



# Security in Azure

## Global Azure Bootcamp 2019

Michael de Blok

Principal Solutions Architect – Cloud  
Infrastructure

[mdeblok@bennettadelson.com](mailto:mdeblok@bennettadelson.com)

**2019**  
Global **Azure**  
**BOOTCAMP**

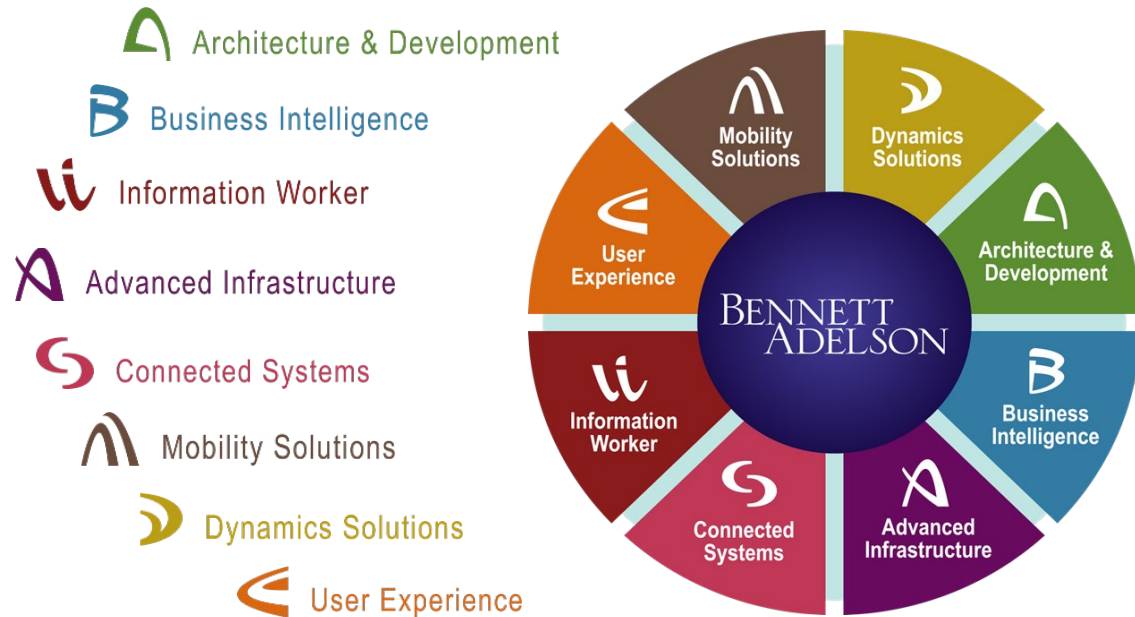
BENNETT ADELSON™

BENNETT ADELSON

## Company Highlights

- Established in 1996, with more than 1,000 clients serviced to date
- Headquartered in Cleveland, with a satellite office in Columbus
- Local and national clients, with international service delivery capabilities and experience

## Eight Practice Disciplines



## Significant Achievements

- 2017 and 2016 Top 200 Microsoft Partners, Redmond Channel Partners
- 2015 Top 100 Most Promising Microsoft Solution Providers, CIO Review
- 2011 Microsoft Partner of the Year, Heartland District
- 2010 Microsoft Partner of the Year Finalist
- Office 365 TAP Member
- Office 365 FastTrack Partner
- Office 365 Preferred Deployment Partner
- Member of Microsoft's SharePoint Patterns & Practices Council
- Members of the Microsoft Partner Advisory Council
- Founded the Cleveland SharePoint and .NET Special Interest Group
- Microsoft Gold Partners: Cloud, Collaboration and Content
- Microsoft Silver Partners: Cloud Productivity, Windows and Devices

# Presentation Overview

- Conditional Access
- PIM - Privileged Identity Management
- JIT – Just in Time
- Azure Active Directory
- Cloud App Security
- App/Device Policies
- Fabric security

# Conditional Access

- Hybrid AD
- Multi Factor Authentication
- Registered Apps
- Locations
- Modern Auth
  - Modern Authentication capability enables Active Directory Authentication Library (ADAL)-based sign-in for Office client apps across different platforms. This enables sign-in features such as Multi-Factor Authentication (MFA), smart card and certificate-based authentication.





# Conditional Access - MFA

Medium Risk MFA CA Policy

Info

Delete

Name

Medium Risk MFA CA Policy

Assignments

Users and groups

All users

Cloud apps

All cloud apps

Conditions

2 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Grant

Select the controls to be enforced.

Block access

Grant access

☒ Require multi-factor authentication

☐ Require device to be marked as compliant

☐ Require Hybrid Azure AD joined device

☐ Require approved client app

☐ Require app protection policy (preview)

[See list of approved client apps](#)

[See list of policy protected client apps](#)

For multiple controls

Require all the selected controls

Require one of the selected controls

BENNETT ADELSON

# Conditional Access – Registered Apps

New

Info

Name

Example: 'Device compliance app policy'

Assignments

Users and groups

All users

Cloud apps

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Cloud apps

Include

Exclude

None

All cloud apps

Select apps

Select

None

Select

Cloud apps

Applications

Search Applications...

Adobe

Adobe Creative Cloud

AA

Azure AD Power BI Content Pack

Azure Analysis Services

Cisco Umbrella

S

Citrix ShareFile

C.

Concur

BENNETT ADELSON

# Conditional Access – Locations

## Conditional Access - Named locations

Azure Active Directory

« Policies

Manage

Named locations

Custom controls (preview)

Terms of use

VPN connectivity

Classic policies

Troubleshooting + Support

Troubleshoot

New support request

+ New location [Configure MFA trusted IPs](#)

Named locations are used by Azure AD security reports to reduce false positives and Azure AD conditional access policies. [Learn more](#)

NAME	TRUSTED	
ACCEL	✓	...
BW 1CC	✓	...
BW 1CC-Backup	✓	...
BW CHA	✓	...
BW CHI	✓	...
BW CMD	✓	...
BW DAL	✓	...
BW DEN	✓	...
BW DET	✓	...
BW GRE	✓	...



# Conditional Access – Modern Auth

Block Legacy Authentication ...	Conditions	Client apps (preview)
<div><div>Info</div><div>Delete</div></div> <div><div>Name</div><div>Block Legacy Authentication CA Policy</div></div> <div><div>Assignments</div><div><div>Users and groups</div><div>All users included and specific use...</div></div><div><div>Cloud apps</div><div>1 app included</div></div><div><div>Conditions</div><div>2 conditions selected</div></div></div> <div><div>Access controls</div><div><div>Grant</div><div>Block access</div></div></div>	<div><div>Info</div></div> <div><div>Sign-in risk</div><div>Not configured</div></div> <div><div>Device platforms</div><div>Not configured</div></div> <div><div>Locations</div><div>Any location and all trusted locati...</div></div> <div><div>Client apps (preview)</div><div>1 included</div></div> <div><div>Device state (preview)</div><div>Not configured</div></div>	<div><div>Configure</div><div>YesNo</div></div> <div><div>Select the client apps this policy will apply to</div><div><div>Browser</div><div>Mobile apps and desktop clients</div><div>Modern authentication clients</div><div>Exchange ActiveSync clients</div><div>Other clients</div></div></div>

# PIM & JIT

- Privileged Identity Management
  - Provide just-in-time privileged access to Azure AD and Azure resources
  - Assign time-bound access to resources using start and end dates
  - Require approval to activate privileged roles
  - Enforce multi-factor authentication to activate any role
- Just in Time
  - Locks down inbound traffic to your Azure VMs by creating a NSG rule
  - You select the ports on the VM to which inbound traffic will be locked down

# Privileged Identity Management

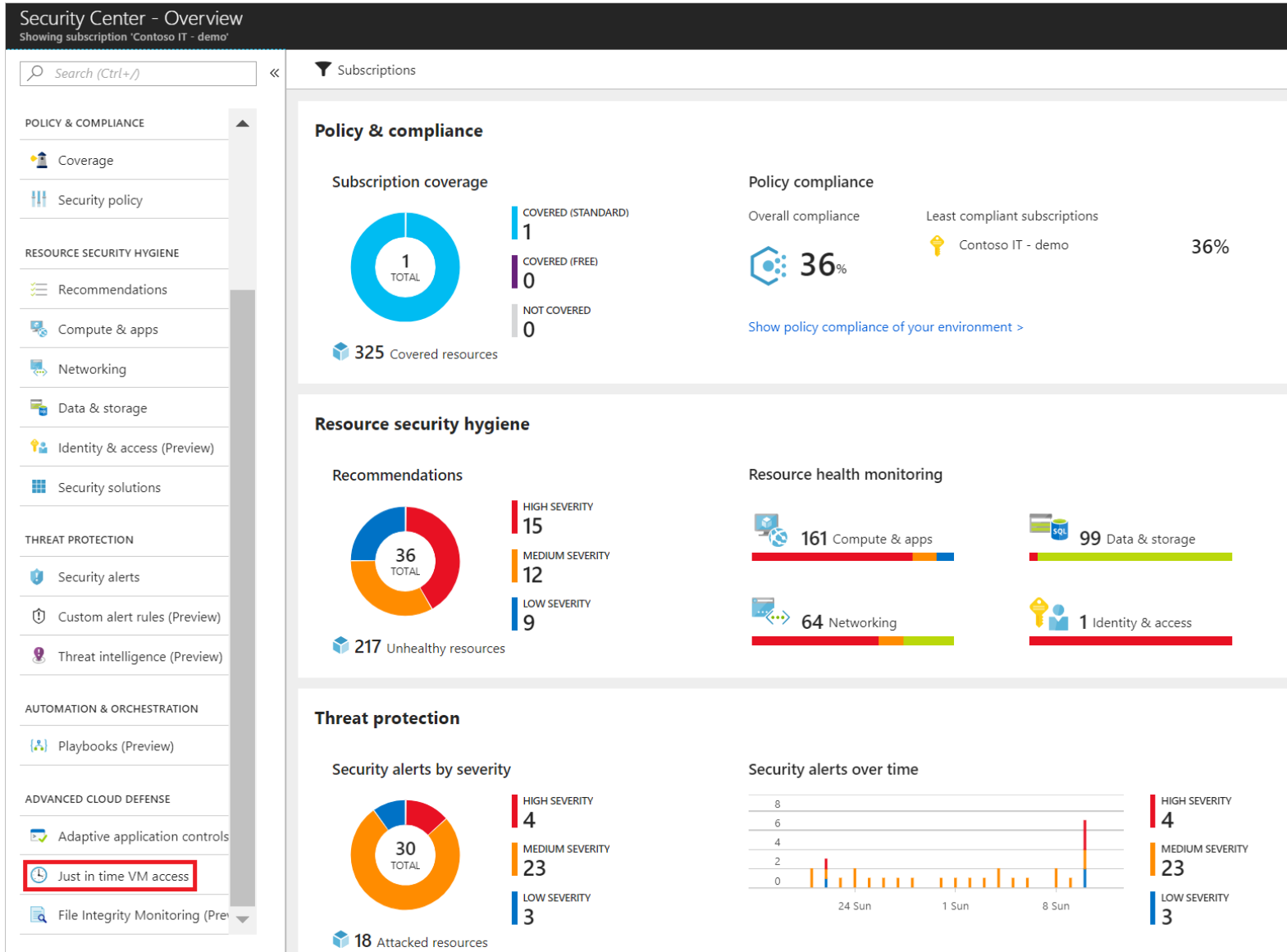
The screenshot displays the Azure AD Privileged Identity Management (PIM) console. The breadcrumb navigation at the top reads: Dashboard > Privileged Identity Management > Azure AD roles - Quick start. The interface is divided into three main sections: a left-hand navigation pane, a central task pane, and a main content area.

**Left-hand navigation pane:** This pane contains a vertical list of icons and labels for navigation. The 'Manage' section is expanded, showing 'Azure AD roles' as the selected item. Other sections include 'Quick start', 'Tasks', 'My roles', 'My requests', 'Approve requests', 'Review access', 'Azure resources', 'Activity', 'My audit history', 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'.

**Central task pane:** This pane mirrors the structure of the left-hand navigation pane, providing a secondary set of links. The 'Quick start' link is highlighted. It includes sections for 'Tasks' (My roles, My requests, Approve requests, Review access), 'Manage' (Roles, Members, Alerts, Access reviews, Wizard, Settings), 'Activity' (Directory roles audit history, My audit history), and 'Troubleshooting + Support' (Troubleshoot, New support request).

**Main content area:** This area features the 'Azure AD Privileged' logo and a brief description: 'Azure AD PIM is a Premium feature that...'. Below this, there is an 'Assign' section with a diagram showing a user icon connected to three role icons. The text states: 'Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary'. A blue button labeled 'Assign eligibility' is positioned at the bottom of this section.

# Just in Time



# Just in Time

Home > Virtual machines > vm-contoso-us - Configuration

Virtual machines  
Microsoft

+ Add ⌚ Reservations ... More

Filter by name...

NAME ↑↓

- vm-usa
- vm-contoso-us**
- vm-europe
- vm-contoso1
- vm-contoso2
- vmcontoso-3
- vm-contoso4
- vm-london
- vm-marketing
- vm-hr
- vm-uni
- vm-contoso-hr
- vm-contoso

vm-contoso-us - Configuration  
Virtual machine

Search (Ctrl+ /)

Save Discard

**Just-in-time access**  
To improve security, enable a just-in-time access policy. ⓘ  
**Enable just-in-time policy**

Azure hybrid benefit  
Use existing Windows license ⓘ  
No Yes

Settings

- Networking
- Disks
- Size
- Security
- Extensions
- Continuous delivery (Preview)
- Availability set
- Configuration**
- Identity (Preview)

# Azure Active Directory

- Risky Logins
- Password protection



# Azure Active Directory – Risky Logins

Account usernames and passwords that have been posted online by attackers. Microsoft collects this data from researchers, industry partners, and law enforcement agencies.

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE		
High	Offline	Users with leaked credentials ⓘ	13 of 25	4/4/2019, 8:28 AM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	2997 of 3380	4/24/2019, 10:24 AM
Medium	Offline	Impossible travels to atypical locations ⓘ	7 of 63	4/25/2019, 12:10 PM
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ	1359 of 4267	4/25/2019, 3:02 PM
Low	Offline	Sign-ins from infected devices ⓘ	1 of 6	4/10/2019, 6:01 AM





















# Azure Active Directory – Risky Logins

## Users with leaked credentials

RISK EVENTS

Last 90 days Details Download Refresh

Apply a user risk policy for automatic mitigation. →

USER	DISCOVERED (UTC)	STATUS
 Amber	4/4/2019 08:28	Active
 Amber	4/2/2019 20:09	Active
 Amber	4/1/2019 07:30	Active
 Derek	3/25/2019 14:03	Active
 Allison	3/8/2019 22:19	Active
 Rachel	3/8/2019 17:06	Active
 Alice	3/8/2019 16:44	Active
 Deanna	3/8/2019 15:51	Active
 Bryan	3/8/2019 14:40	Active
 Steven	3/6/2019 13:10	Active
 Pamela	3/6/2019 09:14	Active
 Mary	3/6/2019 06:55	Active
 Gwendolyn	2/27/2019 16:31	Closed (passwor...
 Joseph	2/27/2019 15:26	Closed (passwor...
 Amy	2/27/2019 09:35	Closed (passwor...
 Brian	2/27/2019 04:41	Closed (passwor...
 Gregory	2/27/2019 01:56	Closed (passwor...
 Amy	2/26/2019 17:25	Closed (passwor...
 Gwendolyn	2/26/2019 05:34	Closed (passwor...
 Gregory	2/26/2019 04:26	Closed (passwor...

## Amber

All sign-ins Reset password Dismiss all events

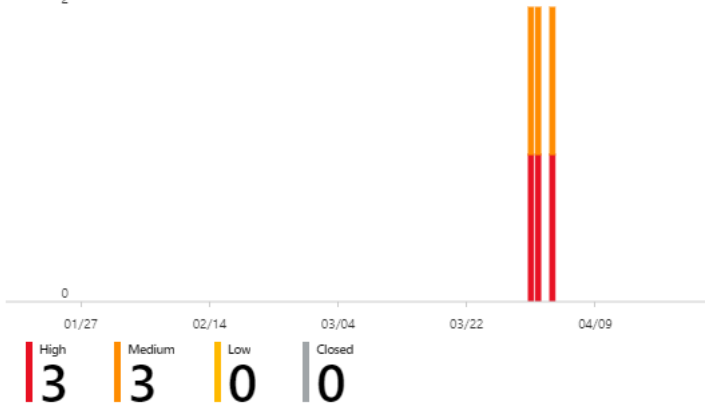
User has a high risk level

Essentials

Risk level	Status
High	At risk
Role	Contact
User	
Location	MFA registered
US	Yes
Department	Object Id
	b64fc709-b71f-4b54-






### Risk events

2



TIME (UTC)	IP ADDRESS	RISK EVENT TYPE	RISK LEVEL
4/4/2019 08:28	118.163.135.17	Sign-in from unfamiliar location	Medium
4/4/2019 08:28		User with leaked credential	High
4/2/2019 20:09	200.175.104.101	Sign-in from unfamiliar location	Medium
4/2/2019 20:09		User with leaked credential	High
4/1/2019 07:30	61.185.139.72	Sign-in from unfamiliar location	Medium

# Azure Active Directory – Risky Logins

Sign-ins from anonymous IP addresses						
RISK EVENTS						
Last 90 days Columns Details Download Refresh						
Apply a sign-in risk policy for automatic mitigation. →						
	Jason	178.175.143.164	Kishinev, Kishinev, Moldova	2/5/2019 5:13 AM	Active	...
	Allen	173.239.199.86	IL, United States	▶ 450 instances	Active	...
	Allen	173.239.199.183	IL, United States	▶ 408 instances	Active	...
	Allen	173.239.199.208	IL, United States	▶ 1426 instances	Active	...
	Allen	173.239.199.31	IL, United States	▶ 291 instances	Active	...

## Impossible travel to atypical locations

RISK EVENTS

	Vamkeswara...	77.247.181.165	Roosendaal, North Brabant,...	1/28/2019 2:35 PM	Active	...
	Vamkeswara...	185.234.217.241	Cork, County Cork, Ireland	1/28/2019 2:25 PM	Active	...
	Vamkeswara...	109.70.100.20	Vienna, Vienna, Austria	1/28/2019 2:11 PM	Active	...

# Azure Active Directory – Password Protection

## Authentication methods - Password protection

Bellwether Enterprise - Azure AD Security

Search (Ctrl+/)



Save Discard

### Manage

Password protection

### Custom smart lockout

Lockout threshold 3 ✓

Lockout duration in seconds 3600 ✓

### Custom banned passwords

Enforce custom list Yes No

Custom banned password list 123456 ✓  
123456789  
qwerty  
Summer2018  
Spring2019  
password  
P@ssw0rd!  
Welcome1

### Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

# Azure Active Directory – Password Protection

## Most hacked passwords revealed as UK cyber survey exposes gaps in online security

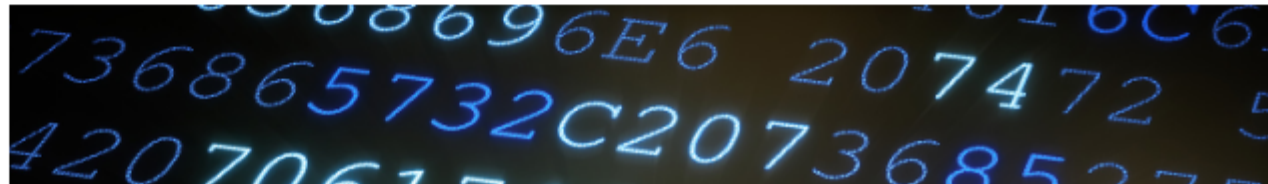
The NCSC's first 'UK cyber survey' published alongside global password risk list

---

PUBLISHED

21 April 2019

---



<https://bit.ly/ncsc-survey>

# Azure Active Directory – Password Protection

Most used in total	Names	Premier League football teams	Musicians	Fictional characters
123456 (23.2m)	ashley (432,276)	liverpool (280,723)	blink182 (285,706)	superman (333,139)
123456789 (7.7m)	michael (425,291)	chelsea (216,677)	50cent (191,153)	naruto (242,749)
qwerty (3.8m)	daniel (368,227)	arsenal (179,095)	eminem (167,983)	tigger (237,290_)
password (3.6m)	jessica (324,125)	manutd (59,440)	metallica (140,841)	pokemon (226,947)
11111 (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)



# Cloud App Security




Dashboard

Discover

Investigate

Control


Alerts

 **General dashboard** >


View dashboard for a specific app

- ✓ Yammer - General
- ! Office 365
- ! Microsoft Exchange Online
- ! Microsoft Exchange Online - General
- ✓ Microsoft SharePoint Online - General
- ✓ Microsoft SharePoint Online
- ! Microsoft OneDrive for Business
- ✓ Office 365 - General
- ✓ Microsoft Azure AD
- ✓ Microsoft OneDrive for Business - General
- ✓ Microsoft Office 365 admin center
- ✓ Microsoft Online Services
- ✓ Concur
- ✓ Microsoft Teams
- ✓ Microsoft Office Online - General
- ✓ Microsoft Forms
- ✓ Microsoft Skype for Business - General
- ✓ Microsoft Azure
- ✓ Microsoft Office Online

Get started with Cloud App Security

 Create a Cloud Discovery report


 Connect apps

 Create policies

[Learn more...](#)





## General dashboard


 **5K+**  
activities monitored

 **95.8K**  
files monitored

 **1.5K**  
accounts monitored




 **Discover your cloud apps**  
upload traffic logs

 **15**  
governance actions taken

 **69**  
user notifications sent

**12** Open alerts  
New over the last month ▾

### RECENT ALERTS

-  **Multiple failed user log on attempts to an app** 11 hours ago  
Office 365
-  **Multiple failed user log on attempts to an app** 11 hours ago  
Office 365
-  **Multiple failed user log on attempts to an app** 12 hours ago  
Office 365

[View all alerts in the last month...](#)

### BY SEVERITY



High  
Medium  
Low

### BY ALERT TYPE



Custom  
Built-in

### Top 3 alert types

- 6** Activity policy alert
- 2** Impossible travel alert
- 2** Uncommon location alert

**4,265** Activity matches  
New over the last month ▾



**5** Administrative activity from a non-corporate IP address

**2** Content matches  
New over the last month ▾



**2** Malware detection

# Cloud App Security

Cloud App Security

1 - 20 of 1,171 activities

New policy from search

Dashboard

Discover

Investigate

Activity log

Files

Users and accounts

Security configuration

OAuth apps

Connected apps (39)

Control

Alerts

Activity	User	App	IP address	Location	Device	Date
Log on	Mike Deblok	Microsoft Cloud ...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Single sign-on log on	Mike Deblok (mdeblok)	Microsoft Cloud ...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Log on	Mike Deblok	Microsoft Cloud ...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Log on	Mike Deblok	Office 365	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Single sign-on log on	Mike Deblok (mdeblok)	Microsoft 365 a...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Log on	Mike Deblok	Office 365	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
FilePreviewed	Mike Deblok	Microsoft Share...	172.58.56.4	United States	Other	Apr 27, 2019, 9:02 AM
SearchQueryPerformed	Mike Deblok	Microsoft Share...	65.52.5.193	United S...	—	Apr 27, 2019, 9:02 AM
FilePreviewed	Mike Deblok	Microsoft Share...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Log on	Mike Deblok	Office 365	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Single sign-on log on	Mike Deblok (mdeblok)	Microsoft Excha...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
FilePreviewed	Mike Deblok	Microsoft Share...	20.190.128.103	United S...		Apr 27, 2019, 9:02 AM
Single sign-on log on	Mike Deblok (mdeblok)	Microsoft Office ...	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Log on	Mike Deblok	Office 365	172.58.56.4	United States		Apr 27, 2019, 9:02 AM
Single sign-on log on	Mike Deblok (mdeblok)	Microsoft Office	172.58.56.4	United States		Apr 27, 2019, 9:02 AM

# Policies

- Apps
- Devices

# Policies – Apps

Create policy

\* Name

Description

\* Platform

Android

Target to all app types

YesNo

\* Apps

32 apps selected

Settings

Default settings configured

Settings

Data protection

Default settings configured

Access requirements

Default settings configured

Conditional launch

Default settings configured

Scope (Tags)

0 scope(s) selected

Data protection

Data Transfer

Backup Org data to Android backup services

AllowBlock

All apps

Select

All apps

AllowBlock

0 selected

Any app

0

EnableDisable

Encryption

Encrypt Org data

RequireNot required

RequireNot required

Functionality

Sync app with native contacts app

EnableDisable

EnableDisable

RequireNot configured

Encrypt Org data on enrolled devices

Printing Org data

Share web content with policy managed browsers

# Policies – Devices

Policy for Windows - Properties

Save Discard

Name

Contoso MDM Compliance Policy for Win ... ✓

Description

Enter a description... ✓

Platform

Windows 10 and later ▼

Settings

21 configured >

Actions for noncompliance

1 configured >

Scope (Tags)

0 scope(s) selected >

Windows 10 compliance policy

Windows 10 and later

Select a category to configure settings.

Device Health

3 of 3 settings configured >

Device Properties

5 settings available >

Configuration Manager Compliance

1 of 1 setting configured >

System Security

15 of 16 settings configured >

Windows Defender ATP

1 of 1 setting configured >

Device Health

Windows 10 and later

Windows Health Attestation Service evaluation rules

Require BitLocker ⓘ

Require Not configured

Require Secure Boot to be enabled on the device ⓘ




























Require Not configured

Require code integrity ⓘ









Require Not configured

# Fabric Security

## NETWORKING (27)

 Virtual networks	★	 Virtual networks (classic)	★	 Load balancers
 Application gateways	★	 Virtual network gateways	★	 Local network gateways
 DNS zones	★	 CDN profiles	★	 Traffic Manager profiles
 ExpressRoute circuits	★	 Network Watcher	★	 Network security groups
 Network security groups (classic)	★	 Network interfaces	★	 Public IP addresses
 Public IP Prefixes	PREVIEW ★	 Reserved IP addresses (classic)	★	 Connections
 On-premises Data Gateways	★	 Route tables	★	 Route filters
 Application security groups	★	 DDoS protection plans	★	 Firewalls
 Front Doors	★	 Service endpoint policies	PREVIEW ★	 Virtual WANs

## SECURITY (8)

 Security Center	★	 Key vaults	★	 Application gateways
 Azure Information Protection	★	 Virtual network gateways	★	 Azure Active Directory
 Application security groups	★	 Azure Sentinel	PREVIEW ★	



# Thank you!

- Please fill out the session feedback forms in order to win a chance of winning an Amazon gift card 😊



# 2019



---

Global **Azure**  
**BOOTCAMP**

Thank You

BENNETT ADELSON<sup>sm</sup>