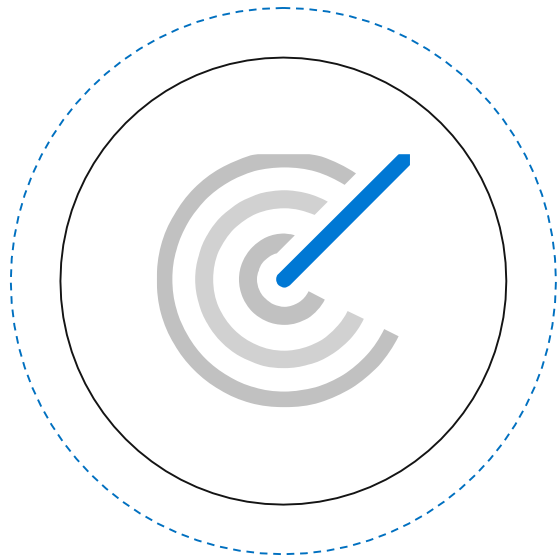


Malicious attacks

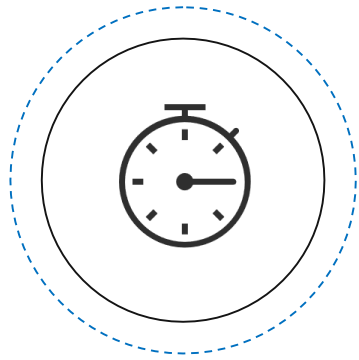


Security issues and risks

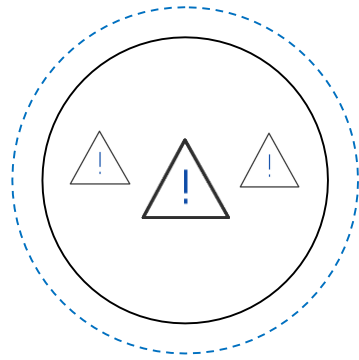
Continuous Detections



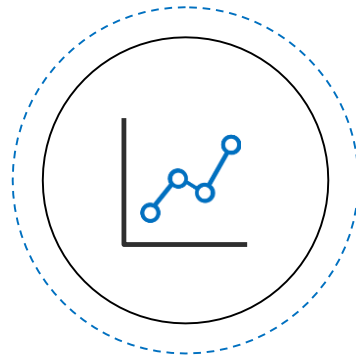
- ▲ Users with **leaked credentials**
- ▲ Sign-ins from **anonymous IP addresses**
- ▲ **Impossible travel** to atypical locations
- ▲ Sign-ins from **infected devices**
- ▲ Abnormal **resource access**
- ▲ Sign-ins from IP addresses with **suspicious activity**
- ▲ Sign-ins from **unfamiliar locations**
- ▲ Abnormal **login hours**
- ▲ Abnormal **principal modification**
- + New risk alerts are added as **new threats** emerge



Real-time



Reduce false positives



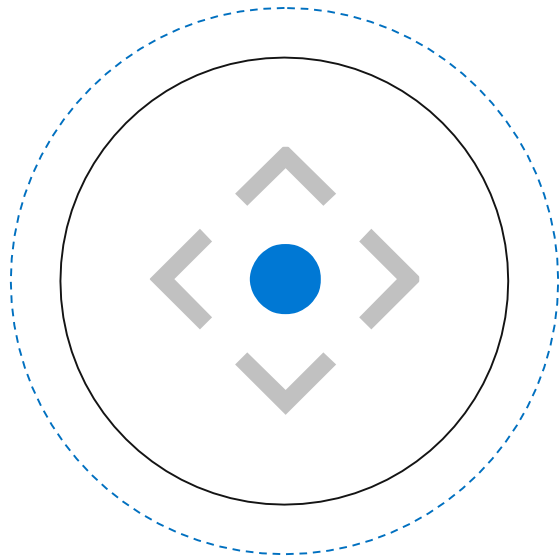
Provide post-breach forensics



Report efficiently

Proactive Protections

Act based on insights



Monitor every user sign-in and session for risk



Define policy-based access controls

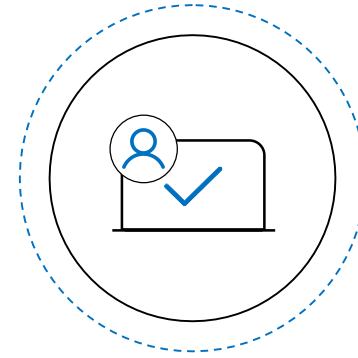
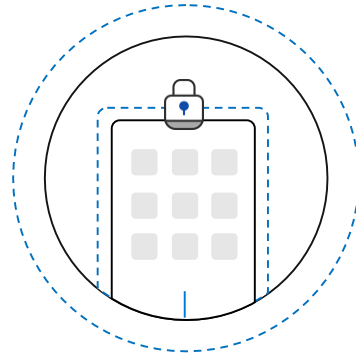
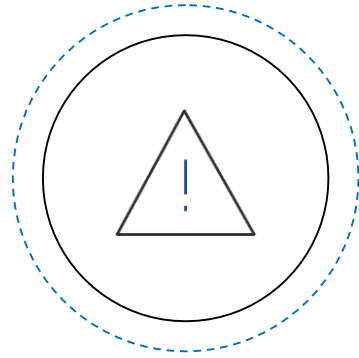


Automatically **reset passwords, disable the user** and **enable MFA** to reduce risk



Prevent identity attacks before they succeed

Automation to address the broad attack surface



Machine Learning that makes your security smarter
and more focused when it comes to
solving advanced persistent threats

Security - Overview

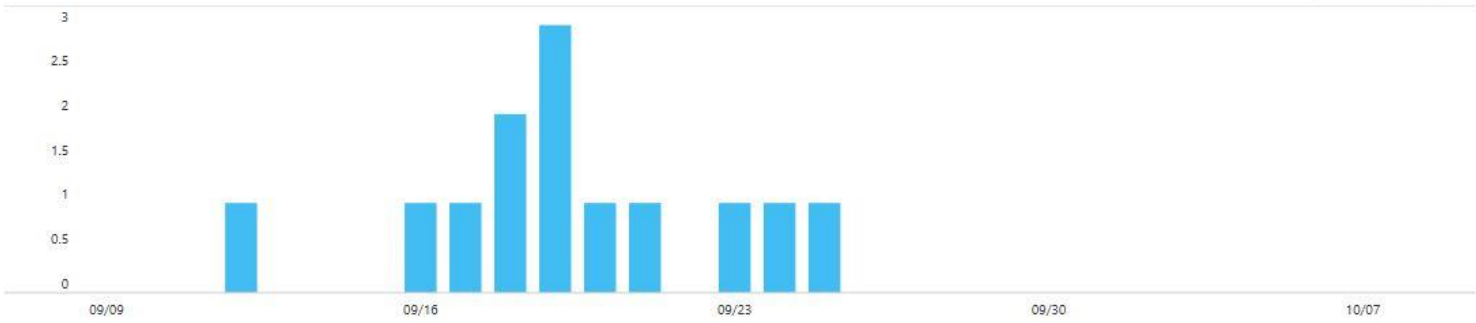
- Search (Ctrl+/)
- Overview
- Investigate
 - Risky users
 - Risky sign-ins
- Protect
 - Identity Secure Score (Preview)
 - User risk policy
 - Sign-in risk policy
 - Alerts
 - Weekly digest
- Manage
 - Named locations
 - Conditional access
 - Authentication methods
 - MFA Server
 - MFA registration policy
- Troubleshooting + Support
 - Troubleshoot
 - New support request

Learn more

Date range = 30 days

New risky users detected

User risk level = All



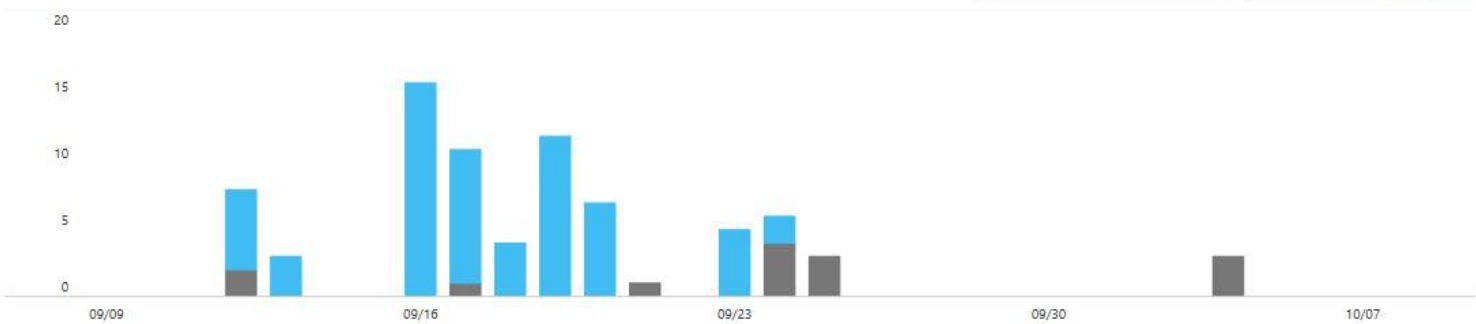
Count
13

Configure user risk policies >

New risky sign-ins detected

Sign-in risk type = Real-time

Sign-in risk level = Medium



Count
79 | **65** | **14**
Unprotected | Protected

Configure sign-in risk policies >

High risk users
4 users
High risk users detected. Investigate users and reset passwords.

Medium risk users
3 users
Medium risk users detected. Investigate users and reset passwords.

Identity Secure Score (Preview) Load error
Monitor and improve your identity security posture.

Microsoft Azure | Search resources, services, and docs | admin@IgniteAATP.c... | IGNITE ATP DEMO

Home > Ignite ATP Demo > Security - Risky users

Security - Risky users

Learn more
Columns
Refresh
Download
Select all
Dismiss user risk

Name:
 Username:
 Risk state:
 Risk level:
 Type:
 Status:

Show dates as:

| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|-------------------|---------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Dana Kaufman | dkaufman@igniteAATP.com | At risk | Medium | - | 10/4/2018 11:23:32 PM | Member | Active |
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| Jeff Leatherman | JeffV@IgniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |
| Admin | admin@igniteAATP.com | At risk | Medium | - | 9/23/2018 5:16:25 PM | Member | Active |
| Esperanza Craft | ecraft@igniteaatpdemo.onmicr... | At risk | Low | - | 9/19/2018 7:09:34 PM | Member | Active |
| Joy Chik | joyc@IgniteAATPDemo.onmicr... | At risk | High | - | 9/19/2018 5:17:31 PM | Member | Active |
| Chancey Mays | CMays@IgniteAATPDemo.onm... | At risk | Medium | - | 9/18/2018 9:35:40 PM | Member | Active |

Details

Microsoft Azure portal interface showing the 'Security - Risky users' page. The page displays a list of users with their risk states and levels. A search bar and filter options are visible at the top. The table below lists the users and their associated risk information.

| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|-------------------|---------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Dana Kaufman | dkaufman@igniteAATP.com | At risk | Medium | - | 10/4/2018 11:23:32 PM | Member | Active |
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| Jeff Leatherman | JeffV@igniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |
| Admin | admin@igniteAATP.com | At risk | Medium | - | 9/23/2018 5:16:25 PM | Member | Active |
| Esperanza Craft | ecraft@igniteaatpdemo.onmicr... | At risk | Low | - | 9/19/2018 7:09:34 PM | Member | Active |
| Joy Chik | joyc@igniteAATPDemo.onmicr... | At risk | High | - | 9/19/2018 5:17:31 PM | Member | Active |
| Chancey Mays | CMays@igniteAATPDemo.onm... | At risk | Medium | - | 9/18/2018 9:35:40 PM | Member | Active |

Microsoft Azure portal interface showing the 'Security - Risky users' page. The page displays a list of users with their risk levels and states. A dropdown menu for 'Risk level' is open, showing options for High, Medium, and Low. The 'Risk level' dropdown is currently set to 'High'.

Search resources, services, and docs

admin@IgniteAATP.c...
IGNITE ATP DEMO

Home > Ignite ATP Demo > Security - Risky users

Security - Risky users

Search (Ctrl+/)

Learn more Columns Refresh Download Select all Dismiss user risk

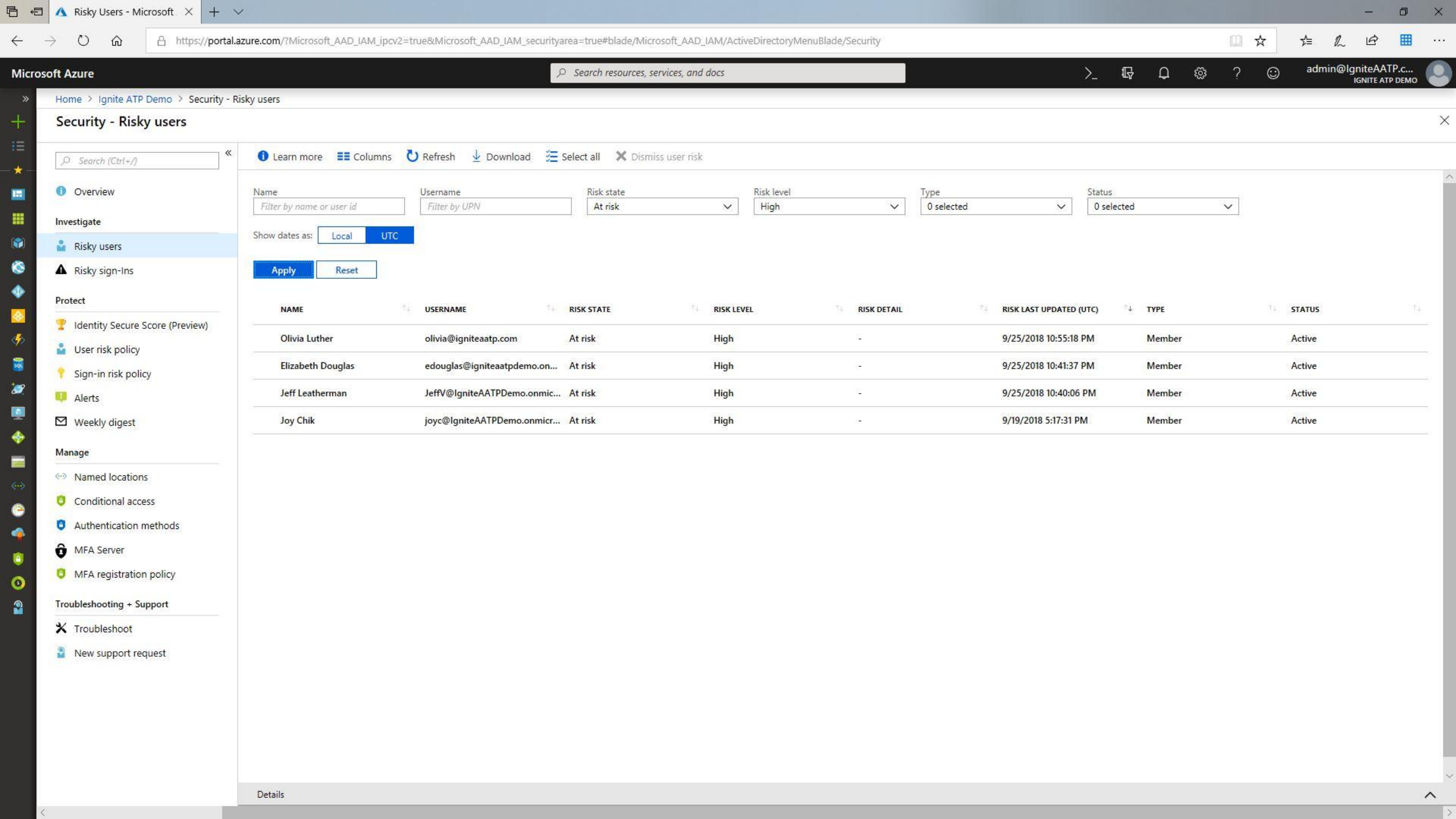
Name: Filter by name or user id Username: Filter by UPN Risk state: At risk Risk level: High Type: 0 selected Status: 0 selected

Show dates as: Local UTC

Apply Reset

| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|-------------------|---------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Dana Kaufman | dkaufman@igniteaatp.com | At risk | Medium | - | 10/4/2018 11:23:32 PM | Member | Active |
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| Jeff Leatherman | JeffV@IgniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |
| Admin | admin@igniteaatp.com | At risk | Medium | - | 9/23/2018 5:16:25 PM | Member | Active |
| Esperanza Craft | ecraft@igniteaatpdemo.onmicr... | At risk | Low | - | 9/19/2018 7:09:34 PM | Member | Active |
| Joy Chik | joyc@IgniteAATPDemo.onmicr... | At risk | High | - | 9/19/2018 5:17:31 PM | Member | Active |
| Chancey Mays | CMays@IgniteAATPDemo.onm... | At risk | Medium | - | 9/18/2018 9:35:40 PM | Member | Active |

Details



Security - Risky users

Search (Ctrl+/)

Learn more Columns Refresh Download Select all Dismiss user risk

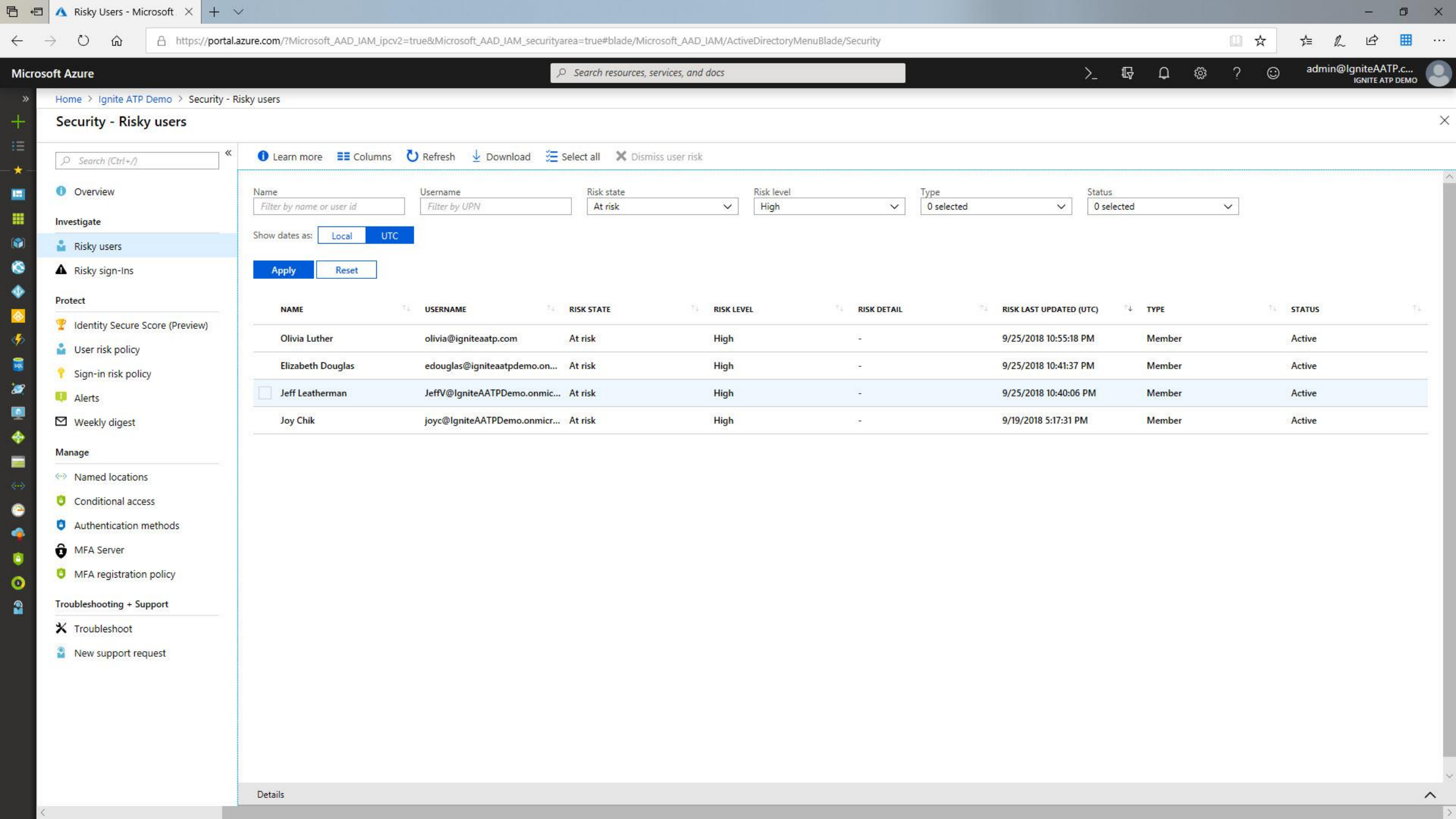
Name Username Risk state Risk level Type Status

Show dates as: Local UTC

Apply Reset

| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|-------------------|-------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| Jeff Leatherman | JeffV@igniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |
| Joy Chik | joyc@igniteAATPDemo.onmicr... | At risk | High | - | 9/19/2018 5:17:31 PM | Member | Active |

- Overview
- Investigate
 - Risky users
 - Risky sign-ins
- Protect
 - Identity Secure Score (Preview)
 - User risk policy
 - Sign-in risk policy
 - Alerts
 - Weekly digest
- Manage
 - Named locations
 - Conditional access
 - Authentication methods
 - MFA Server
 - MFA registration policy
- Troubleshooting + Support
 - Troubleshoot
 - New support request



Security - Risky users

Search (Ctrl+/)

Learn more Columns Refresh Download Select all Dismiss user risk

Name Username Risk state Risk level Type Status

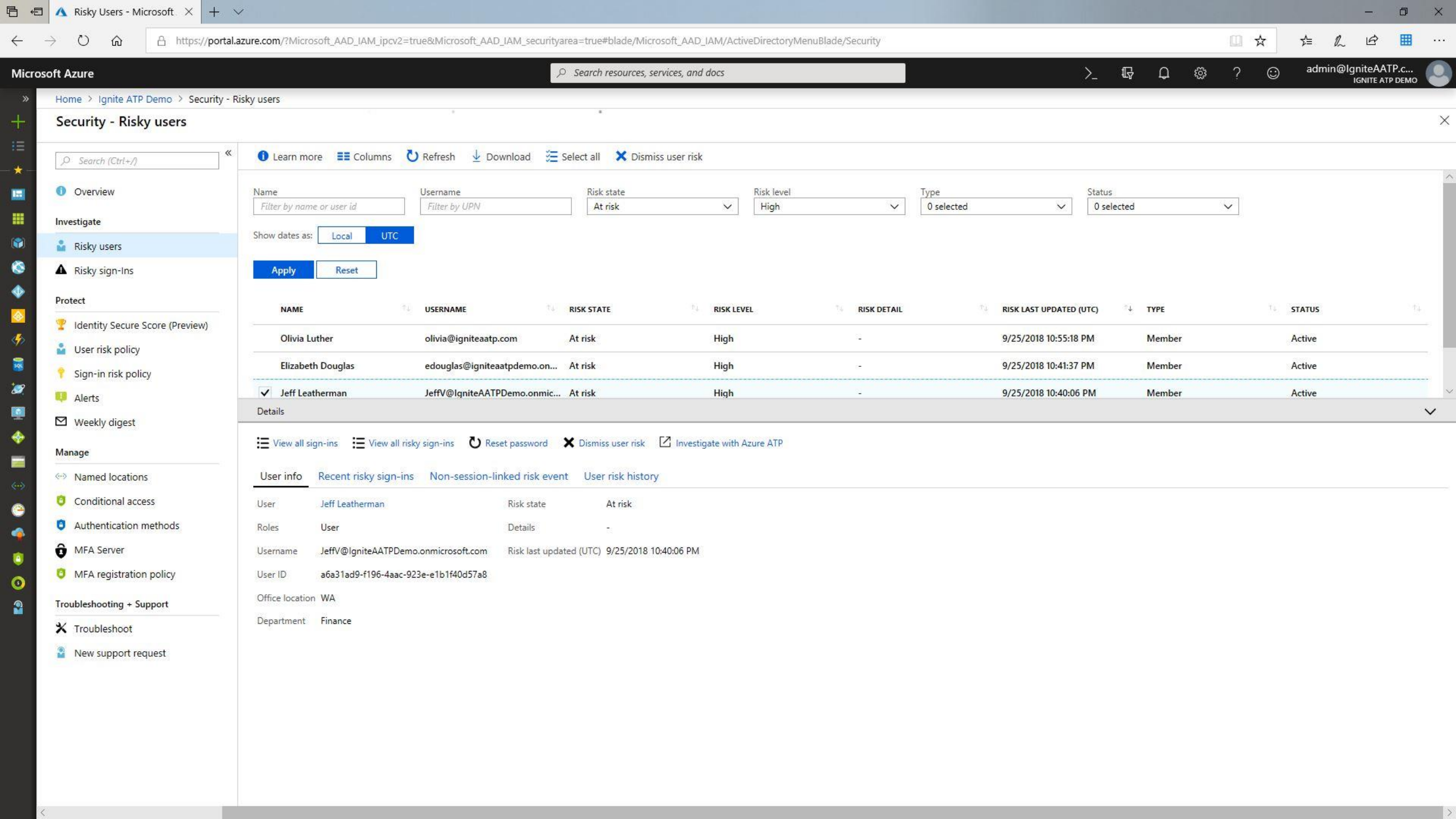
Show dates as: Local UTC

Apply Reset

| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|--|-------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| <input type="checkbox"/> Jeff Leatherman | JeffV@igniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |
| Joy Chik | joyc@igniteAATPDemo.onmicr... | At risk | High | - | 9/19/2018 5:17:31 PM | Member | Active |

- Overview
- Investigate
 - Risky users
 - Risky sign-ins
- Protect
 - Identity Secure Score (Preview)
 - User risk policy
 - Sign-in risk policy
 - Alerts
 - Weekly digest
- Manage
 - Named locations
 - Conditional access
 - Authentication methods
 - MFA Server
 - MFA registration policy
- Troubleshooting + Support
 - Troubleshoot
 - New support request

Details



Security - Risky users

Search (Ctrl+/)

Overview

Investigate

Risky users

Risky sign-ins

Protect

Identity Secure Score (Preview)

User risk policy

Sign-in risk policy

Alerts

Weekly digest

Manage

Named locations

Conditional access

Authentication methods

MFA Server

MFA registration policy

Troubleshooting + Support

Troubleshoot

New support request

Learn more Columns Refresh Download Select all Dismiss user risk

Name Username Risk state Risk level Type Status

Show dates as: Local UTC

Apply Reset

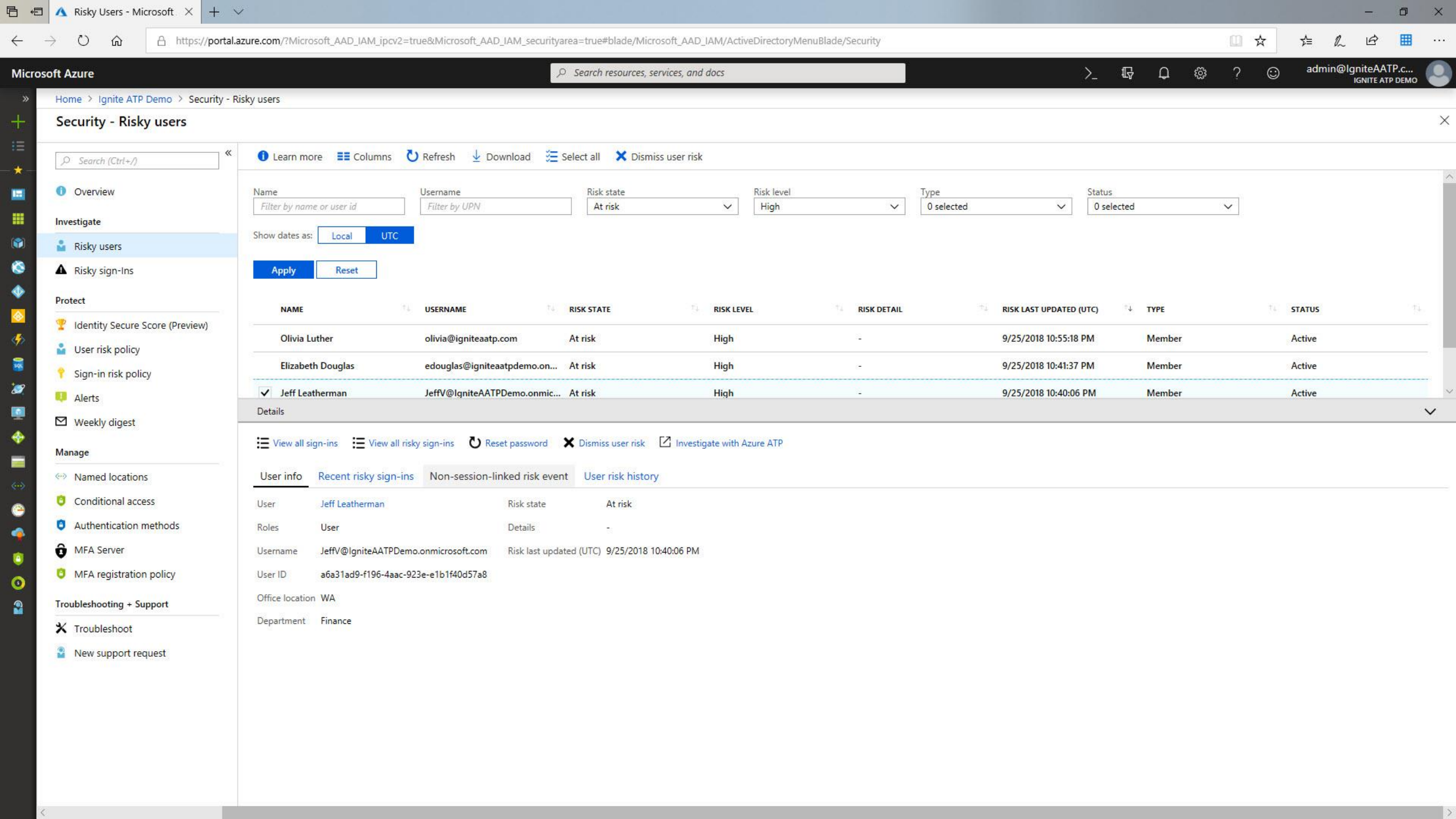
| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|---|-------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| <input checked="" type="checkbox"/> Jeff Leatherman | JeffV@igniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |

Details

View all sign-ins View all risky sign-ins Reset password Dismiss user risk Investigate with Azure ATP

User info Recent risky sign-ins Non-session-linked risk event User risk history

| | | | |
|-----------------|--------------------------------------|-------------------------|-----------------------|
| User | Jeff Leatherman | Risk state | At risk |
| Roles | User | Details | - |
| Username | JeffV@igniteAATPDemo.onmicrosoft.com | Risk last updated (UTC) | 9/25/2018 10:40:06 PM |
| User ID | a6a31ad9-f196-4aac-923e-e1b1f40d57a8 | | |
| Office location | WA | | |
| Department | Finance | | |



Security - Risky users

Search (Ctrl+/)

- Overview
- Investigate
 - Risky users
 - Risky sign-ins
- Protect
 - Identity Secure Score (Preview)
 - User risk policy
 - Sign-in risk policy
 - Alerts
 - Weekly digest
- Manage
 - Named locations
 - Conditional access
 - Authentication methods
 - MFA Server
 - MFA registration policy
 - Troubleshooting + Support
 - Troubleshoot
 - New support request

[Learn more](#)
[Columns](#)
[Refresh](#)
[Download](#)
[Select all](#)
[Dismiss user risk](#)

Name:
 Username:
 Risk state:
 Risk level:
 Type:
 Status:

Show dates as:


| NAME | USERNAME | RISK STATE | RISK LEVEL | RISK DETAIL | RISK LAST UPDATED (UTC) | TYPE | STATUS |
|---|-------------------------------|------------|------------|-------------|-------------------------|--------|--------|
| Olivia Luther | olivia@igniteaatp.com | At risk | High | - | 9/25/2018 10:55:18 PM | Member | Active |
| Elizabeth Douglas | edouglas@igniteaatpdemo.on... | At risk | High | - | 9/25/2018 10:41:37 PM | Member | Active |
| <input checked="" type="checkbox"/> Jeff Leatherman | JeffV@igniteAATPDemo.onmic... | At risk | High | - | 9/25/2018 10:40:06 PM | Member | Active |

Details

[View all sign-ins](#)
[View all risky sign-ins](#)
[Reset password](#)
[Dismiss user risk](#)
[Investigate with Azure ATP](#)

[User info](#)
[Recent risky sign-ins](#)
[Non-session-linked risk event](#)
[User risk history](#)

| | | | |
|-----------------|--------------------------------------|-------------------------|-----------------------|
| User | Jeff Leatherman | Risk state | At risk |
| Roles | User | Details | - |
| Username | JeffV@igniteAATPDemo.onmicrosoft.com | Risk last updated (UTC) | 9/25/2018 10:40:06 PM |
| User ID | a6a31ad9-f196-4aac-923e-e1b1f40d57a8 | | |
| Office location | WA | | |
| Department | Finance | | |



Jeff Leatherman

Financial Accounting Manager
Finance

User threat

Investigation priority Alerts
6 open alerts

▲ 83

Risk score
▲ High

Basic information

Email
JeffV@IgniteAATPDemo.onmicrosoft.co

Phone
[1-425-93-MSPHONE](tel:1-425-93-MSPHONE)

Manager
[Roderick Brooks](#)

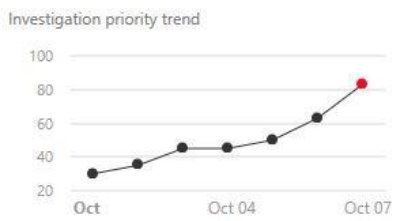
Last seen
Sep 25, 2018

Extended information

Overview | Threat analysis | Additional data | Lateral movement paths

Investigation priority

▲ **83** + 20 since yesterday
Higher than 93% of other users



- Top 90 percentile investigation priority
- Investigation priority

Summary

4 devices

2 resources

5 accounts

3 locations

| Latest | Latest | Latest | Common |
|---------------------------------|---------------------------------------|--|-----------------------------|
| RDPsrv 13 days ago | FinanceSrv53 13 days ago | jeffv@igniteatpdemo.onmic 13 days ago | United Kingdom 57% usage |
| Common Jeff-DSK 62% usage | Common SharePoint-SRV 60% usage | Common jeffv@igniteatpdemo.onmic 56% usage | United States 28% usage |
| RDPsrv 28% usage | FinanceSrv53 30% usage | jeffv@igniteatpdemo.onmic 34% usage | |

Open alerts

6 open alerts

● 1 High ● 5 Medium

- ■ **Reconnaissance using directory services queries** 19 days ago

🌐 10.42.70.95 👤 Jeff Leatherman
- ■ **Suspicious VPN connection** 20 days ago

👤 Jeff Leatherman

Top activities contributing to investigation priority

There's no relevant data to display

[View all activities](#)

Basic information

Email: JeffV@igniteAATPDemo.onmicrosoft.co

Phone: 1-425-93-MSPHONE

Manager: [Roderick Brooks](#)

Last seen: Sep 25, 2018

Extended information

- Top 90 percentile investigation priority
- Investigation priority

RDPsrv
28% usage

FinanceSrv53
30% usage

jeffv@igniteatpdemo.onmic
34% usage

United States
28% usage

Open alerts

6 open alerts

1 High 5 Medium

| | | |
|--|---|-------------|
| | Reconnaissance using directory services queries 10.42.70.95 Jeff Leatherman | 19 days ago |
| | Suspicious VPN connection Jeff Leatherman | 20 days ago |
| | Abnormal access to protected data 84.59.125.30 Jeff Leatherman | 21 days ago |
| | Suspicious inbox forwarding 185.220.101.45 Jeff Leatherman | 21 days ago |
| | Risky sign-in: Unfamiliar sign-in properties DE 185.220.102.6 Jeff Leatherman | 21 days ago |
| | Leaked credentials Jeff Leatherman | 21 days ago |

[View all alerts](#)

Top activities contributing to investigation priority

There's no relevant data to display

[View all activities](#)



Alerts > Suspicious inbox forwarding 21 DAYS AGO

Dismiss... Resolve... [Dropdown]

MEDIUM SEVERITY [Settings]

What happened?

A suspicious inbox forwarding rule was set on a user's inbox. This may indicate that the user account is compromised, and that the mailbox is being used to exfiltrate information from your organization. The user Jeff Leatherman (jeffv@igniteatpdemo.onmicrosoft.com) created or updated an inbox forwarding rule that forwards all incoming email to the external address notarealaddress@gmx.com.

Additional risks in this user session:

- 185.220.101.45 is a Tor IP address.
- 185.220.101.45 was used for the first time in 15 days in your organization.
- Microsoft Exchange Online was accessed from the ISP Zwiebelfreunde e.V. for the first time in 14 days.
- ISP Zwiebelfreunde e.V. was used for the first time in 15 days by this user.

Recommendations

Investigate

- Make sure the user is familiar with this activity
- If this alert represent a risky situation - Choose a relevant governance action and [Resolve this alert](#)
- Consider adding an [Access policy](#) to restrict access from this location
- If this was a false positive - [dismiss this alert and send us feedback](#)

Get insights

User | IP address | Device | App



Jeff Leatherman
Financial Accounting Manager
Finance

OPEN ALERTS

6

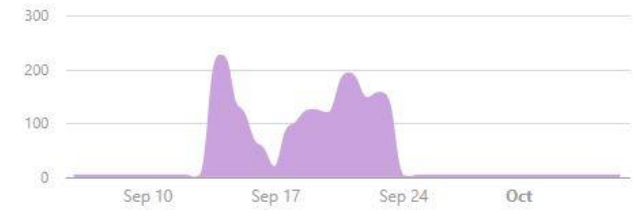
ACTIVITIES

1.3K

CONNECTED FROM (30 DAYS)


3 countries | 11 ISPs | 25 IP addresses

USER ACTIVITIES (30 DAYS) [See all](#)



FREQUENT LOCATIONS





Jeff Leatherman
 Financial Accounting Manager
 Finance

User threat

Investigation priority ▲ 83 Alerts: 6 open alerts

Risk score ▲ High

Basic information

Email: JeffV@IgniteAATPDemo.onmicrosoft.co

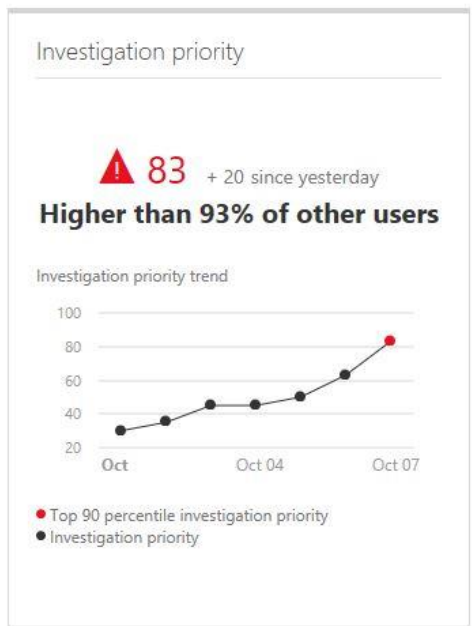
Phone: 1-425-93-MSPHONE

Manager: [Roderick Brooks](#)

Last seen: Sep 25, 2018

Extended information

Overview Threat analysis Additional data Lateral movement paths



Summary

4 devices

2 resources

5 accounts

3 locations

Latest

- RDPsrv
13 days ago

Common

- Jeff-DSK
62% usage
- RDPsrv
28% usage

Latest

- FinanceSrv53
13 days ago

Common

- SharePoint-SRV
60% usage
- FinanceSrv53
30% usage

Latest

- jeffv@igniteatpdemo.onmic
13 days ago

Common

- jeffv@igniteatpdemo.onmic
56% usage
- jeffv@igniteatpdemo.onmic
34% usage

Common

- United Kingdom
57% usage
- United States
28% usage

Open alerts

6 open alerts

● 1 High ● 5 Medium

■ ■ ■ **Reconnaissance using directory services queries** 19 days ago

10.42.70.95 Jeff Leatherman

■ ■ ■ **Suspicious VPN connection** 20 days ago

Jeff Leatherman

Top activities contributing to investigation priority

There's no relevant data to display

View all activities

Azure ATP

Basic information

Email: JeffV@igniteAATPDemo.onmicrosoft.co

Phone: 1-425-93-MSPHONE

Manager: [Roderick Brooks](#)

Last seen: Sep 25, 2018

Extended information

• Top 90 percentile investigation priority
• Investigation priority

RDPsrv 28% usage

FinanceSrv53 30% usage

jeffv@igniteatpdemo.onmic 34% usage

United States 28% usage

Open alerts

6 open alerts

1 High 5 Medium

- Reconnaissance using directory services queries** 19 days ago
10.42.70.95 Jeff Leatherman
- Suspicious VPN connection** 20 days ago
Jeff Leatherman
- Abnormal access to protected data** 21 days ago
84.59.125.30 Jeff Leatherman
- Suspicious inbox forwarding** 21 days ago
185.220.101.45 Jeff Leatherman
- Risky sign-in: Unfamiliar sign-in properties** 21 days ago
DE 185.220.102.6 Jeff Leatherman
- Leaked credentials** 21 days ago
Jeff Leatherman

[View all alerts](#)

Top activities contributing to investigation priority

There's no relevant data to display

[View all activities](#)

Alerts > Suspicious VPN connection 20 DAYS AGO

Dismiss... Resolve... v

MEDIUM SEVERITY

What happened?

Jeff Leatherman connected to a suspicious VPN using LanovoX470 from Manila, Philippines.

Important info:

- User Jeff Leatherman does not usually connect from Manila, Philippines. The user usually connects from London, UK.
- LanovoX470 isn't a computer that Jeff Leatherman uses on a regular basis.

Recommendations

Investigate

- Make sure Jeff Leatherman is familiar with this activity
- If this alert represent a risky situation - Choose a relevant governance action and [Resolve this alert](#)
- Consider adding a [conditional access policy](#) to restrict access from this location
- If this was a false positive - [dismiss this alert and send us feedback](#)

Get insights

User IP address Device App



Jeff Leatherman
Financial Accounting Manager
Finance

OPEN ALERTS

6

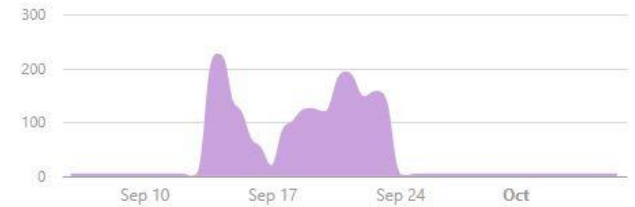
ACTIVITIES

1.3K

CONNECTED FROM (30 DAYS)


3 countries 11 ISPs 25 IP addresses

USER ACTIVITIES (30 DAYS) [See all](#)



FREQUENT LOCATIONS





Jeff Leatherman

Financial Accounting Manager
Finance

User threat

Investigation priority ▲ 83 Alerts 6 open alerts

Risk score ▲ High

Basic information

Email: JeffV@IgniteAATPDemo.onmicrosoft.co

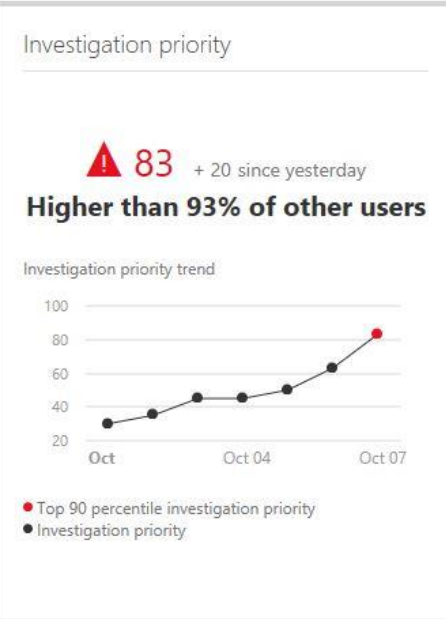
Phone: [1-425-93-MSPHONE](tel:1-425-93-MSPHONE)

Manager: [Roderick Brooks](#)

Last seen: Sep 25, 2018

Extended information

Overview | Threat analysis | Additional data | Lateral movement paths












Summary

4 devices

2 resources

5 accounts

3 locations

| Latest | Latest | Latest | Common |
|---|---|--|---|
| <div style="border: 1px solid #ccc; padding: 5px;">  RDPsrv 13 days ago </div> | <div style="border: 1px solid #ccc; padding: 5px;">  FinanceSrv53 13 days ago </div> | <div style="border: 1px solid #ccc; padding: 5px;">  jeffv@igniteatpdemo.onmic 13 days ago </div> | <div style="border: 1px solid #ccc; padding: 5px;"> United Kingdom 57% usage </div> |
| <div style="border: 1px solid #ccc; padding: 5px;">  Jeff-DSK 62% usage </div> | <div style="border: 1px solid #ccc; padding: 5px;">  SharePoint-SRV 60% usage </div> | <div style="border: 1px solid #ccc; padding: 5px;">  jeffv@igniteatpdemo.onmic 56% usage </div> | <div style="border: 1px solid #ccc; padding: 5px;"> United States 28% usage </div> |
| <div style="border: 1px solid #ccc; padding: 5px;">  RDPsrv 28% usage </div> | <div style="border: 1px solid #ccc; padding: 5px;">  FinanceSrv53 30% usage </div> | <div style="border: 1px solid #ccc; padding: 5px;">  jeffv@igniteatpdemo.onmic 34% usage </div> | |

Open alerts

6 open alerts

● 1 High ● 5 Medium


■ ■ ■
Reconnaissance using directory services queries
19 days ago

🌐 10.42.70.95 👤 Jeff Leatherman

■ ■ ■
Suspicious VPN connection
20 days ago

👤 Jeff Leatherman

Top activities contributing to investigation priority



There's no relevant data to display

View all activities

Basic information

Email: JeffV@igniteAATPDemo.onmicrosoft.co

Phone: 1-425-93-MSPHONE

Manager: [Roderick Brooks](#)

Last seen: Sep 25, 2018

Extended information

- Top 90 percentile investigation priority
- Investigation priority

RDPsrv
28% usage

FinanceSrv53
30% usage

jeffv@igniteatpdemo.onmic
34% usage

United States
28% usage

Open alerts

6 open alerts

1 High 5 Medium

- Reconnaissance using directory services queries** (19 days ago)
10.42.70.95 Jeff Leatherman
- Suspicious VPN connection** (20 days ago)
Jeff Leatherman
- Abnormal access to protected data** (21 days ago)
84.59.125.30 Jeff Leatherman
- Suspicious inbox forwarding** (21 days ago)
185.220.101.45 Jeff Leatherman
- Risky sign-in: Unfamiliar sign-in properties** (21 days ago)
DE 185.220.102.6 Jeff Leatherman
- Leaked credentials** (21 days ago)
Jeff Leatherman

[View all alerts](#)

Top activities contributing to investigation priority

There's no relevant data to display

[View all activities](#)

Alerts > Reconnaissance using directory services queries 19 DAYS AGO

Dismiss... Resolve...

MEDIUM SEVERITY

What happened?

User, **Jeff Leatherman** working on **RDPSrv** sent suspicious SAMR queries to domain controller DC1, searching for user: **Ron Harper** and group: **HelpDesk**

Important info:

- These specific SAMR queries were not observed recently from **RDPSrv**.
- These queried entities were not observed logging into **RDPSrv**.
- The behavior of this user during the last two weeks for **RDPSrv** included 29 SAMR queries.

Recommendations

Investigate

- Make sure **Jeff Leatherman** is familiar with this activity
- If this alert represent a risky situation - Choose a relevant governance action and [Resolve this alert](#)
- Consider adding a [conditional access policy](#) to restrict access from this location
- If this was a false positive - [dismiss this alert and send us feedback](#)

Get insights

User IP address Device App



Jeff Leatherman
Financial Accounting Manager
Finance

OPEN ALERTS

6

ACTIVITIES

1.3K

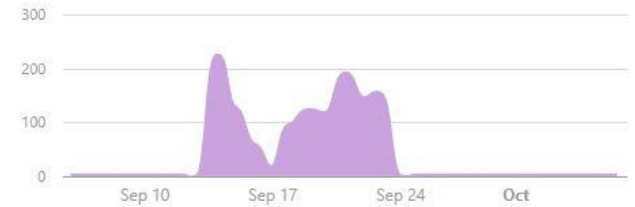
CONNECTED FROM (30 DAYS)

3 countries

11 ISPs

25 IP addresses

USER ACTIVITIES (30 DAYS) [See all](#)



FREQUENT LOCATIONS





Ron Harper

Helpdesk Engineer
IT

User threat

Investigation priority
▲ 81

Alerts
1 open alert

Risk score
No user sign-in risk

Basic information

Email
RonHD@IgniteAATPDemo.onmicrosoft.com

Phone
[1-425-93-MSPHONE](tel:1-425-93-MSPHONE)

Manager
[Elizabeth King](#)

Last seen
Sep 25, 2018

Extended information

Overview

Threat analysis

Additional data

Lateral movement paths

Investigation priority

▲ 81 + 20 since yesterday

Higher than 93% of other users

Investigation priority trend



- Top 90 percentile investigation priority
- Investigation priority

Summary

3 devices

2 resources

4 accounts

2 locations

Latest

RDPsrv
21 days ago

Latest

FinanceSrv53
21 days ago

Latest

ronhd@igniteatpdemo.onm
13 days ago

Common

FinanceSrv53
62% usage

Common

SharePoint-SRV
60% usage

Common

ronhd@igniteatpdemo.onm
56% usage

Common

United Kingdom
50% usage

Israel
50% usage

RDPsrv
28% usage

FinanceSrv53
30% usage

ronhd@igniteatpdemo.onm
34% usage

Open alerts

1 open alert

● 1 High

Identity theft using pass-the-ticket attack

19 days ago

🌐 10.42.70.95 👤 Ron Harper

[View all alerts](#)

Top activities contributing to investigation priority

There's no relevant data to display

[View all activities](#)

Alerts > Identity theft using pass-the-ticket attack 19 DAYS AGO

Dismiss... Resolve... ▾

HIGH SEVERITY

What happened?

An actor took **Ron Harper's** Kerberos ticket from **RDPsrv** and used it on **FinanceSrv53** to access **SharePoint-SRV**

Important info:

- This Kerberos ticket was first observed on 9/3/18 20:00 PM on **RDPsrv** 10.42.70.95.
- Ron Harper** was not observed accessing **SharePoint-SRV** before.
- Ron Harper** was not observed logging into **FinanceSrv53** before.

Recommendations

Investigate

- Make sure **Ron Harper** is familiar with this activity
- If this was a false positive - dismiss this alert and send us feedback
- Investigate this Machine in **Windows Defender ATP**

Activity log

1 - 1 of 1 activities

Investigate in Activity log

| Activity | User | App | IP address | Location | Device | Date |
|-----------------------------------|------------|---------------|------------|----------|--------|-------------------|
| ResourceAccess: device SharePoint | Ron Harper | Active Direct | 10.0.5.6 | — | RDPsrv | Sep 19, 2018, ... |

Get insights

User IP address Device App



Ron Harper
Helpdesk Engineer
IT

OPEN ALERTS

1

ACTIVITIES

147

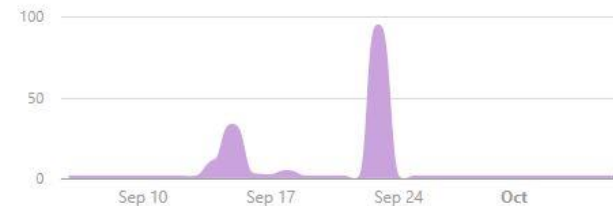
CONNECTED FROM (30 DAYS)

2 countries

5 ISPs

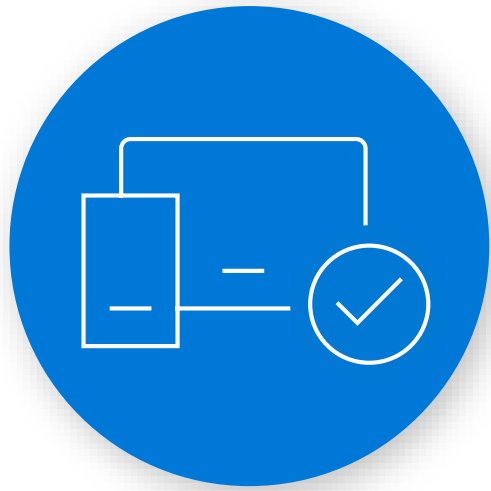
10 IP addresses

USER ACTIVITIES (30 DAYS) [See all](#)



FREQUENT LOCATIONS





Conditional access

HOW MUCH **CONTROL** DO
YOU HAVE OVER **ACCESS**?



Who is accessing? What is their role?
Is the account compromised?



Where is the user based? From where is the user signing in? Is the IP anonymous?



Which app is being accessed?
What is the business impact?

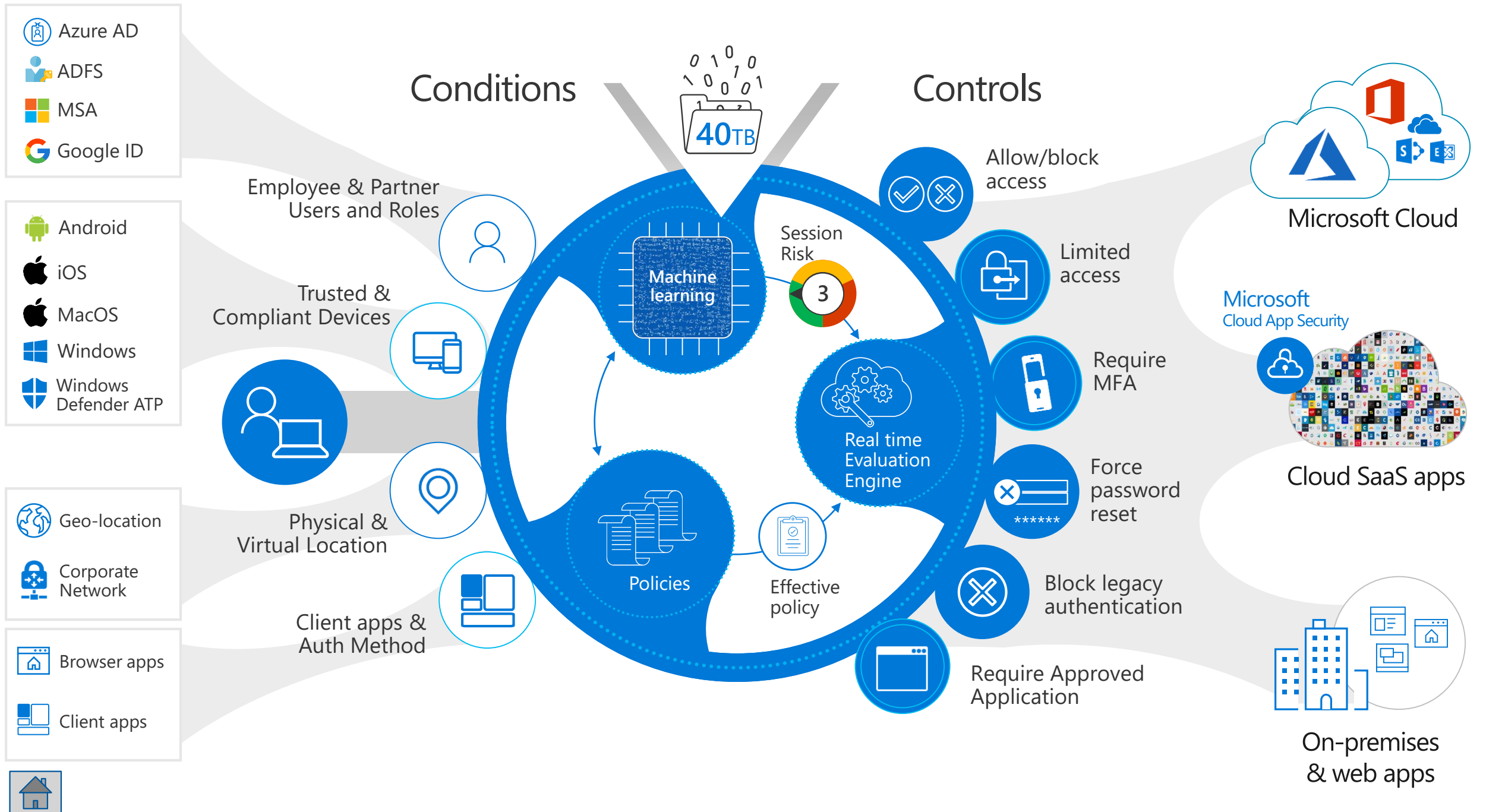


Is the device healthy? Is it managed?
Has it been in a botnet?



What data is being accessed?
Is it classified? Is it allowed off premises?





- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

Home > Adatum Corp > Conditional access - Policies

Conditional access - Policies

Azure Active Directory

- Policies
- Manage
 - Named locations
 - Custom controls (preview)
 - Terms of use
 - VPN connectivity
 - Classic policies
- Troubleshooting + Support
 - Troubleshoot
 - New support request

[+ New policy](#) [What If](#)

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

| POLICY NAME | ENABLED | |
|--|---------|-----|
| Baseline policy: Require MFA for admins (Preview) | | ... |
| SharePoint App Restriction | ✓ | ... |
| [SharePoint admin center]Block access from apps on unmanaged devices - 2018/08/31 | | ... |
| [SharePoint admin center]Use app-enforced Restrictions for browser access - 2018/08/31 | | ... |
| [SharePoint admin center]Block access from apps on unmanaged devices - 2018/09/04 | | ... |
| [SharePoint admin center]Use app-enforced Restrictions for browser access - 2018/09/04 | | ... |
| SharePoint displays Terms of Use | ✓ | ... |

- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

SharePoint App Restriction

Info Delete

* Name
SharePoint App Restriction

Assignments

Users and groups ⓘ
All users >

Cloud apps ⓘ
1 app included >

Conditions ⓘ
1 condition selected >

Access controls

Grant ⓘ
1 control selected >

Session ⓘ
Use app enforced restrictions >

Enable policy

On Off

Save



- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

SharePoint App Restriction

Info Delete

Name: SharePoint App Restriction

Assignments

- Users and groups: All users
- Cloud apps: 1 app included**
- Conditions: 1 condition selected

Access controls

- Grant: 1 control selected
- Session: Use app enforced restrictions

Enable policy: **On** Off

Cloud apps

Include Exclude

None
 All cloud apps
 Select apps

Select: Office 365 SharePoint Online

- Office 365 SharePoint Online ...

- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

SharePoint App Restriction

Info Delete

Name: SharePoint App Restriction

Assignments

- Users and groups: All users
- Cloud apps: 1 app included
- Conditions: 1 condition selected**

Access controls

- Grant: 1 control selected
- Session: Use app enforced restrictions

Enable policy: On Off

Save

Conditions

Info

- Sign-in risk: Not configured
- Device platforms: Not configured
- Locations: Not configured
- Client apps (preview): 1 included**
- Device state (preview): Not configured

Done

Client apps (preview)

Configure: Yes No

Select the client apps this policy will apply to:

- Browser
- Mobile apps and desktop clients

Advanced

Done

Microsoft Azure navigation sidebar with links to services like Dashboard, SQL databases, and Security Center.

Main configuration area for 'SharePoint App Restriction' with tabs for 'Info', 'Assignments', 'Access controls', and 'Enable policy'.

'Grant' configuration panel with radio buttons for 'Block access' and 'Grant access', and checkboxes for various security controls like 'Require multi-factor authentication'.

- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

SharePoint App Restriction

[Info](#) [Delete](#)

Name
SharePoint App Restriction

Assignments

Users and groups [Info](#) >
All users

Cloud apps [Info](#) >
1 app included

Conditions [Info](#) >
1 condition selected

Access controls

Grant [Info](#) >
1 control selected

Session [Info](#) >
Use app enforced restrictions

Enable policy

On Off

[Save](#)

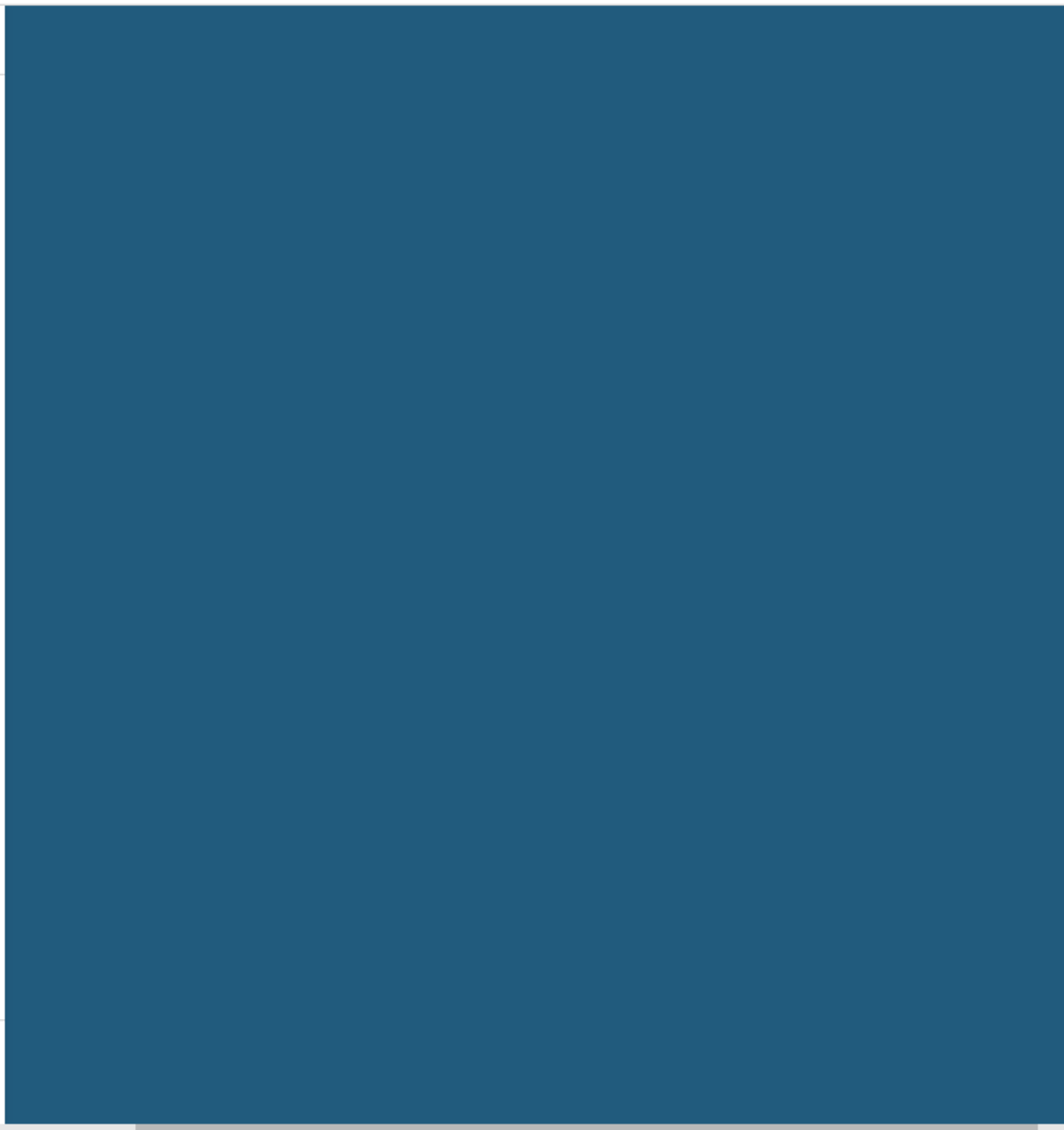
Session

Session controls enable limited experiences within a cloud app. Select the session usage requirements. [Learn more](#)

Use app enforced restrictions [Info](#)

Use Conditional Access App Control [Info](#)

[Select](#)





Adatum Corp terms of use

In order to access Adatum Corp resource, you must read the terms of use.

[Adatum Corp Terms of Use](#)



Please click Accept to confirm that you have read and understood the terms of use.

Decline

Accept

Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune. For help, contact your IT department. More info.

SM Sales and Marketing

Public group | Confidential

3 members

Search this site

+ New

Published 9/19/2018 Edit

- Home
- Conversations
- Documents
- Notebook
- Pages
- Site contents
- Recycle bin
- Edit

Documents See all

+ New Upload Sync Export to Excel All Documents


| Name | Modified | Modified By |
|-----------------------------|---------------|----------------|
| Marketing Plan.xlsx | 4 minutes ago | Beverly Spalla |
| Press release - draft.docx | 6 minutes ago | Venia Huang |
| Sales outlook for 2019.docx | 8 minutes ago | Beverly Spalla |


Quick links

- Learn about a team site
- Learn how to add a page

Activity

Sales and Marketing


 View and share files
 Collaborate on content with your


 Get organized
 Use lists to keep team activities

ⓘ Your organization doesn't allow you to download, print, or sync using this device. To use these actions, use a device that's joined to a domain or marked compliant by Intune. For help, contact your IT department.

SM Sales and Marketing

Public group | Confidential

Search this site

- Home
- Conversations
- Documents
- Notebook
- Pages
- Site contents
- Recycle bin
- Edit





+ New ▾

Documents

See all

Quick links

+ New ▾ ↑ Upload ▾ ↻ Sync 📄 Export to Excel ☰ All Documents ▾

|  Name ▾ | Modified ▾ | Modified By ▾ |
|---|---------------|----------------|
|  [!] Marketing Plan.xlsx | 4 minutes ago | Beverly Spalla |
|  [!] Press release - draft.docx | 6 minutes ago | Venia Huang |
|  Sales outlook for 2019.docx | 8 minutes ago | Beverly Spalla |



Learn abo



Learn ho

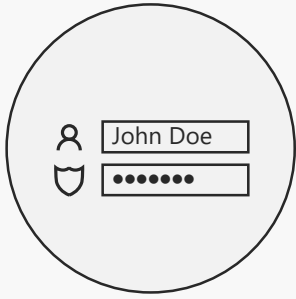


Secure authentication

On the road to...

NO PASSWORDS

A photograph of a two-lane asphalt road stretching into the distance under a clear blue sky. The road is flanked by low, scrubby vegetation on a hillside. In the background, several white wind turbines are visible on a ridge. In the foreground on the right, a blue sign with a black border and the text "NO PASSWORDS" in bold black letters is mounted on a post. A yellow and blue striped guardrail is visible below the sign. The overall scene suggests a remote or off-grid location.



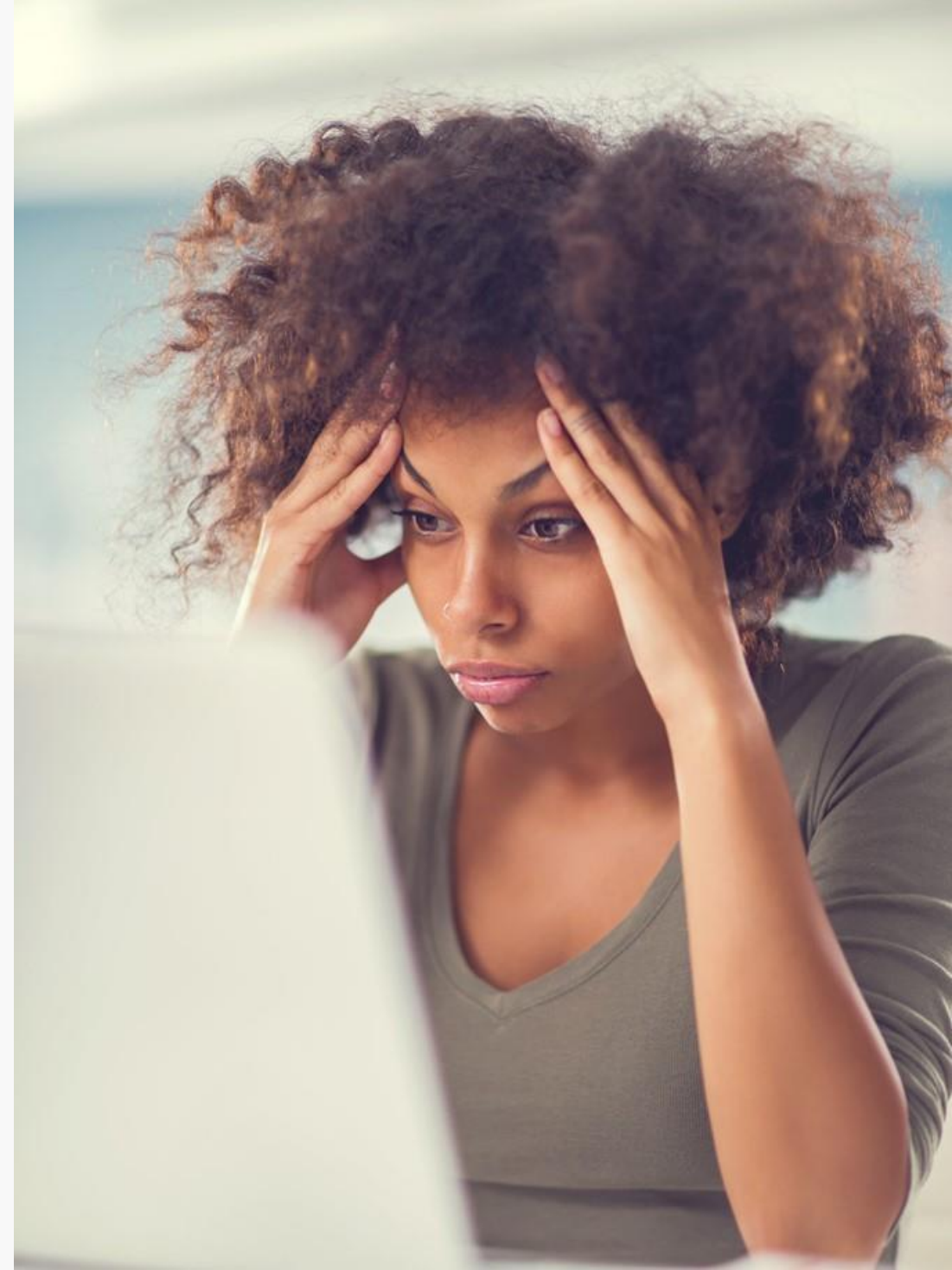
Nobody likes passwords

Alpha-numeric passwords are hard for humans to remember and easy for computers to guess

On mobile devices entering passwords is impossible

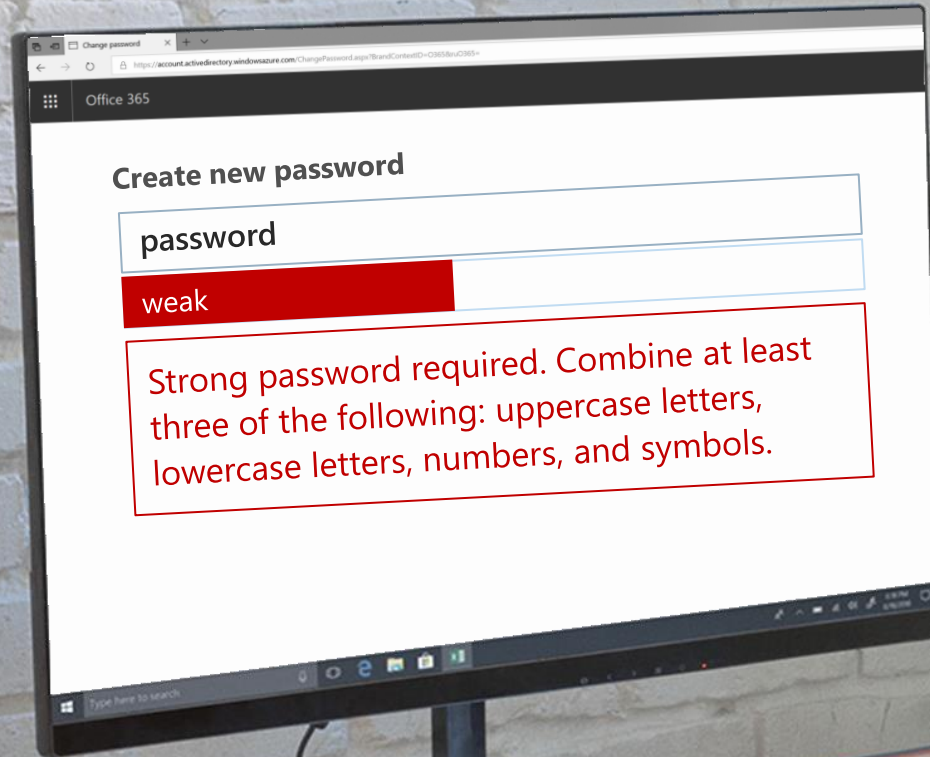
Credential reuse across multiple services increases attack surfaces

Even the strongest passwords are easily phishable



One weak password is all it takes

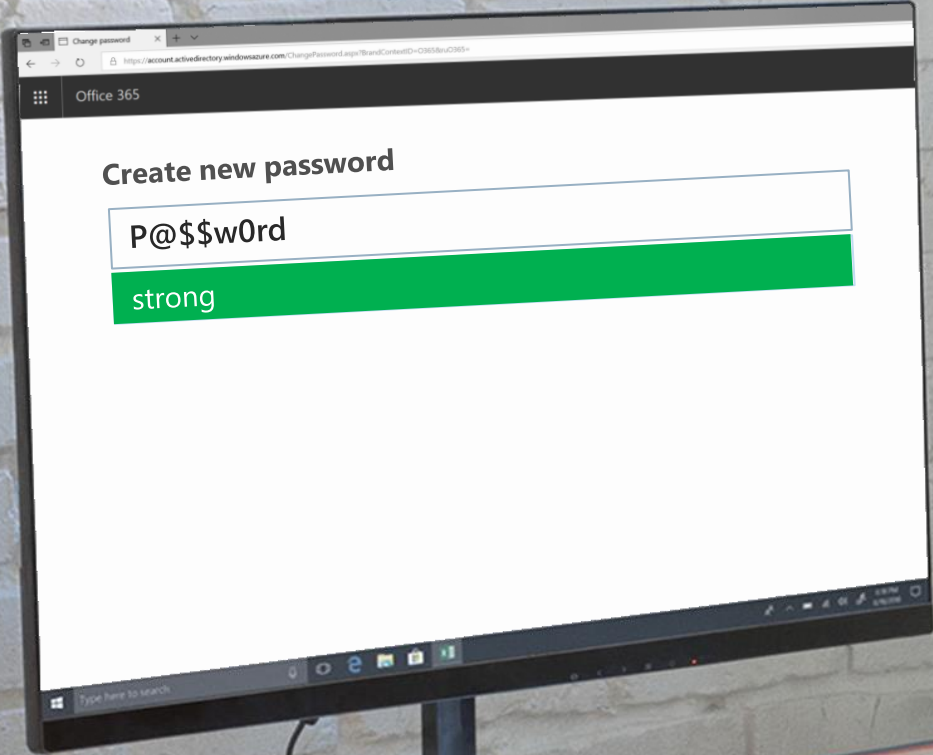
IT Admin



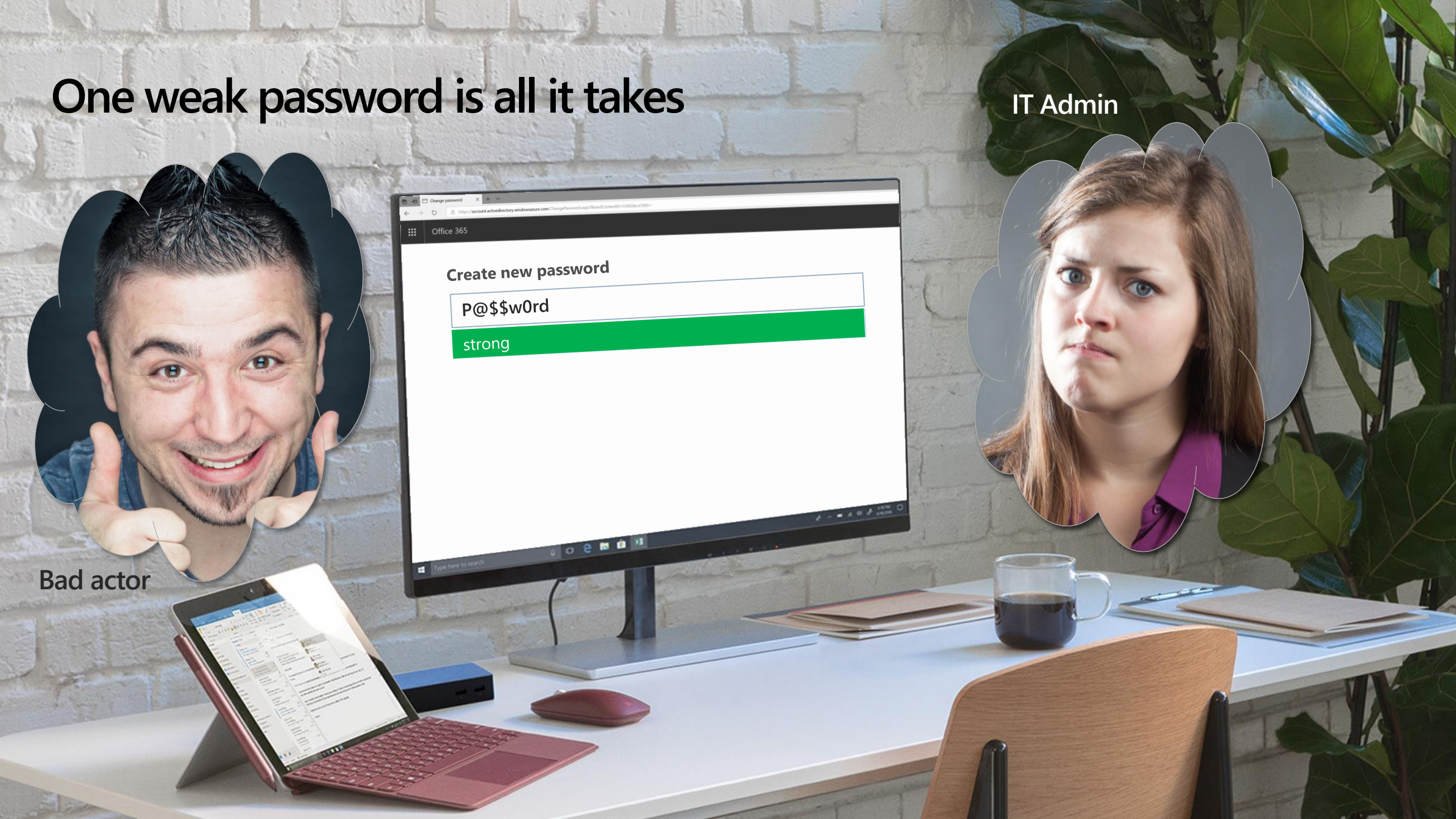
One weak password is all it takes



Bad actor



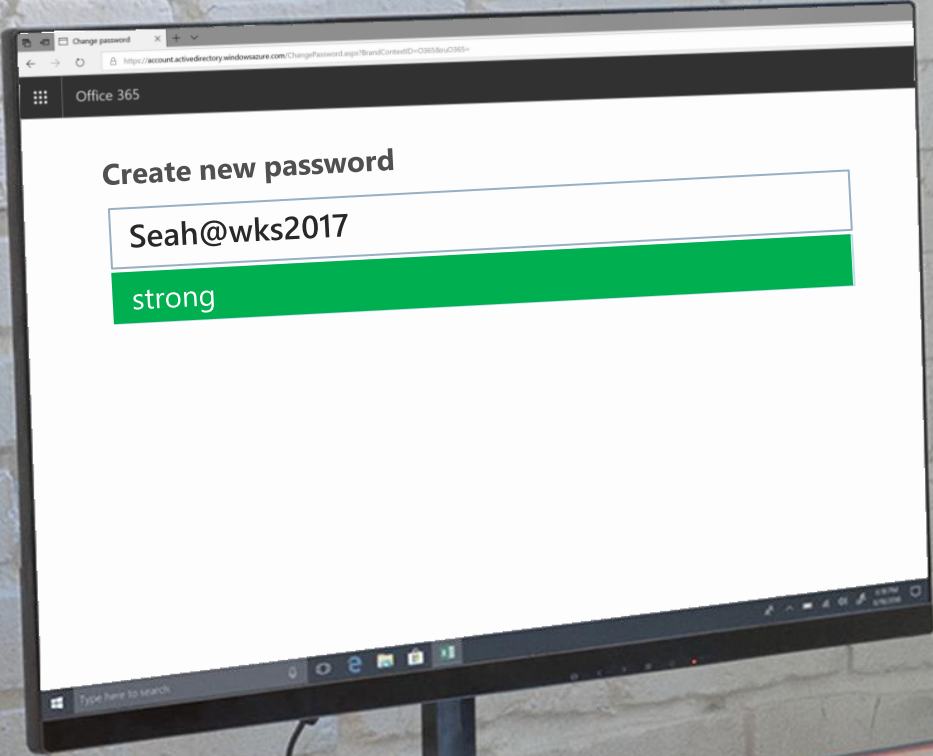
IT Admin



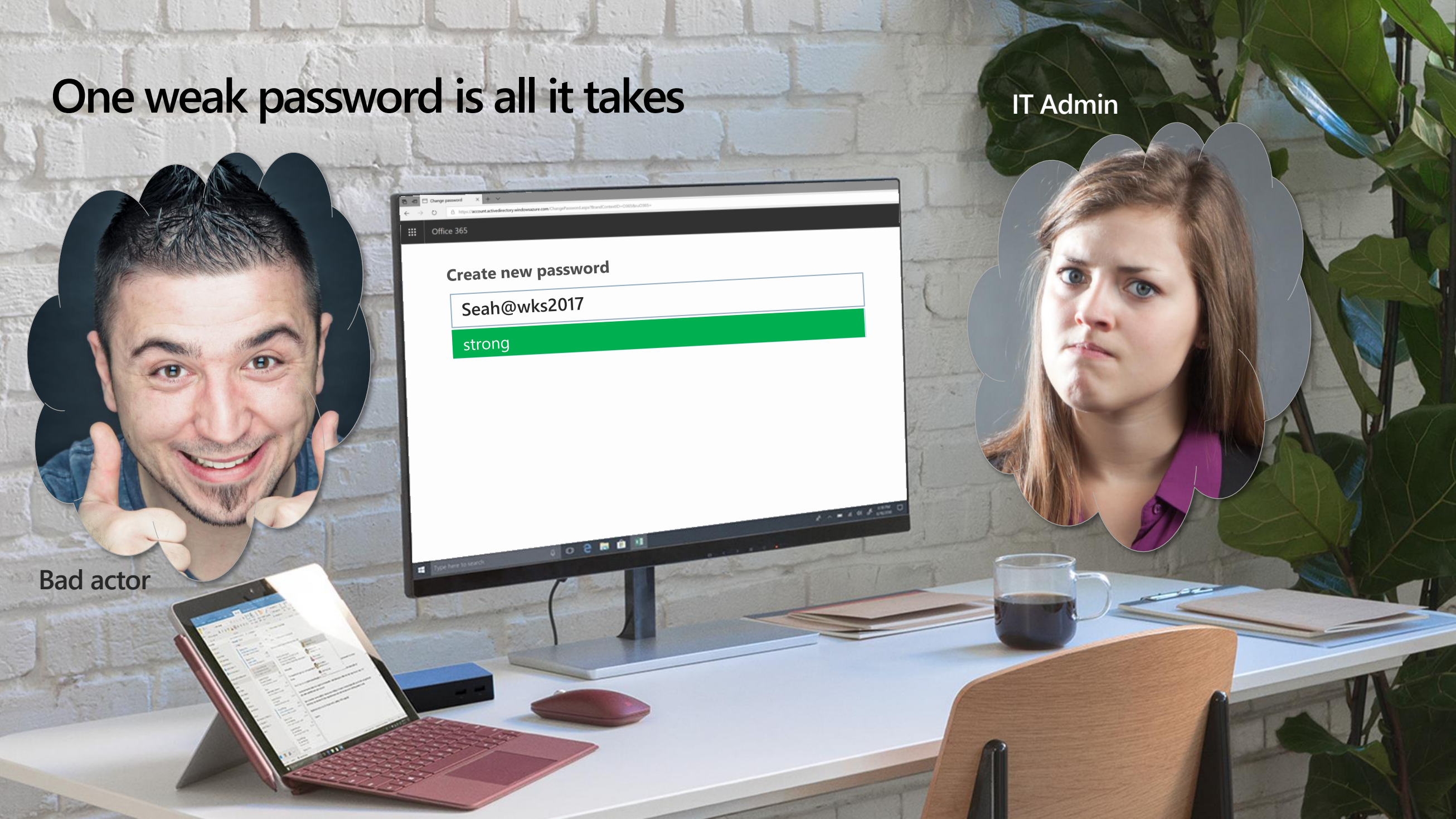
One weak password is all it takes



Bad actor



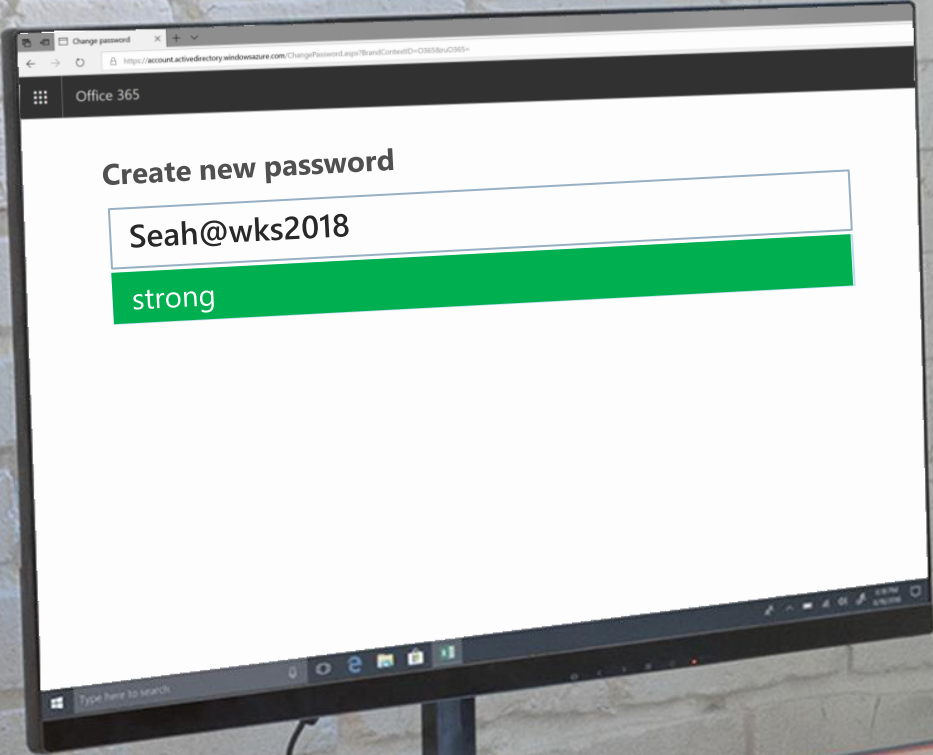
IT Admin



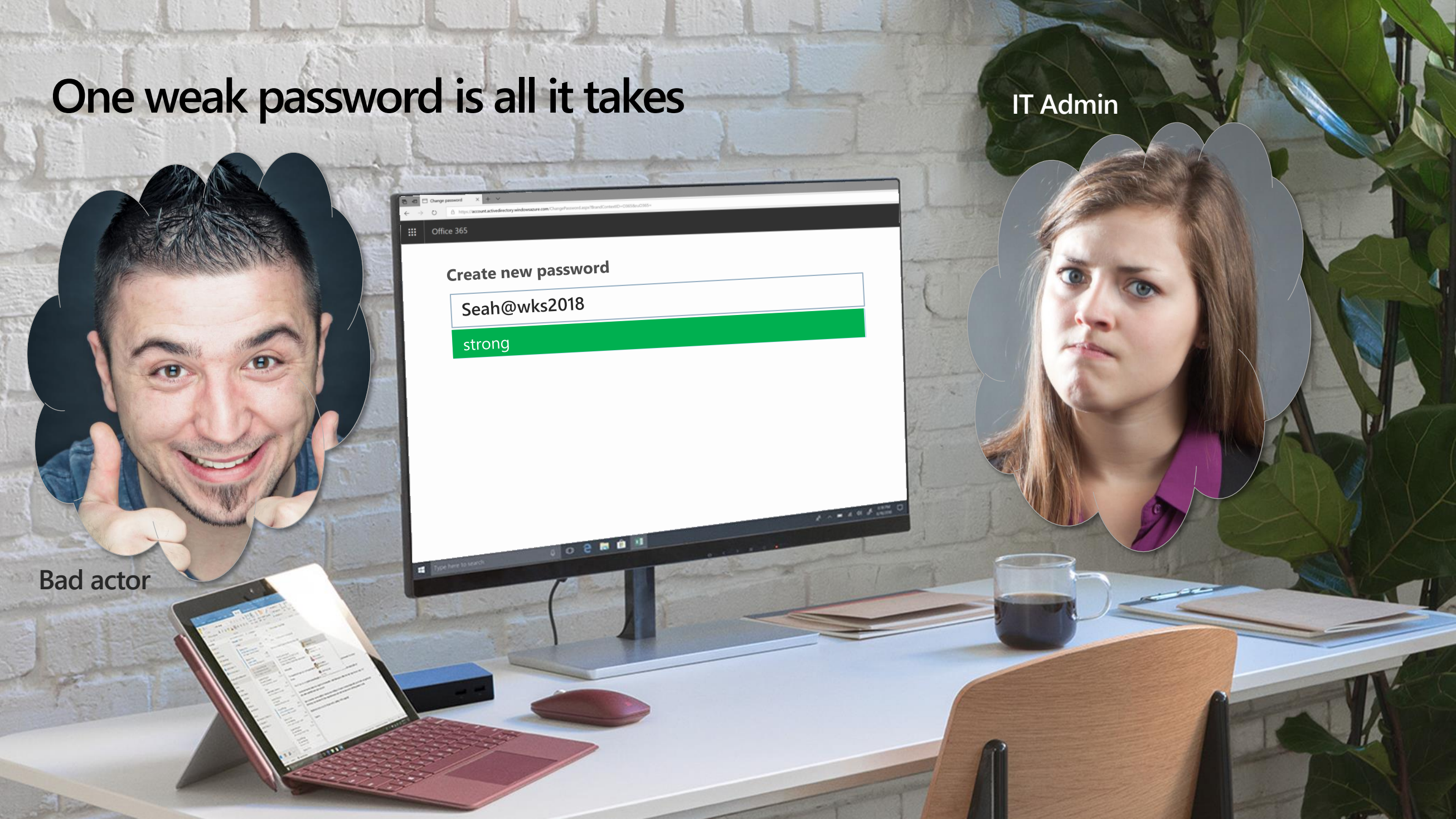
One weak password is all it takes



Bad actor



IT Admin

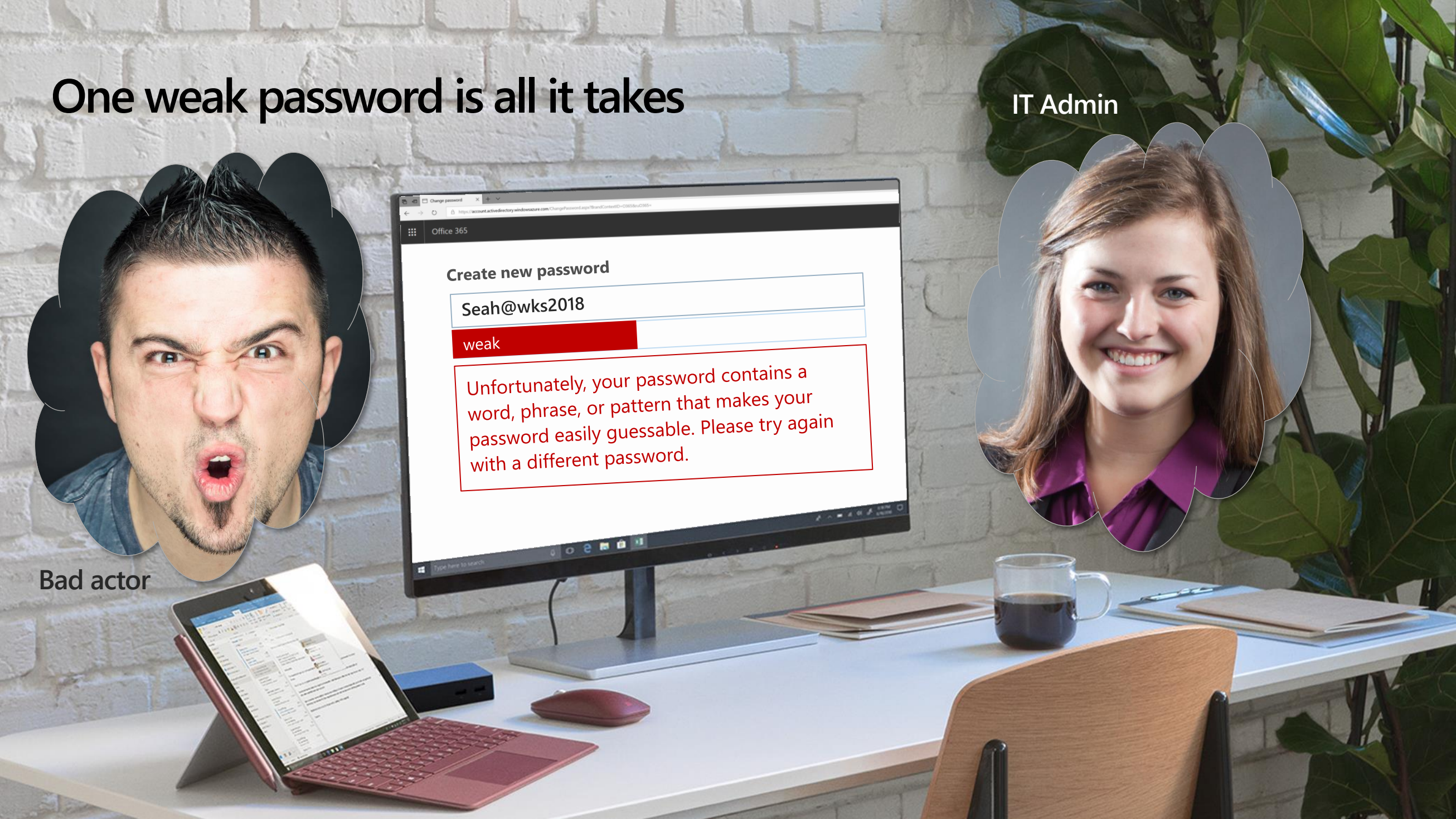
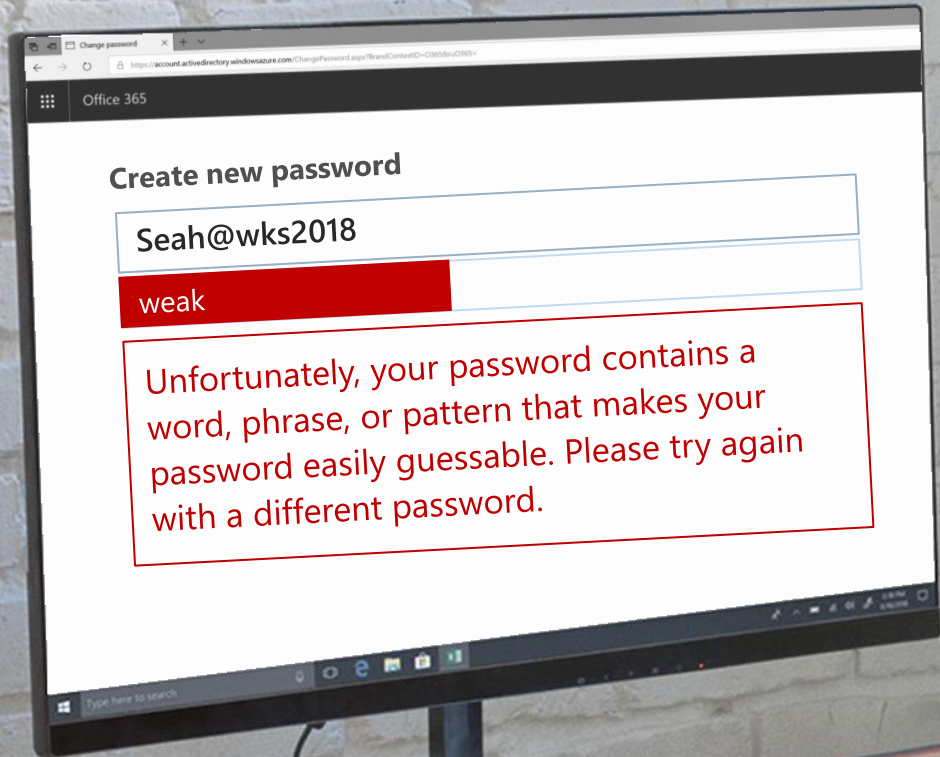


One weak password is all it takes

IT Admin



Bad actor



Azure AD Password Protection

Cloud intelligence to ensure strong passwords

Dynamic banning of passwords based on known bad patterns and those you define.

Smart Lockout to thwart bad actors trying to guess passwords.

Built for hybrid environments.

Unified admin experience for on-premises and cloud.

The screenshot shows the 'Authentication methods - Password Protection' configuration page in the Azure AD portal. The breadcrumb trail is 'Home > fab identity > Security > Authentication methods - Password Protection'. The page title is 'Authentication methods - Password Protection' with sub-breadcrumbs 'fab identity' and 'Azure AD Security'. At the top, there are 'Save' and 'Discard' buttons. The configuration is divided into several sections: 1. 'Custom smart lockout' with 'Lockout threshold' set to 10 and 'Lockout duration in seconds' set to 60. 2. 'Custom banned passwords' with 'Enforce custom list' set to 'Yes' and a list of banned passwords including 'identity', 'fabric', and 'contoso'. 3. 'Password protection for Windows Server Active Directory' with 'Enable password protection on Windows Server Active Directory' set to 'Yes' and 'Mode' set to 'Enforced'.

Home > fab identity > Security > Authentication methods - Password Protection

Authentication methods - Password Protection

fab identity > Azure AD Security

Save Discard

Custom smart lockout

Lockout threshold 10

Lockout duration in seconds 60

Custom banned passwords

Enforce custom list Yes No

Custom banned password list identity
fabric
contoso

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

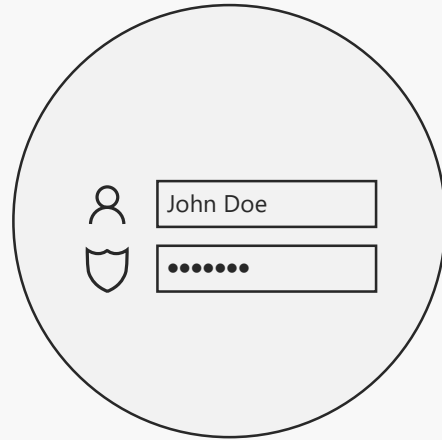


Nobody likes standard 2FA

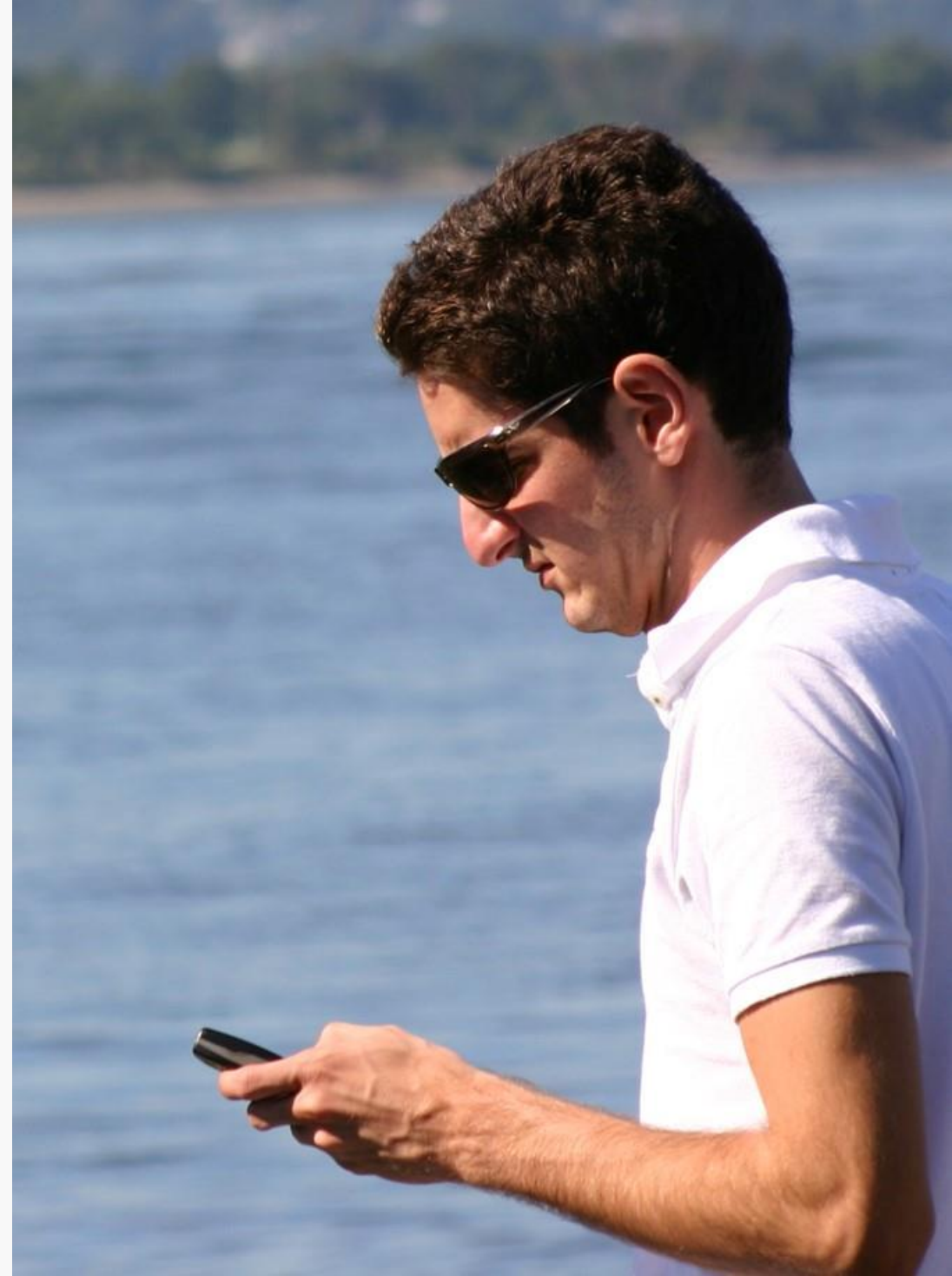
Passwords + 2FA is more secure, but also more complicated and difficult to use.



2FA



Passwords



Multi-factor authentication

Prevents 99.9% of identity attacks



Push-approval



SMS



Voice call



OATH
Token



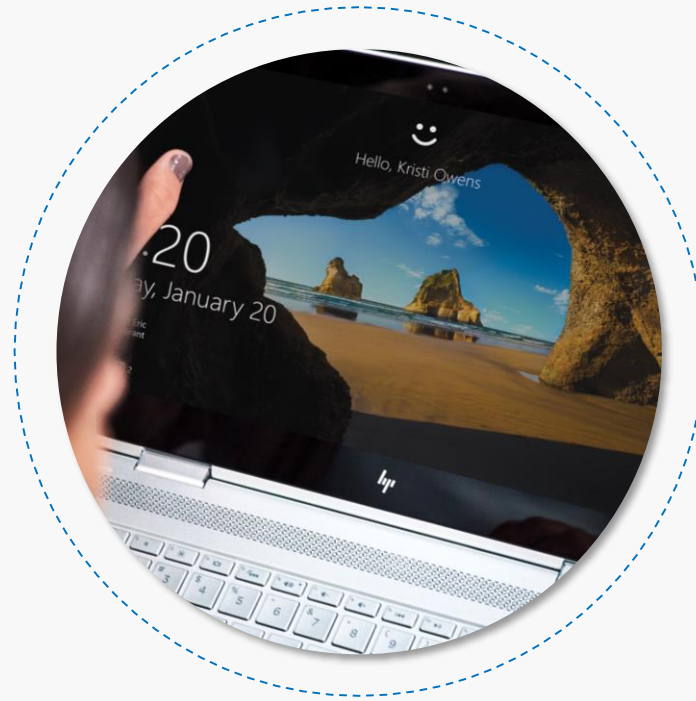
OATH
codes

Go password-less with Windows 10 Hello

Enterprise-grade security



User-friendly experience



Password-less authentication



47M
active Windows
Hello users



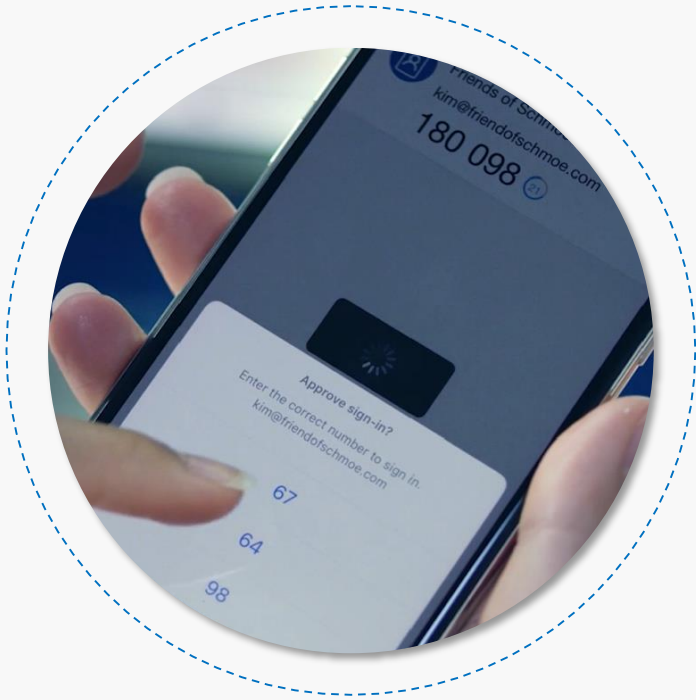
6.5K
enterprises have deployed
Windows Hello for Business



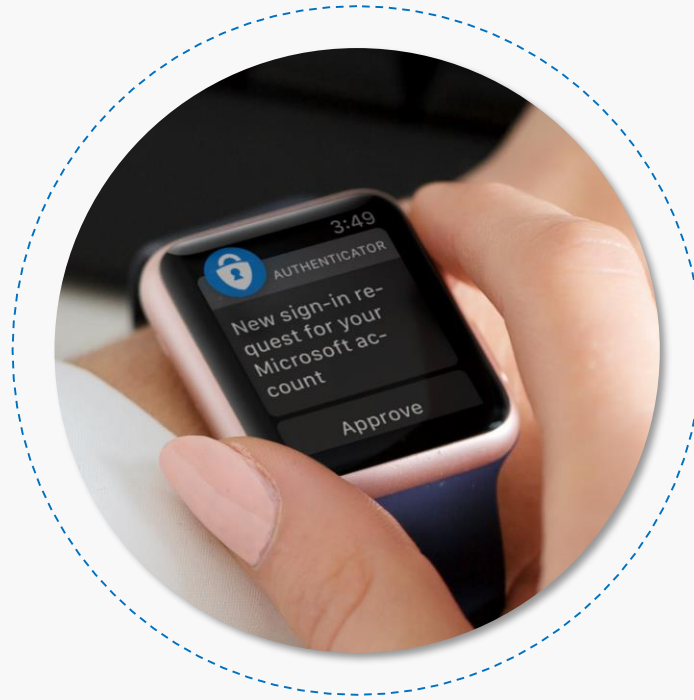
350%
growth in biometric
capable computers

Go password-less with Microsoft Authenticator

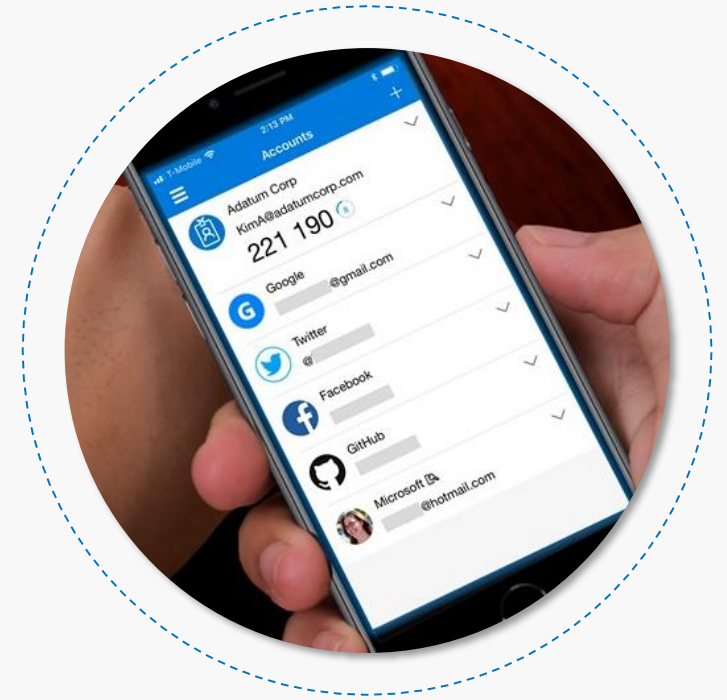
Password-less authentication



User-friendly experience




OATH passcodes for 3rd party accounts






5M+ active users




20M+ downloads

 Microsoft



Pick an account


-  MeganB@adatumcorp.com 
-  Use another account



 Microsoft

Pick an account

 MeganB@adatumcorp.com 

 Use another account





← meghanb@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

62

[Use your password instead](#)

Adatum Corp
MeghanB@adatumcorp.com
589 535 20



Approve sign-in?

Enter the correct number to sign in.
MeghanB@adatumcorp.com

62

16

48

Deny



← meganb@adatumcorp.com

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

62

[Use your password instead](#)

Adatum Corp
MeganB@adatumcorp.com
589 535

Touch ID for "Authenticator"

Cancel



meganb@adatumcorp.com

Approved.



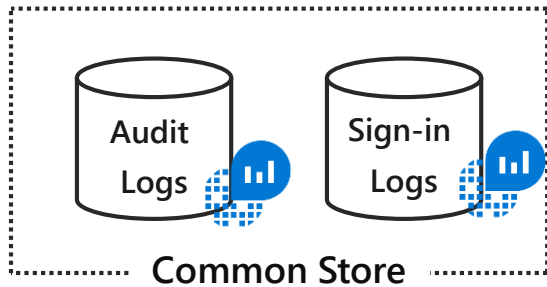
MeganB@adatumcorp.com

589 535 6



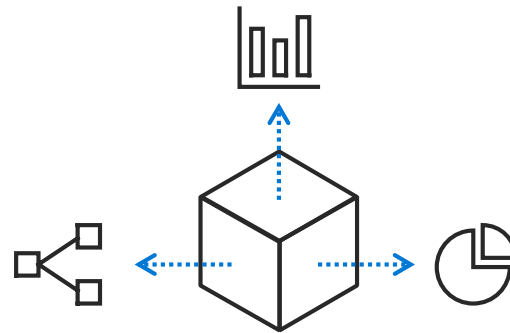
Better Insights

Azure AD Monitor



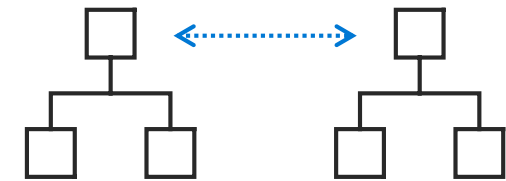
Unified Monitoring

A common platform for all Azure AD logs



Analyze

Rich Insights, advanced analytics and smart machine learning powered by Log Analytics



Workflow Integrations

Rich ecosystem of popular issue management, SIEM, and ITSM tools

Advanced Queries with Log Analytics

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

The image displays two screenshots of the Azure Log Analytics interface. The top screenshot shows a Kusto query being executed in the 'f/128 Photography - Logs' workspace. The query is:

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

The bottom screenshot shows the 'Azure AD Account Provisioning Events' dashboard. It features three main sections: 'NEW USERS PROVISIONED' (Successful add operations: 46.0, Failed add operations: 898), 'USERS UPDATED' (Successful update operations: 45k), and a table of application counts.

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

The world's #1 enterprise identity service

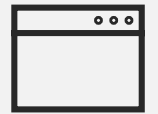
19.3M
organizations



1.2B
identities



810k
3rd party apps
in Azure AD



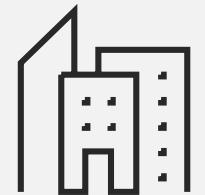
104k
paid Azure AD /
EMS customers



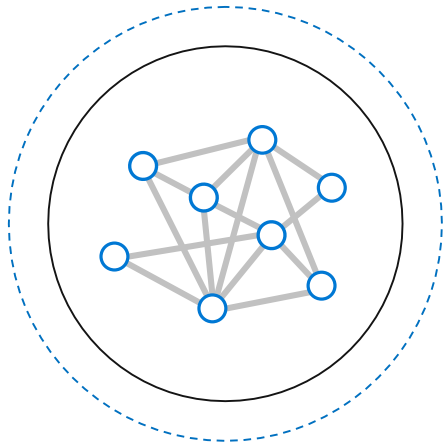
8B
daily Azure AD
authentications



90%
of Fortune 500
companies

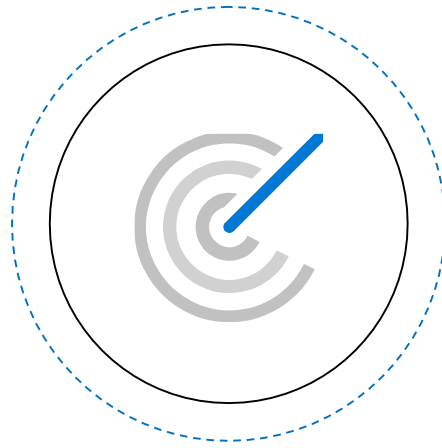


The promise of Intelligent Security



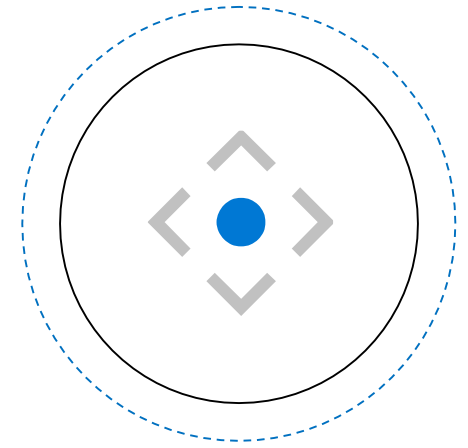
Connected Intelligence

Observe trillions of signals and risk events from cloud systems



Continuous Detection

Apply artificial intelligence and human expertise to derive accurate insights



Actionable Insights

Alert, self-mitigate, and automatically remediate threats



Thank you.