Security in Azure

Global Azure Bootcamp 2019

Michael de Blok

Principal Solutions Architect – Cloud Infrastructure

mdeblok@bennettadelson.com

2019 Global Azure BOOTCAMP

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

Architecture & Development

Business Intelligence

Information Worker

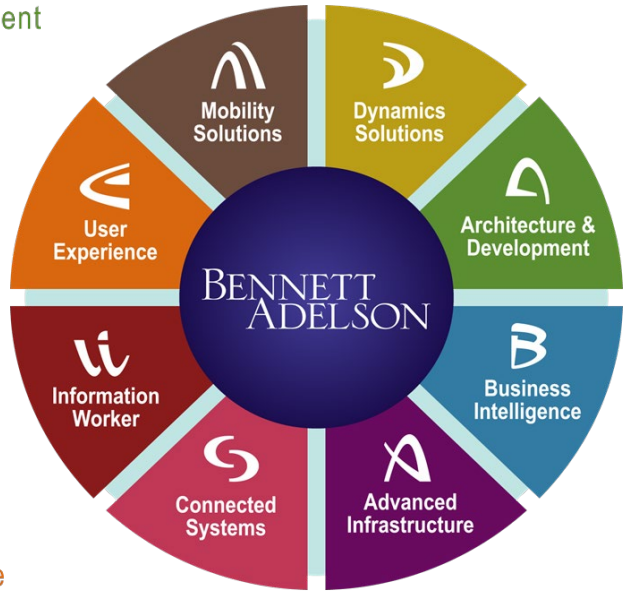
Advanced Infrastructure

Connected Systems

Mobility Solutions

Dynamics Solutions

User Experience



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

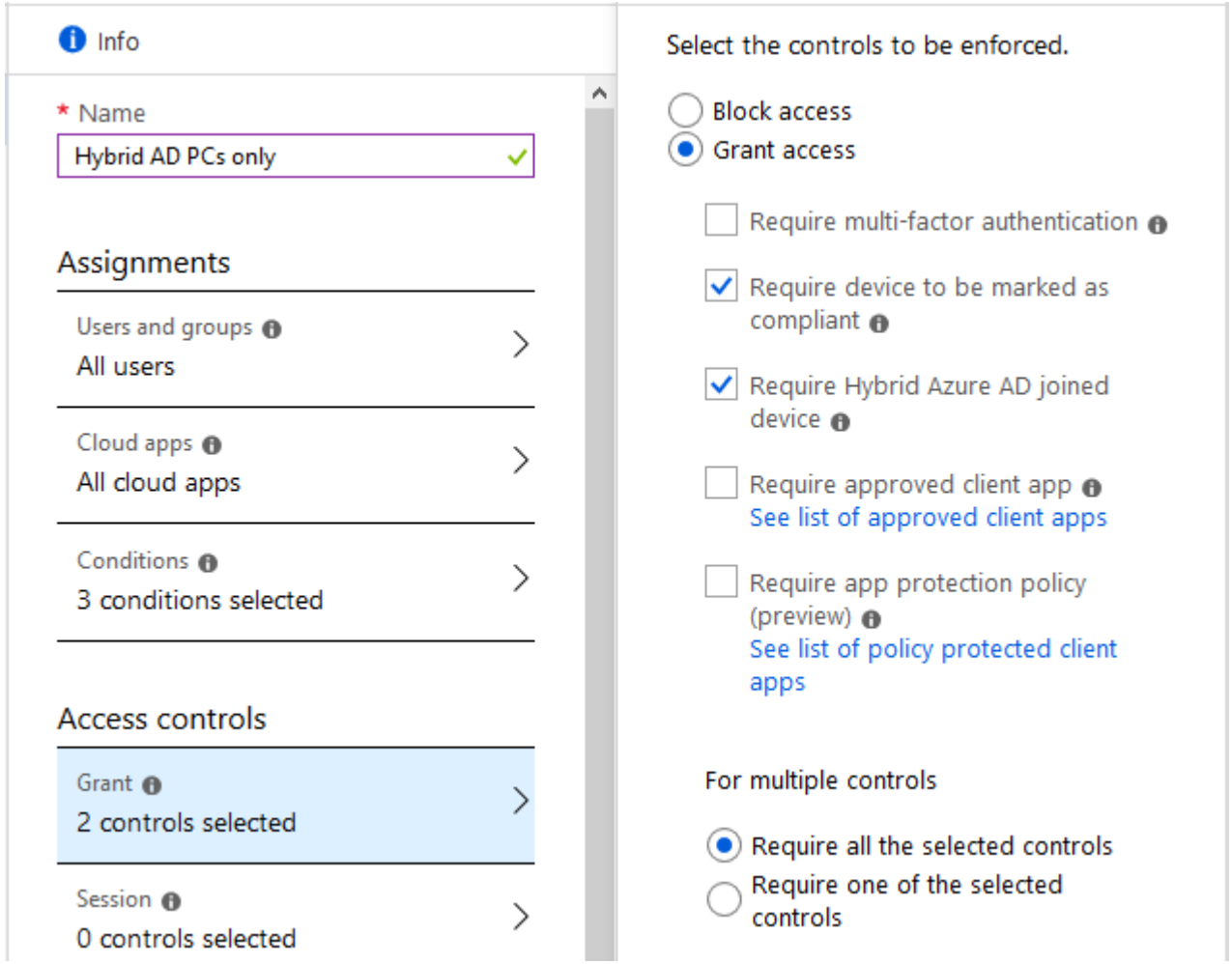
Presentation Overview

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

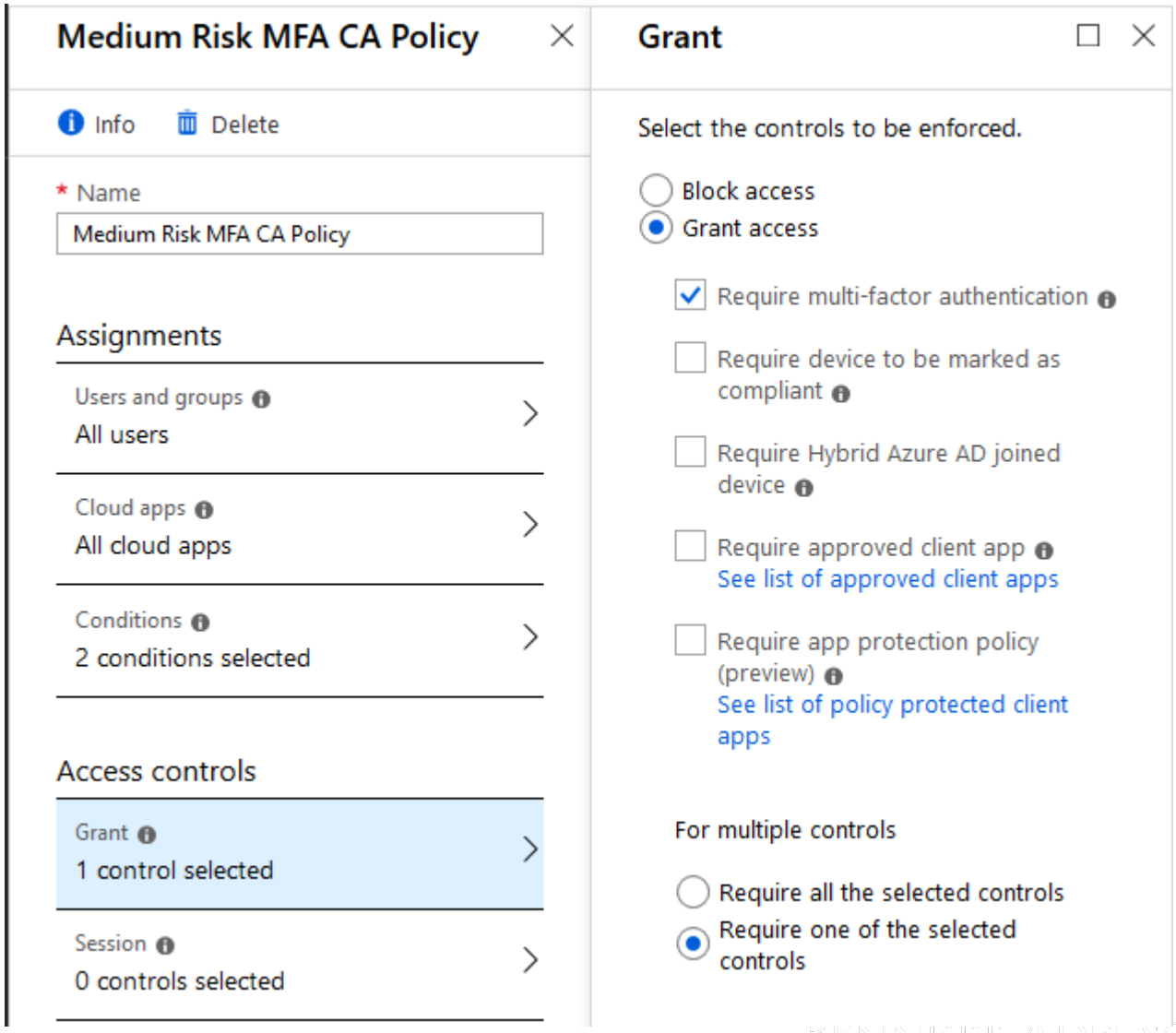
Conditional Access

- 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.

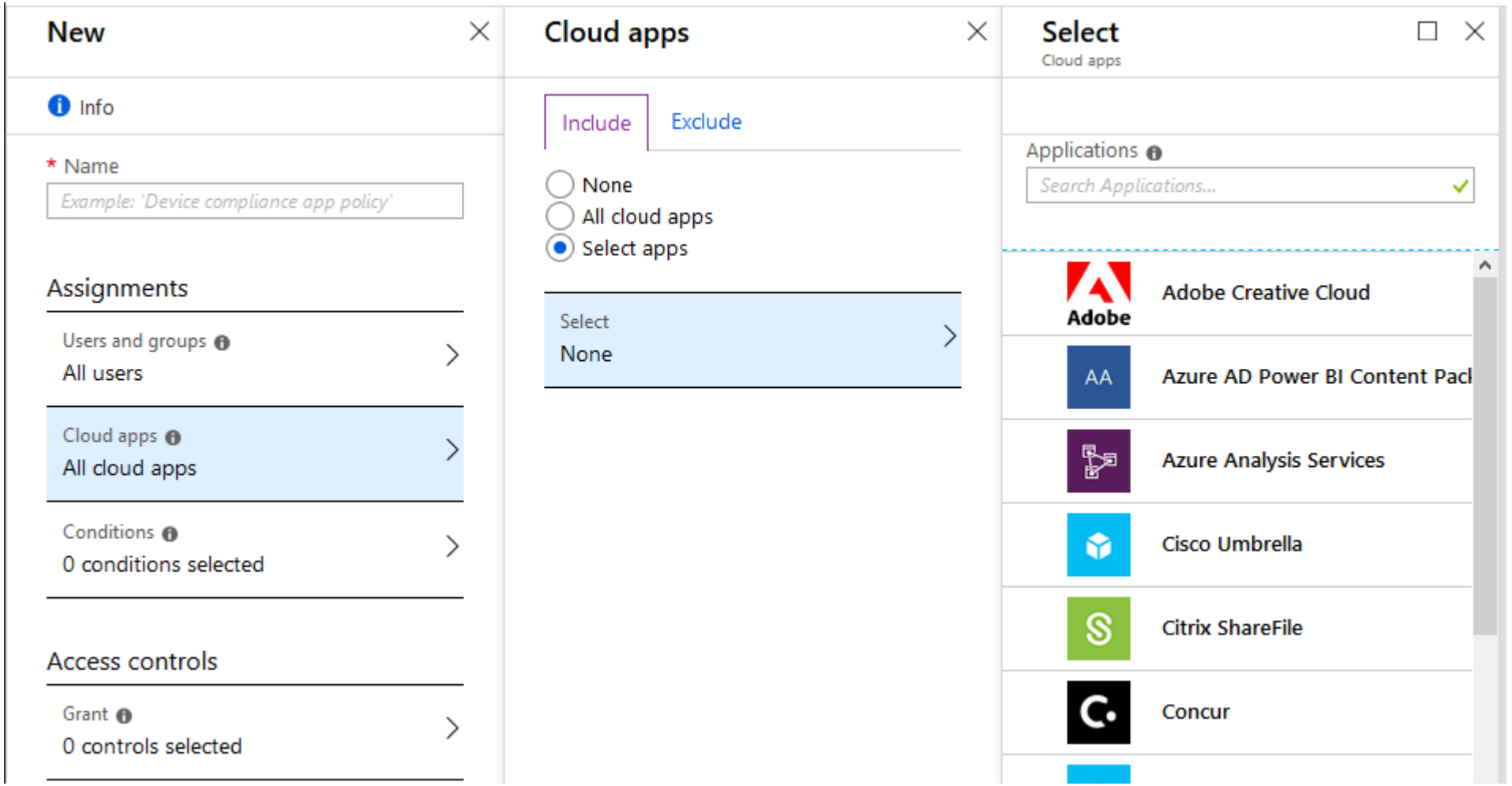
Conditional Access – Hybrid AD



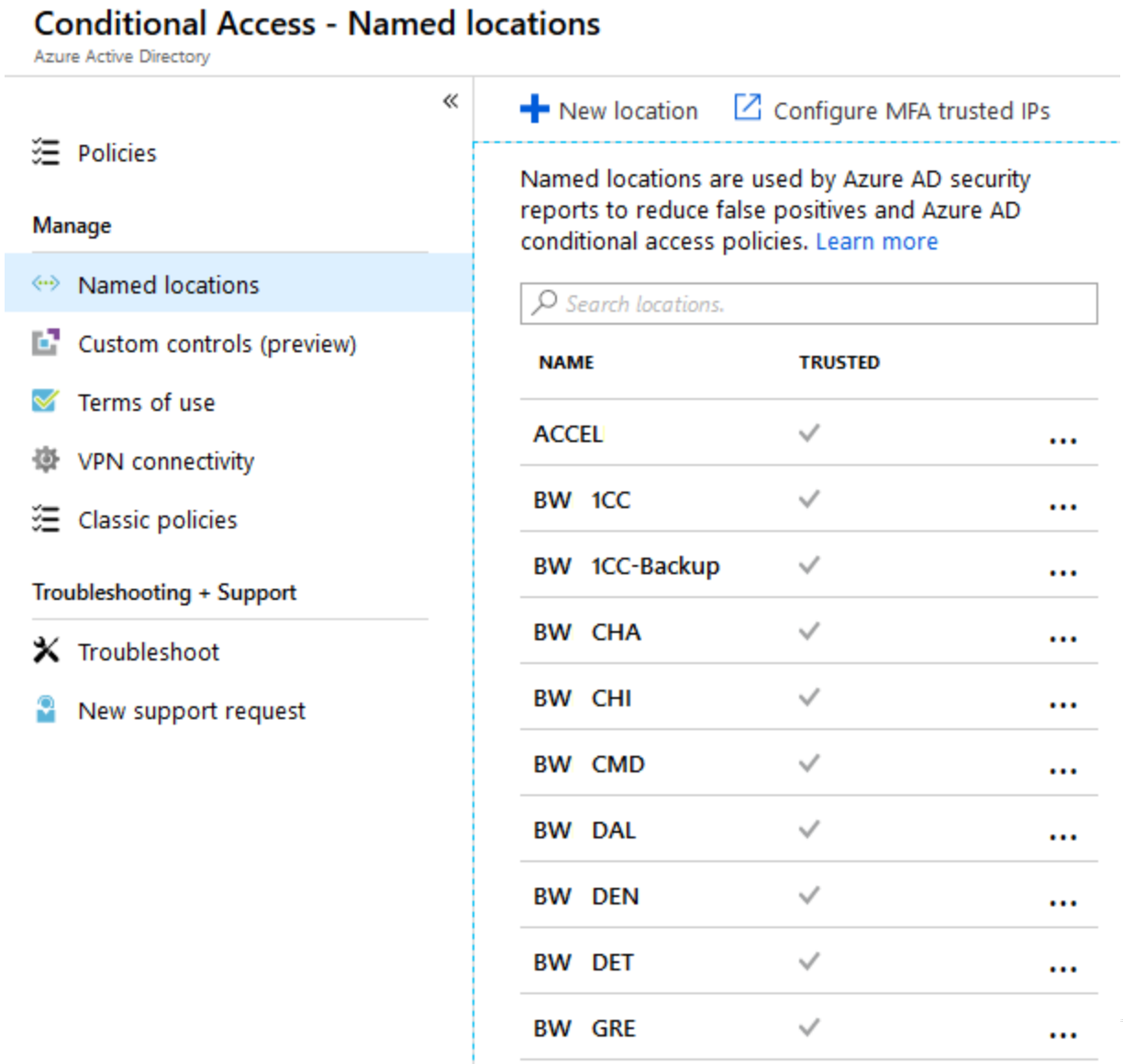
Conditional Access - MFA



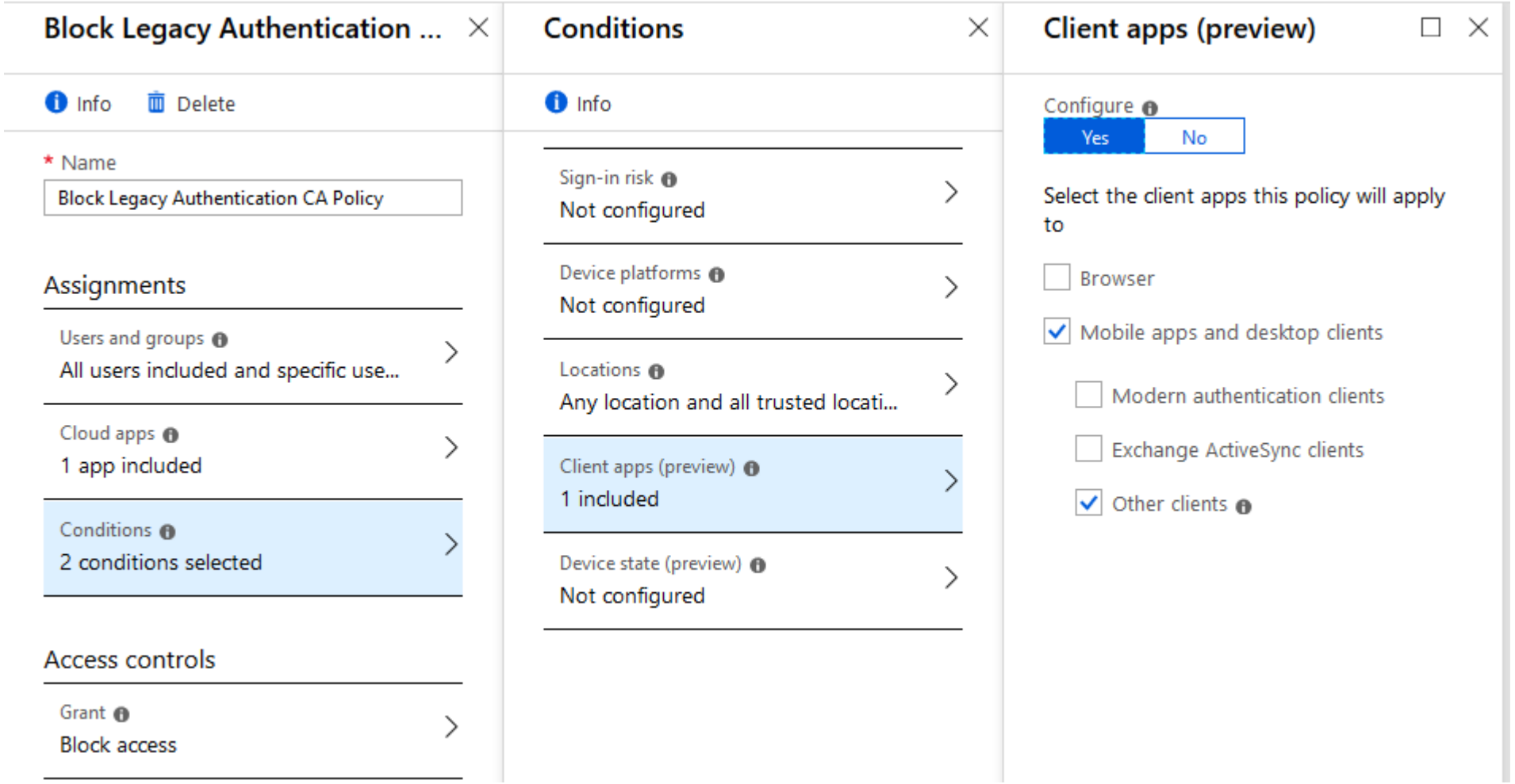
Conditional Access – Registered Apps



Conditional Access – Locations



Conditional Access – Modern Auth

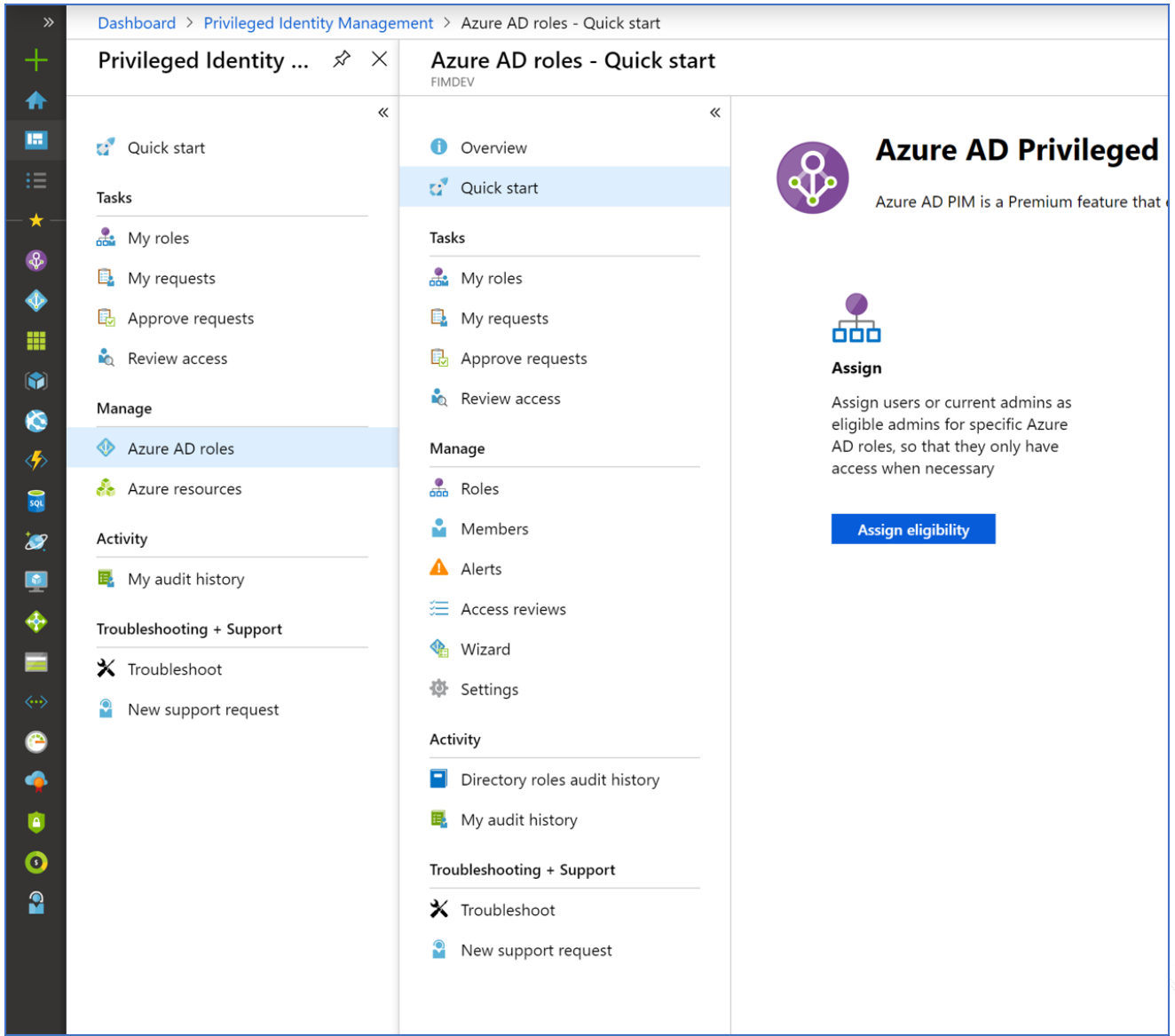


PIM & JIT

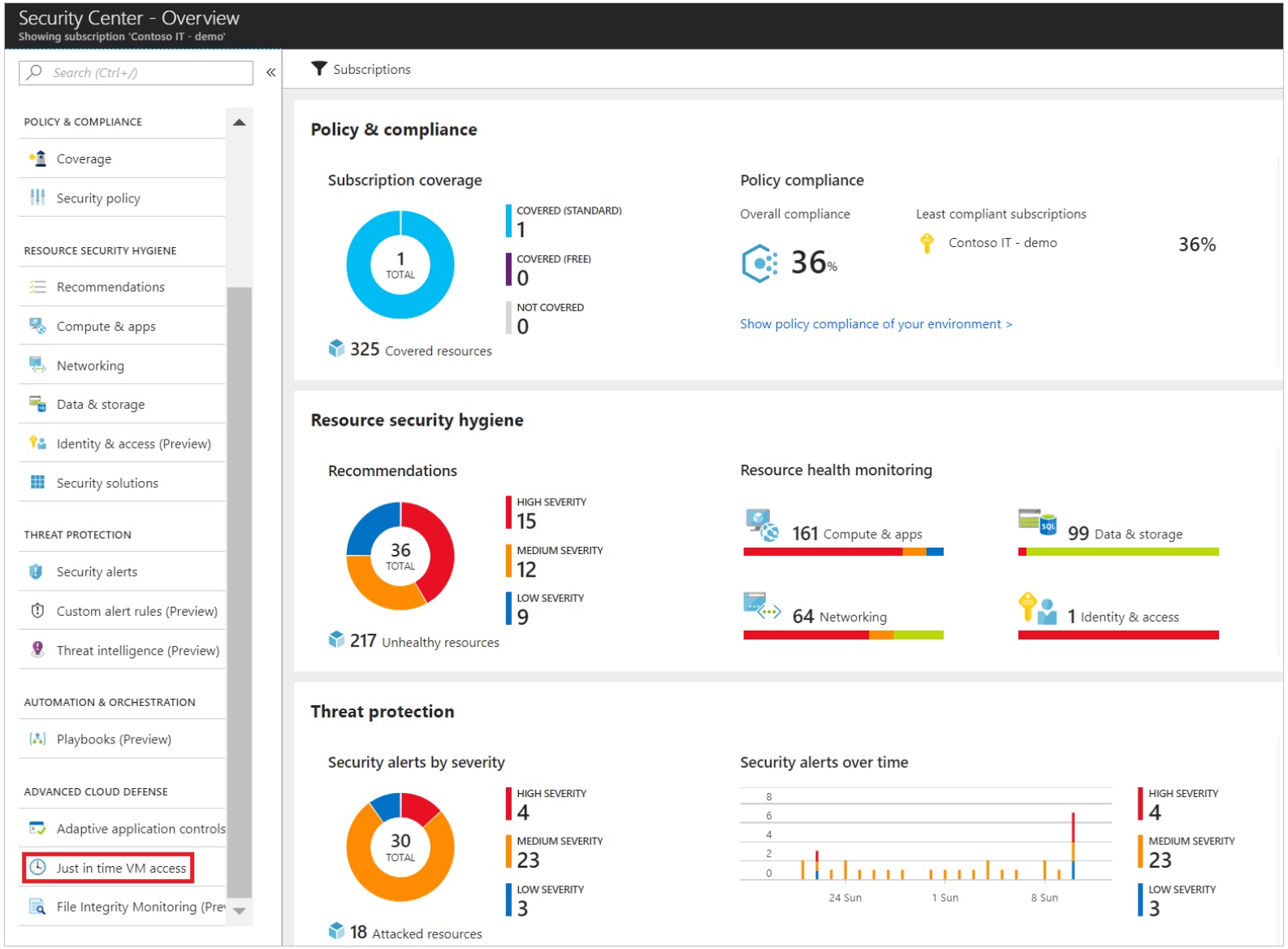
- Privileged Identity Management
  - Provide just-in-time privileged access to Azure AD and Azure resources
  - Assign time-bound access to resources using start and end dates
  - Require approval to activate privileged roles
  - Enforce multi-factor authentication to activate any role

- 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

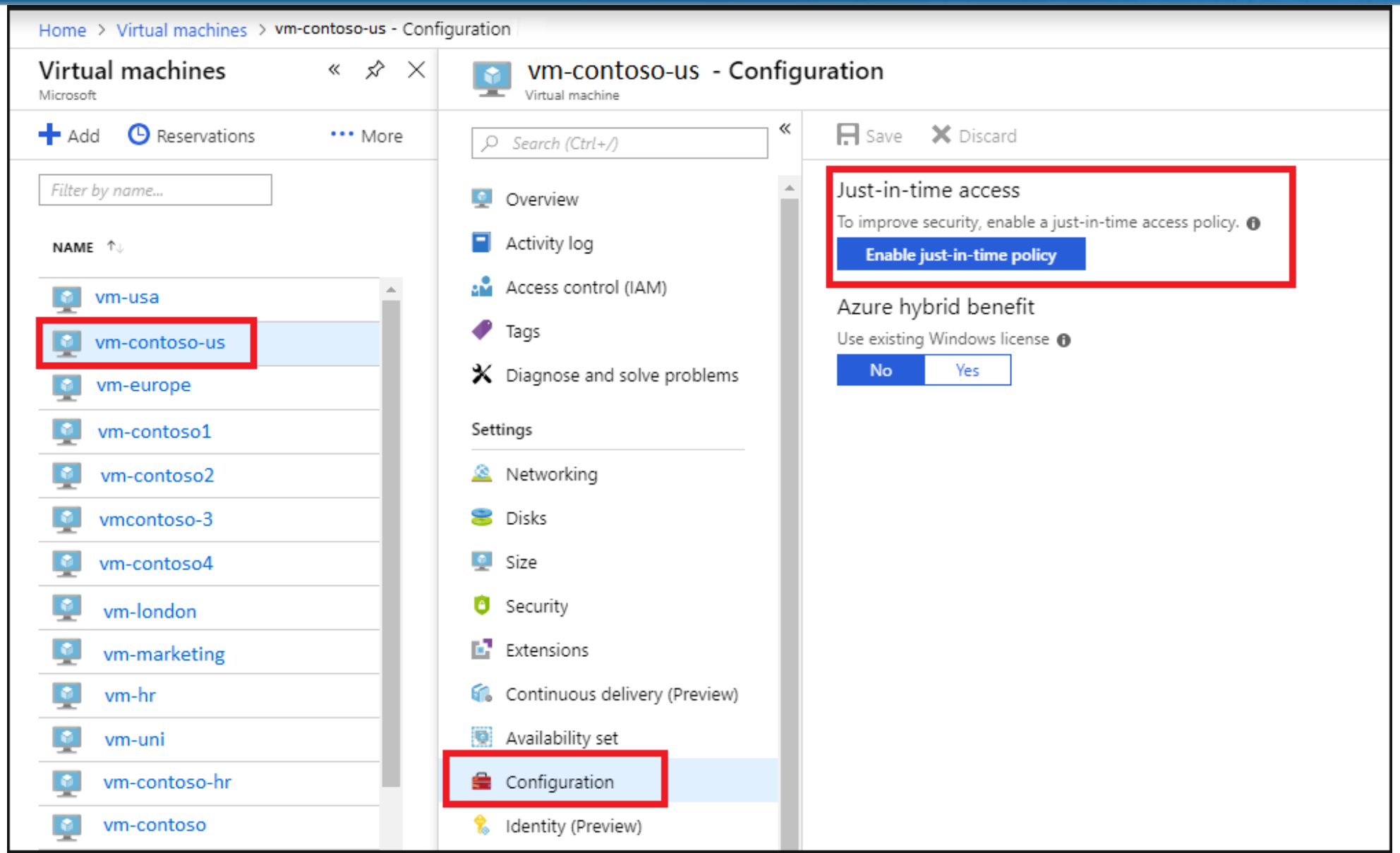
Privileged Identity Management



Just in Time


Security Center - Overview
Showing subscription 'Contoso IT - demo'
Search (Ctrl+/)
Subscriptions
POLICY & COMPLIANCE
Coverage
Security policy
RESOURCE SECURITY HYGIENE
Recommendations
Compute & apps
Networking
Data & storage
Identity & access (Preview)
Security solutions
THREAT PROTECTION
Security alerts
Custom alert rules (Preview)
Threat intelligence (Preview)
AUTOMATION & ORCHESTRATION
Playbooks (Preview)
ADVANCED CLOUD DEFENSE
Adaptive application controls
Just in time VM access
File Integrity Monitoring (Pre
Policy & compliance
Subscription coverage
1 TOTAL
COVERED (STANDARD) 1
COVERED (FREE) 0
NOT COVERED 0
325 Covered resources
Policy compliance
Overall compliance
36%
Least compliant subscriptions
Contoso IT - demo 36%
Show policy compliance of your environment >
Resource security hygiene
Recommendations
36 TOTAL
HIGH SEVERITY 15
MEDIUM SEVERITY 12
LOW SEVERITY 9
217 Unhealthy resources
Resource health monitoring
161 Compute & apps
99 Data & storage
64 Networking
1 Identity & access
Threat protection
Security alerts by severity
30 TOTAL
HIGH SEVERITY 4
MEDIUM SEVERITY 23
LOW SEVERITY 3
18 Attacked resources
Security alerts over time
8
6
4
2
0
24 Sun
1 Sun
8 Sun
HIGH SEVERITY 4
MEDIUM SEVERITY 23
LOW SEVERITY 3

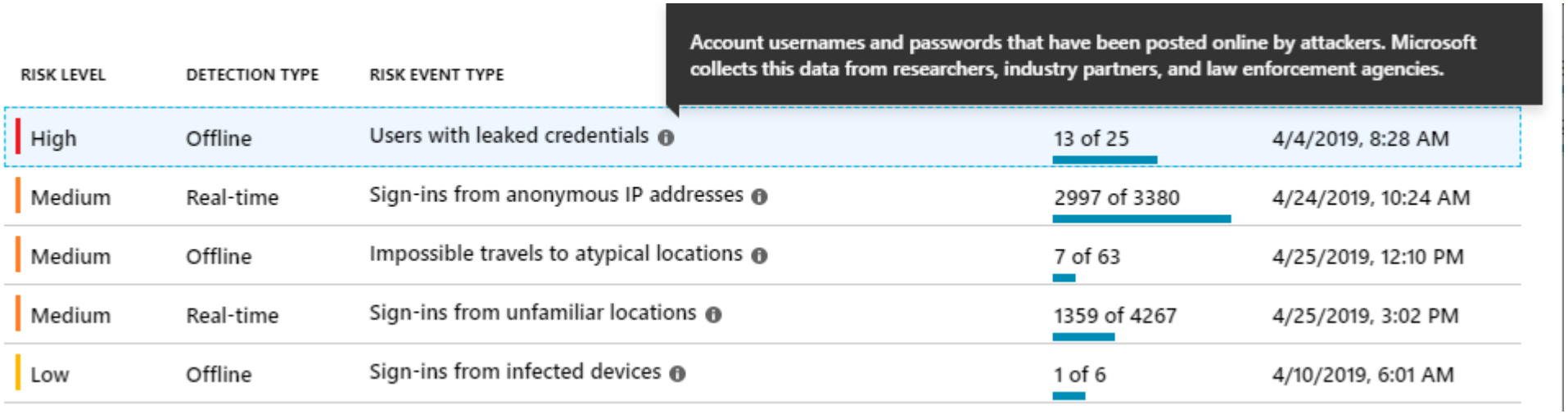
Just in Time


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+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Disks
Size
Security
Extensions
Continuous delivery (Preview)
Availability set
Configuration
Identity (Preview)
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

Azure Active Directory

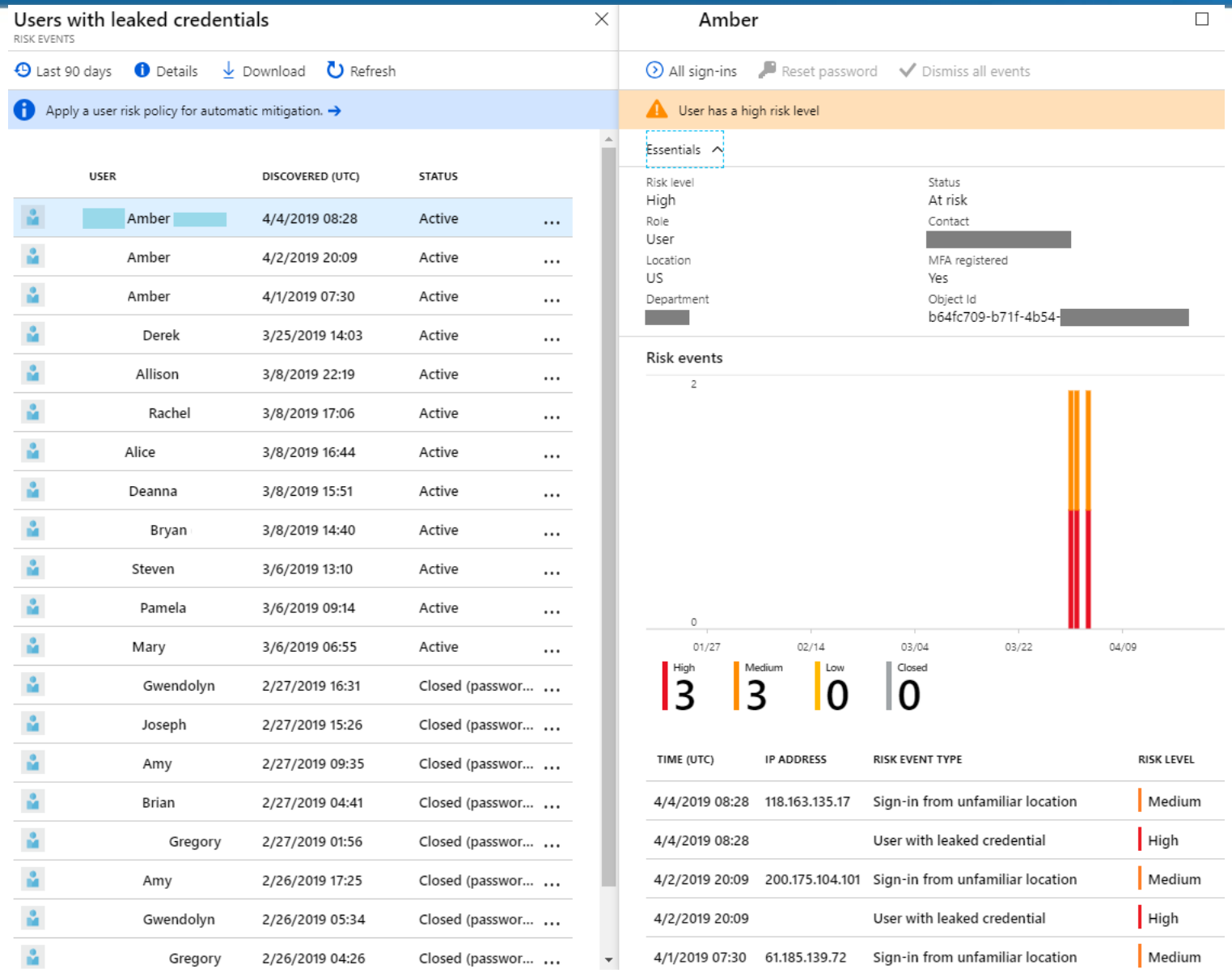
- Risky Logins
- Password protection

Azure Active Directory – Risky Logins

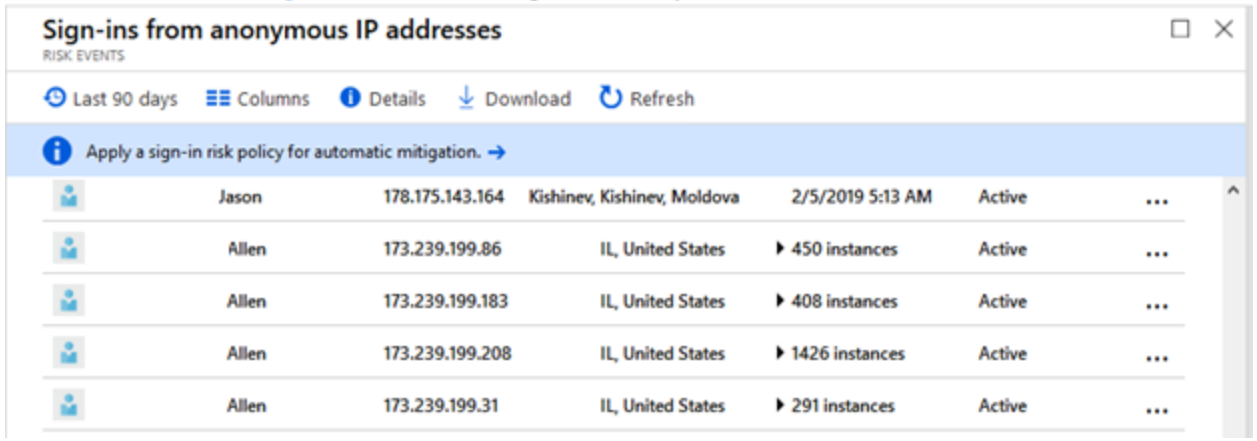


RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE		
High	Offline	Users with leaked credentials	13 of 25	4/4/2019, 8:28 AM
Medium	Real-time	Sign-ins from anonymous IP addresses	2997 of 3380	4/24/2019, 10:24 AM
Medium	Offline	Impossible travels to atypical locations	7 of 63	4/25/2019, 12:10 PM
Medium	Real-time	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

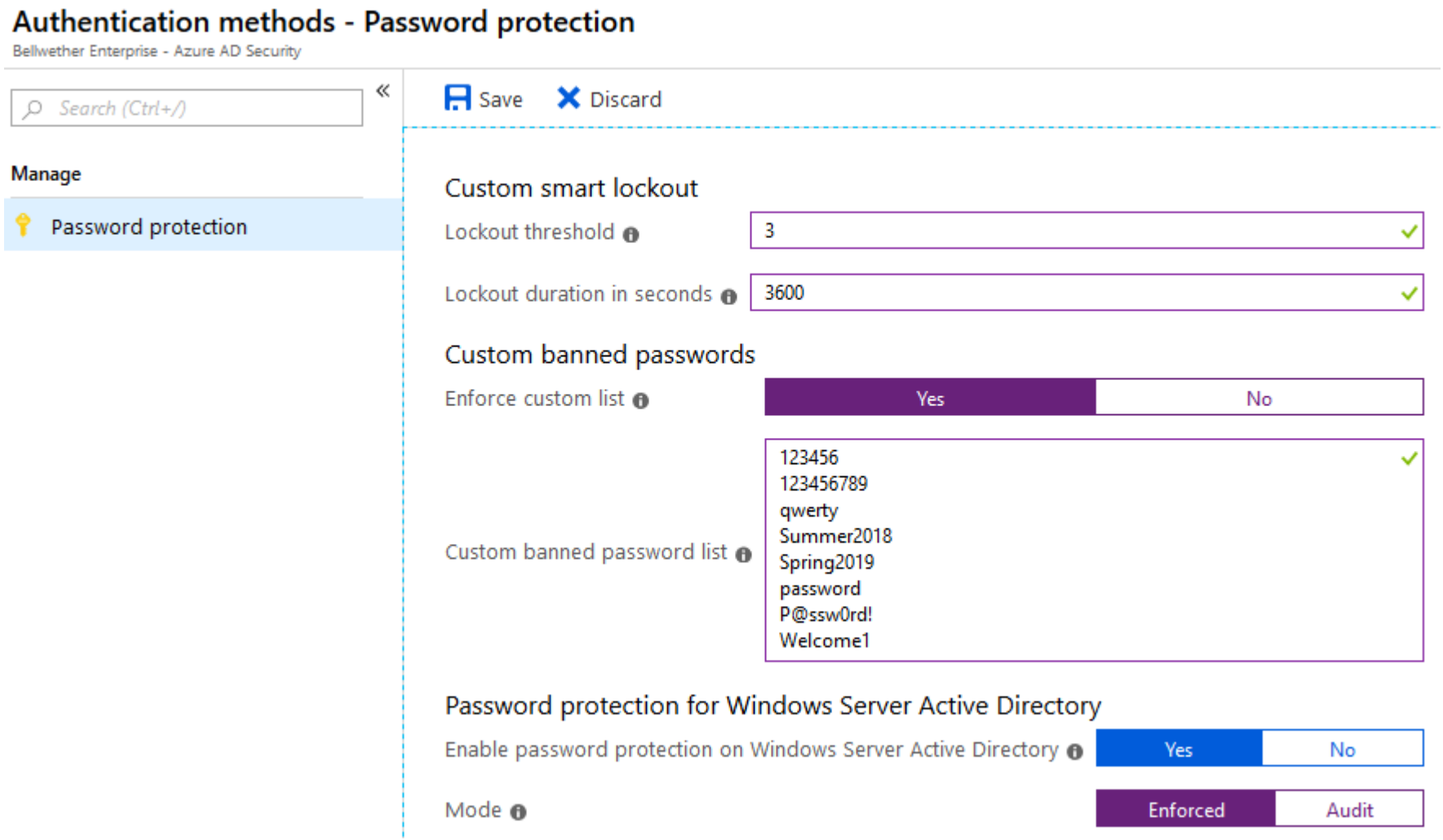
Azure Active Directory – Risky Logins



Azure Active Directory – Risky Logins



Azure Active Directory – Password Protection



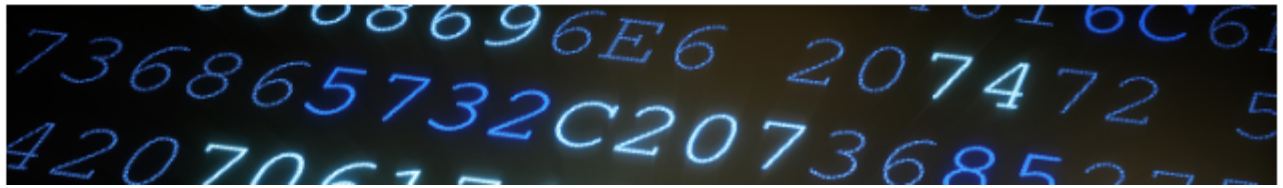
Azure Active Directory – Password Protection

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

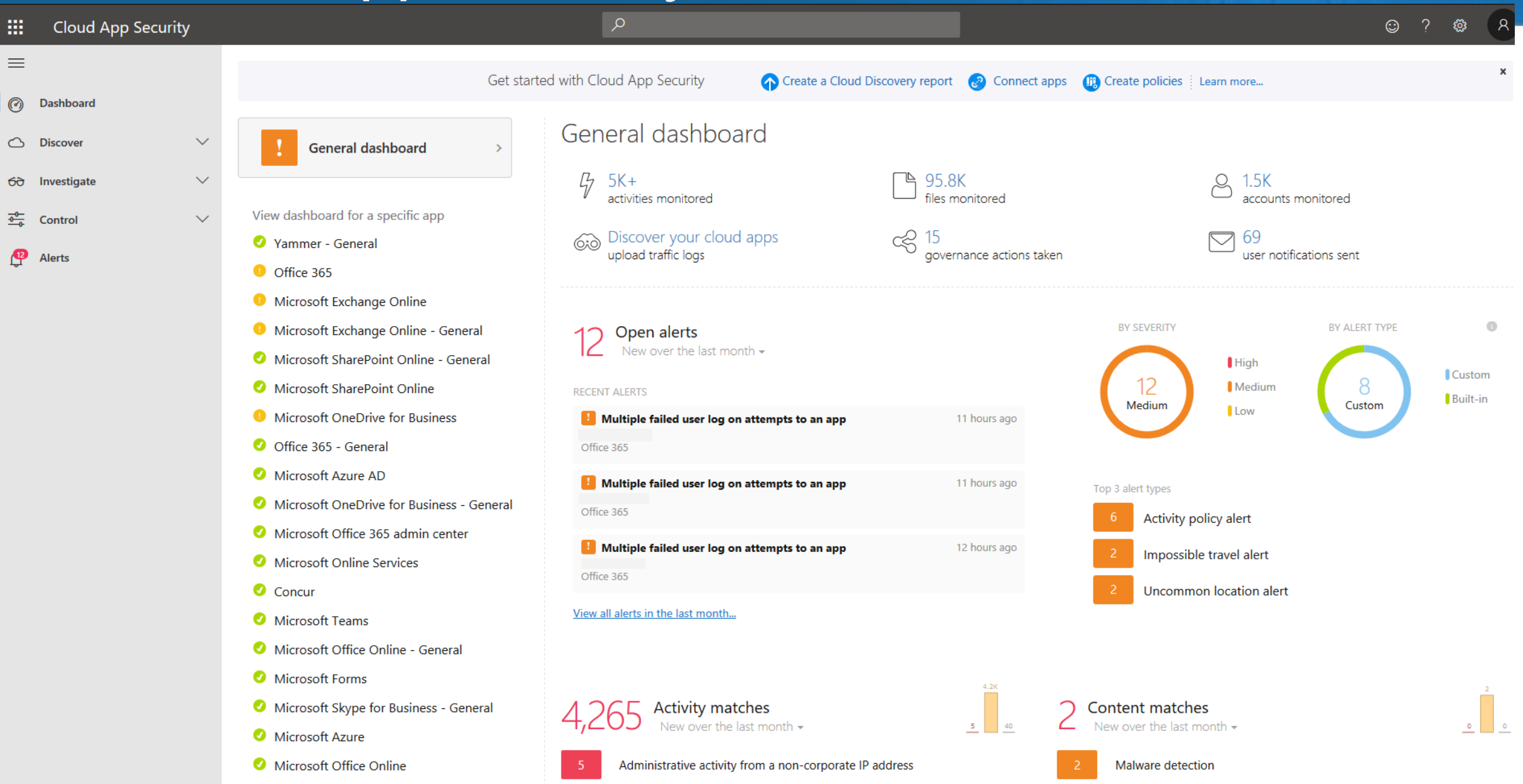


https://bit.ly/ncsc-survey

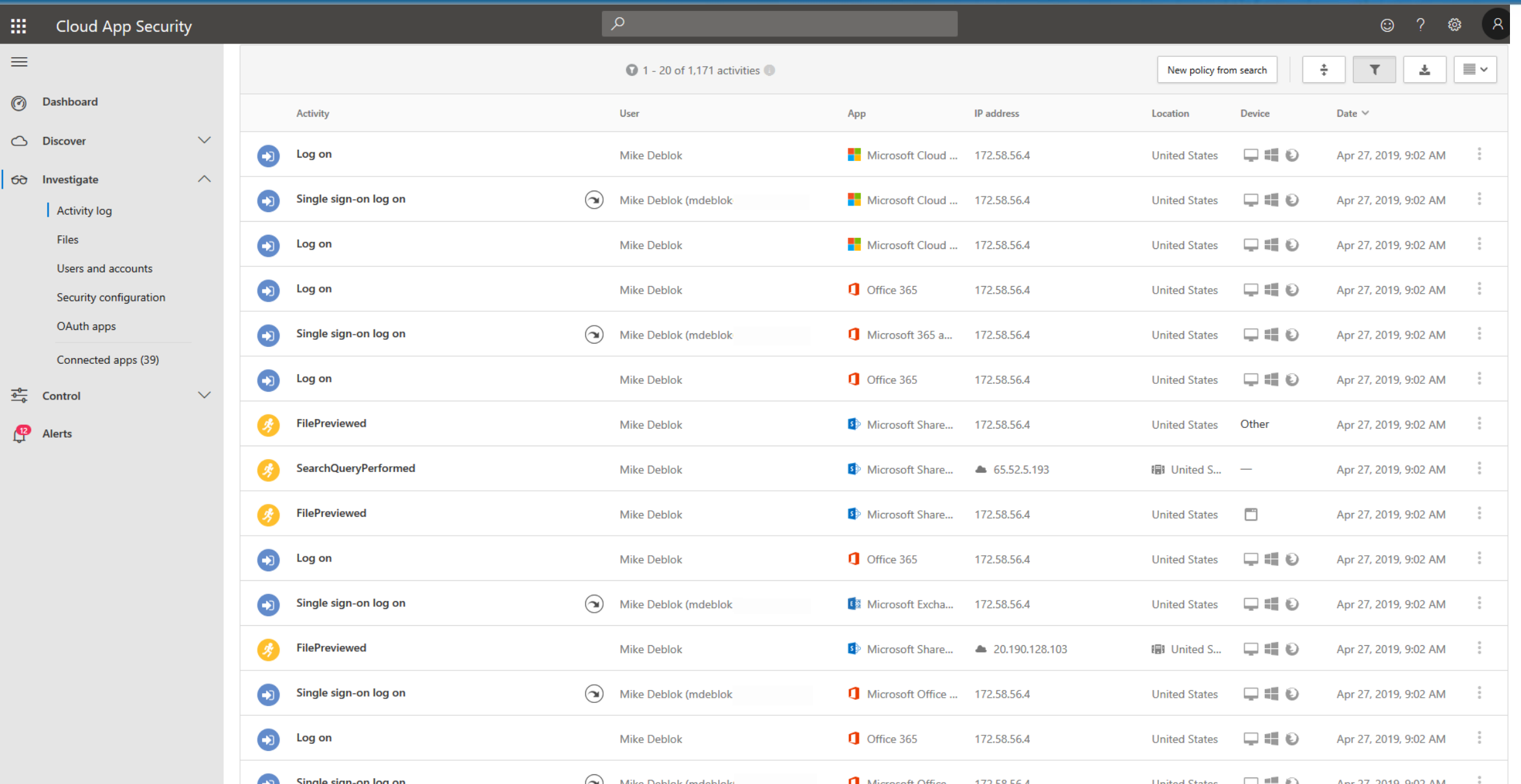
Azure Active Directory – Password Protection

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)
111111 (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)

Cloud App Security



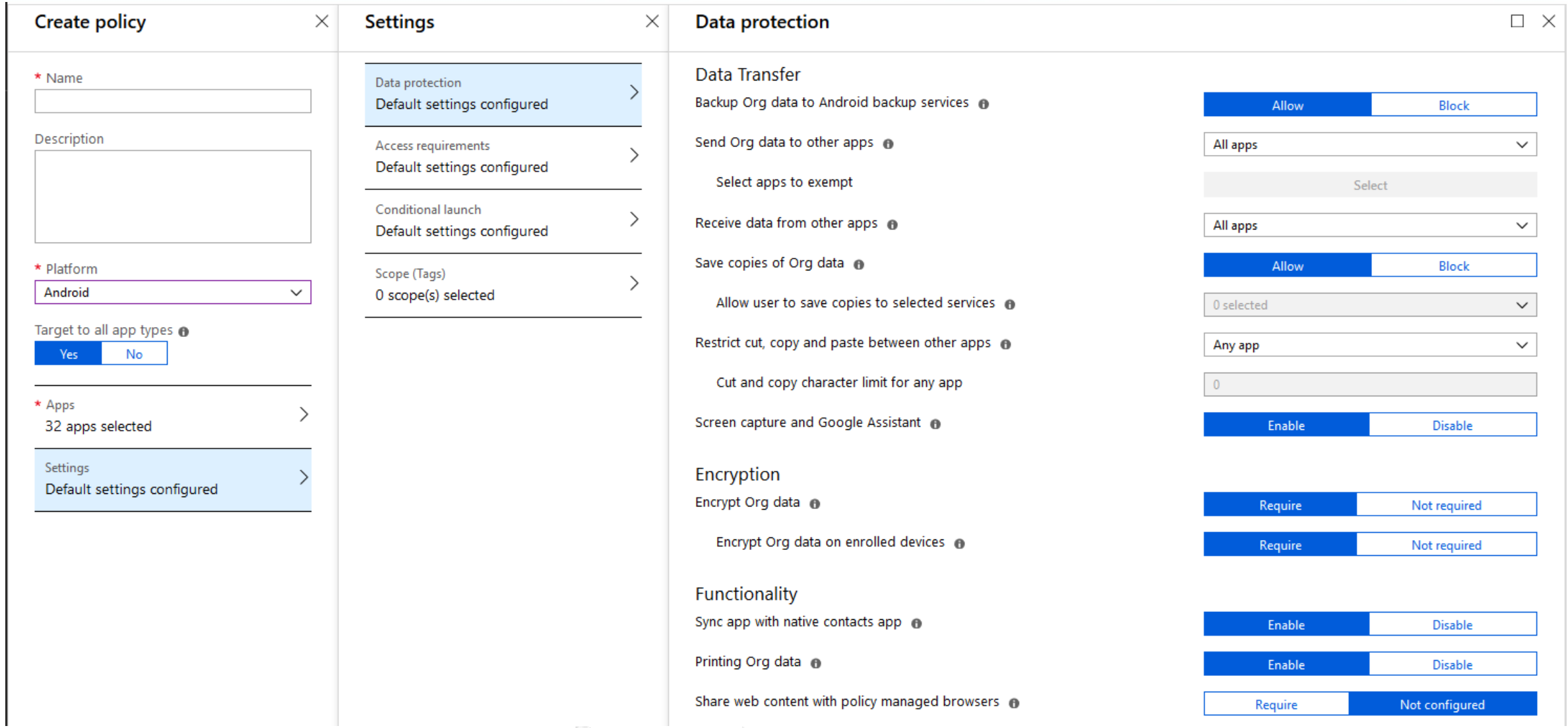
Cloud App Security



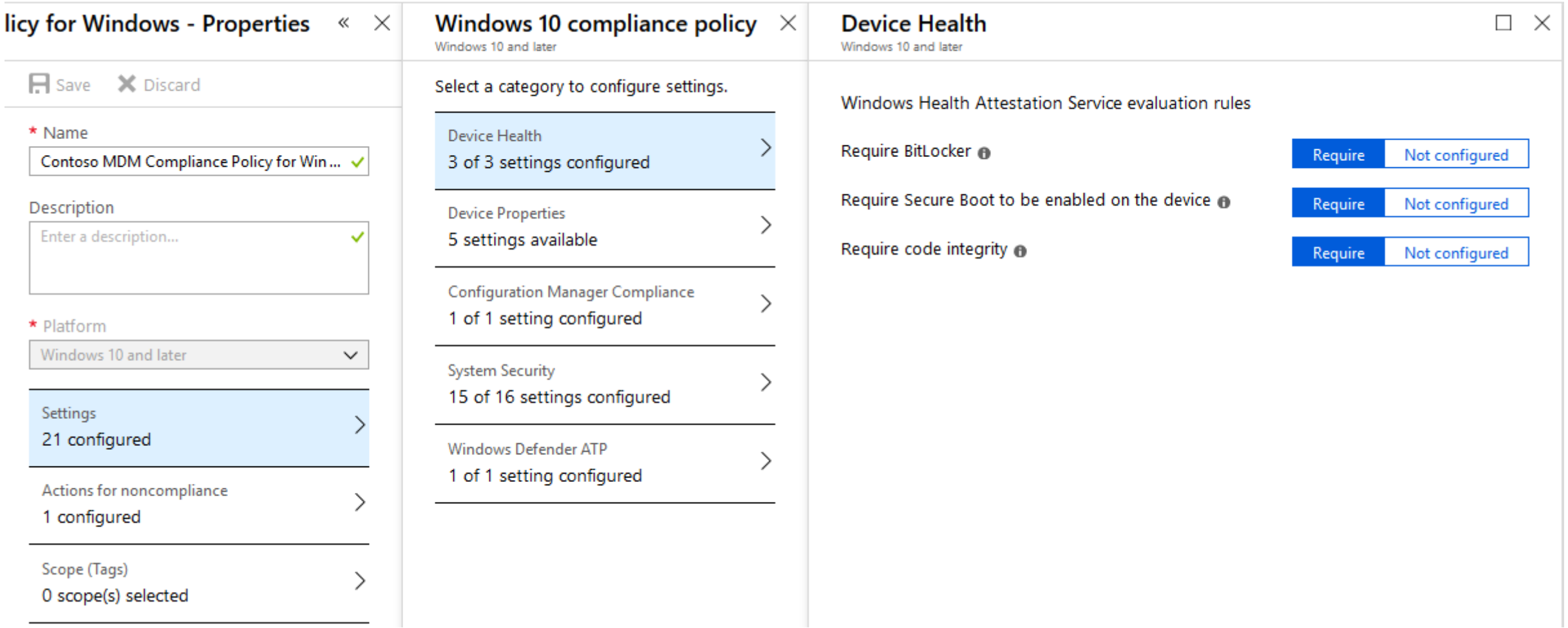
Policies

- Apps
- Devices

Policies – Apps



Policies – Devices



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 ☺

Thank You

BENNETT ADELSON℠