Post-Compromise Persistence and Detection within IdPs

Chaim Sanders

Head of Security Operations

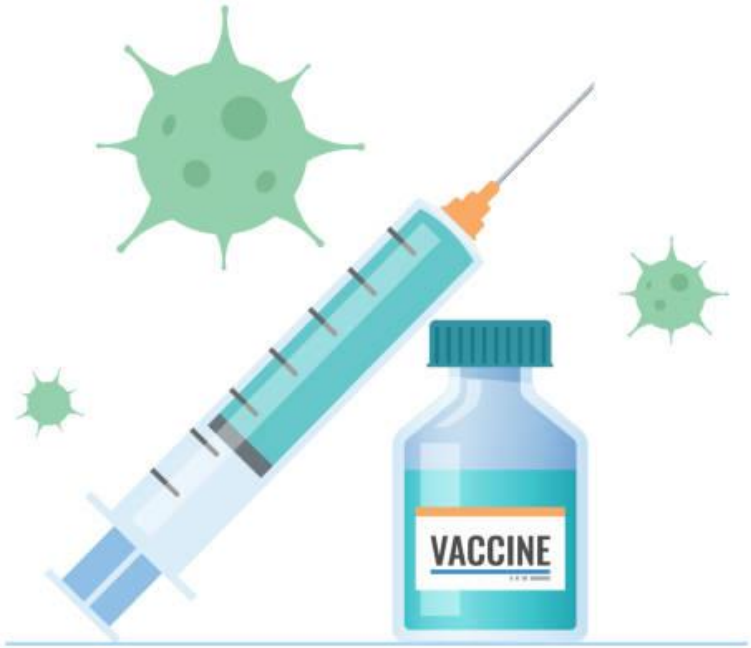
Lyft

IdPs Are Critical

- IdPs such as Okta and Azure are driving centralized security decisions but also centralizing risk.
- What is your response to a potential compromise of these environments?
- SSO providers will espouse the ‘Shared Responsibility Model’, how does this play in?

Prevention

- Reduce admin users
- Strong Authentication
  - Regularly Password Phishing
  - MFA Phishing
  - Physical Theft
  - Session Theft
  - Compromised Endpoints
- Reups for high risk activities would resolve lots of these



Persistence/Detection

- Delegated Credentials
- Delegated Upstream Authentication
- Directory Persistence
- Selective Policy Enforcement
- Application Persistence
- Upstream Integrations
- IdP Specific Vectors

Delegated Credentials

Approach	Okta	Azure
API Tokens	**UI**, **Logs**, **Detection**	N/A
Client Cred OAuth App	**UI**, **Logs**, **Detection**	**UI**, **Logs**, **Detection**
Trusted Origin	**UI**, **Logs**, **Detection**	(N/A, App Proxy)

Okta Demo of CORS to Application with API Access

Preview Sandbox: This is a preview of next week's release. See a problem? File a case or visit our support site.

okta

Search for people, apps and groups

- Dashboard
- Directory
- Customizations
- Applications
- Security
  - General
  - HealthInsight
  - Authenticators
  - Authentication Policies
  - Global Session Policy
  - Profile Enrollment
  - Identity Providers
  - Delegated Authentication

API

Help

Authorization Servers | Tokens | Trusted Origins

Add Origin URLs to redirect users to custom pages or enable browser-based applications to access Okta APIs from JavaScript (CORS).

+ Add origin

Search...

Filters

- All
- CORS
- Redirect
- iFrame embed

Name	Origin URL	Type	Actions

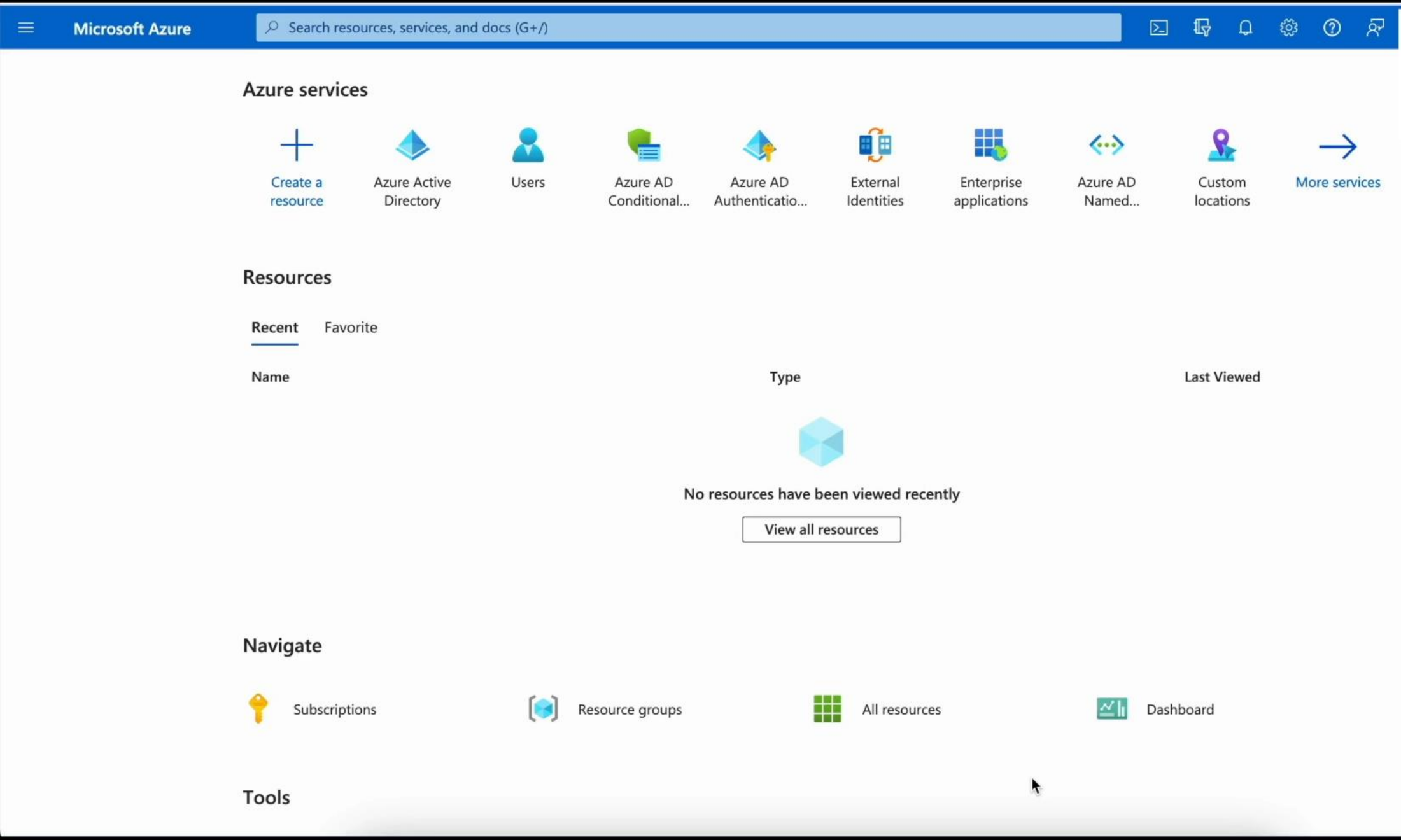
Nothing to show

Try searching or filtering

Delegated Upstream Authentication

Approach	Okta	Azure
AD/LDAP/RADIUS	UI, Logs, Detection	UI, Logs, Detection
Upstream IdP	UI, Logs, Detection	UI, Logs, Detection
Custom Factors/Controls	UI, Logs, Detection	UI, Logs, Detection

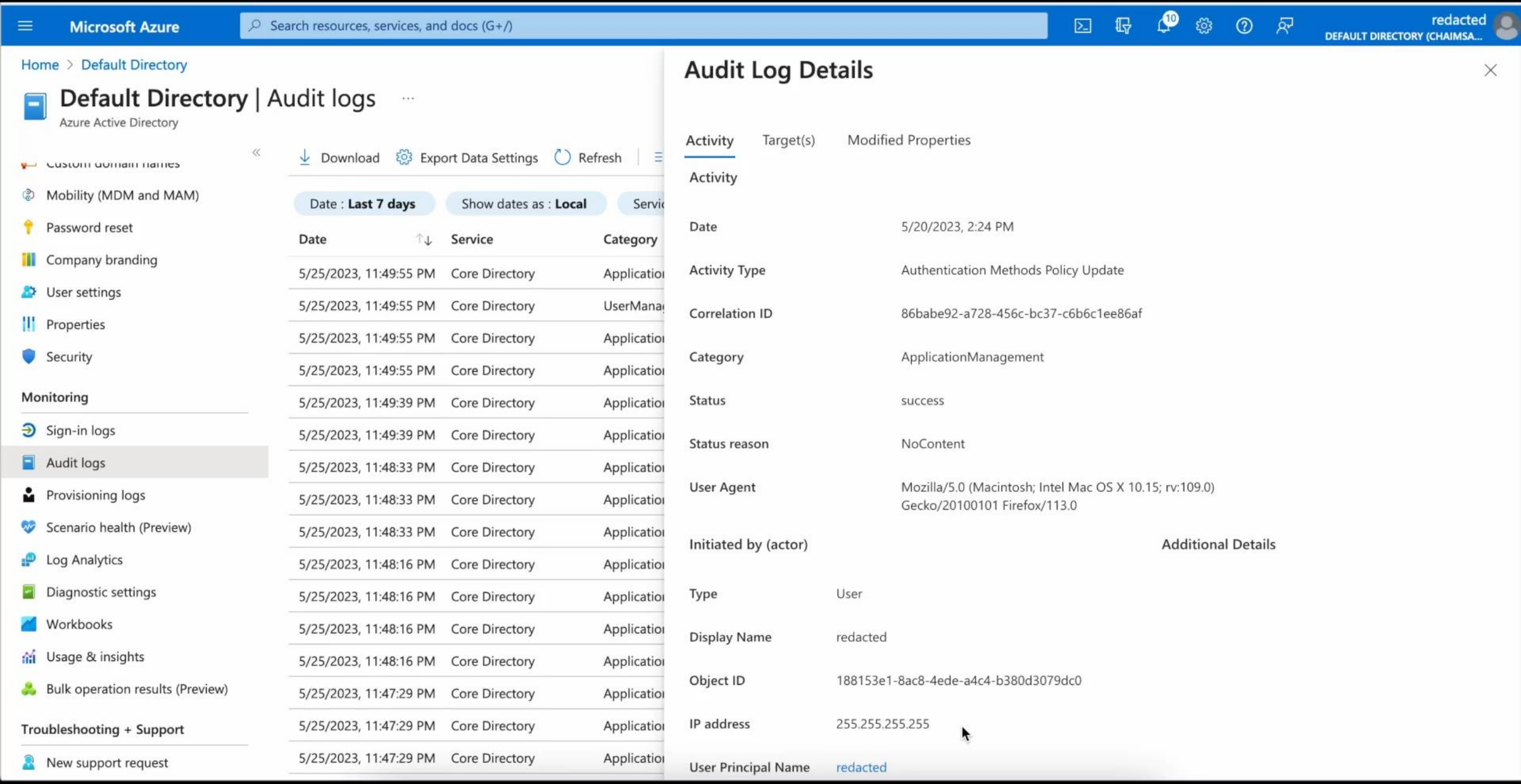
Azure Demo with Upstream IDP enrollment


Microsoft Azure
Search resources, services, and docs (G+/)
Azure services
Create a resource
Azure Active Directory
Users
Azure AD Conditional...
Azure AD Authenticatio...
External Identities
Enterprise applications
Azure AD Named...
Custom locations
More services
Resources
Recent
Favorite
Name
Type
Last Viewed
No resources have been viewed recently
View all resources
Navigate
Subscriptions
Resource groups
All resources
Dashboard
Tools

Directory Persistence

Approach	Okta	Azure
User Creation	UI, Logs, Detection	UI, Logs, Detection
Group Modification	UI, Logs, Detection	UI, Logs, Detection
Factor Modification	UI, Logs, Detection	UI, Logs*, Detection

Azure Factor Modification Logs


Microsoft Azure
Search resources, services, and docs (G+/)
redacted
DEFAULT DIRECTORY (CHAIMSA...
Home > Default Directory
Default Directory | Audit logs
Azure Active Directory
Download
Export Data Settings
Refresh
Date : Last 7 days
Show dates as : Local
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Sign-in logs
Audit logs
Provisioning logs
Scenario health (Preview)
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Date
Service
Category
5/25/2023, 11:49:55 PM Core Directory
5/25/2023, 11:49:55 PM Core Directory
5/25/2023, 11:49:55 PM Core Directory
5/25/2023, 11:49:55 PM Core Directory
5/25/2023, 11:49:39 PM Core Directory
5/25/2023, 11:49:39 PM Core Directory
5/25/2023, 11:48:33 PM Core Directory
5/25/2023, 11:48:33 PM Core Directory
5/25/2023, 11:48:33 PM Core Directory
5/25/2023, 11:48:16 PM Core Directory
5/25/2023, 11:48:16 PM Core Directory
5/25/2023, 11:48:16 PM Core Directory
5/25/2023, 11:48:16 PM Core Directory
5/25/2023, 11:47:29 PM Core Directory
5/25/2023, 11:47:29 PM Core Directory
5/25/2023, 11:47:29 PM Core Directory
Audit Log Details
Activity
Target(s)
Modified Properties
Activity
Date 5/20/2023, 2:24 PM
Activity Type Authentication Methods Policy Update
Correlation ID 86babe92-a728-456c-bc37-c6b6c1ee86af
Category ApplicationManagement
Status success
Status reason NoContent
User Agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/113.0
Initiated by (actor)
Additional Details
Type User
Display Name redacted
Object ID 188153e1-8ac8-4ede-a4c4-b380d3079dc0
IP address 255.255.255.255
User Principal Name redacted

Selective Policy Enforcement

Approach	Okta	Azure
Global Session Policy	UI, Logs, Detection	N/A
Auth Policy	UI*, Logs*, Detection	UI*, Logs*, Detection
Enrollment Policies	UI, Logs, Detection	UI*, Logs*, Detection
Network Policy	UI, Logs, Detection	UI, Logs, Detection

Okta Auth Policy Modification

Preview Sandbox: This is a preview of next week's release. See a problem? File a case or visit our support site.

okta

Search for people, apps and groups

chaim

- Dashboard
- Directory
- Customizations
- Applications
- Security
  - General
  - HealthInsight
  - Authenticators
  - Authentication Policies
  - Global Session Policy
  - Profile Enrollment
  - Identity Providers
  - Delegated Authentication

← Back to all Authentication Policies

AWS Account Federation

Actions ▾ Help

Rules (2) Applications (1)

Add rule

Priority	Rule	Status	Actions
1	Require MFA	ENABLED	Actions ▾

IF Any request

THEN **Access:** Allowed with possession factor

Your org's authenticators that satisfy this requirement:

1 factor type

Duo Security or Duo Universal Prompt (IdP) or Okta Verify or Phone or

Application Persistence

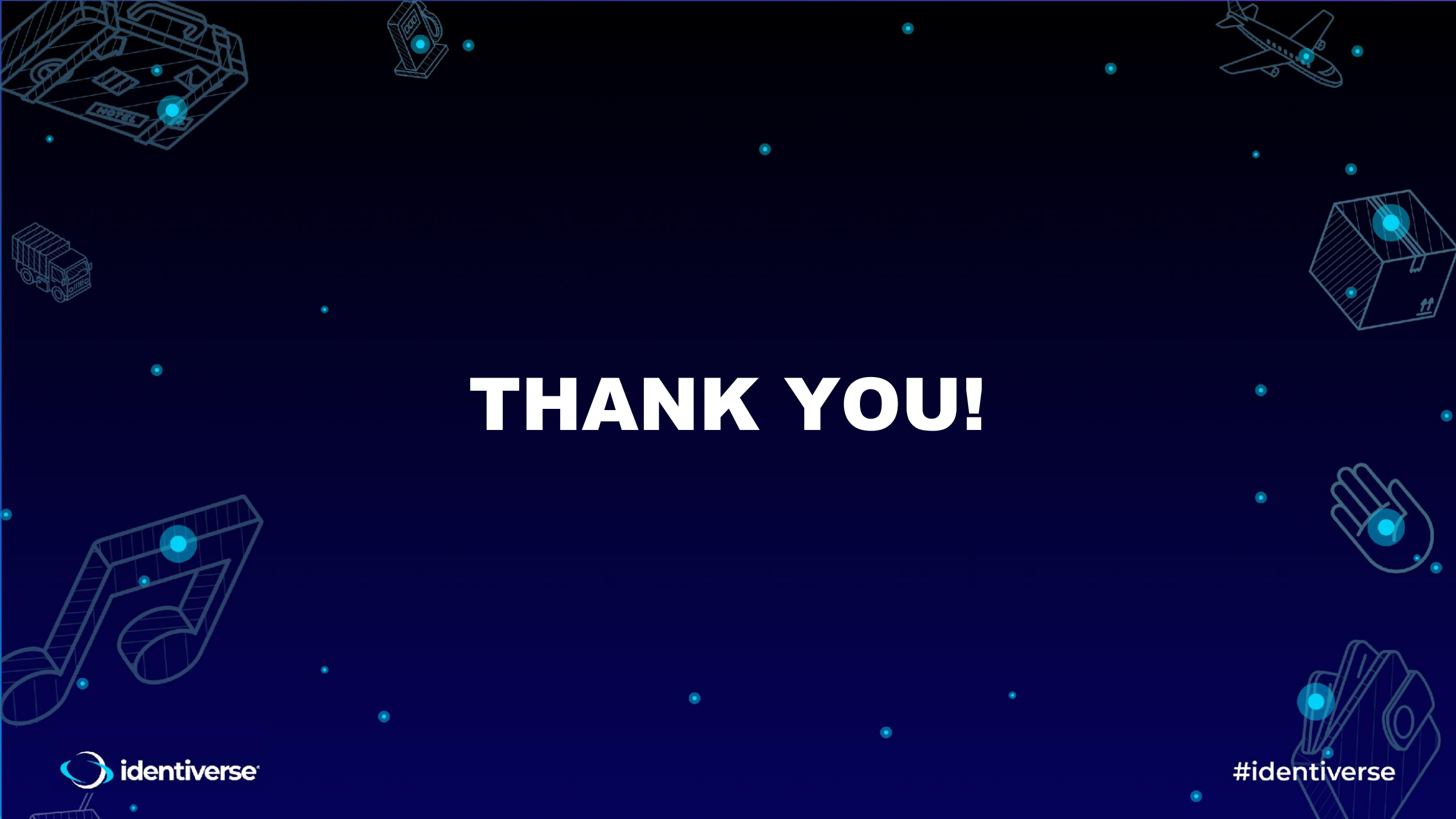
Approach	Okta	Azure
Apps with Integrations	UI, Logs, Detection	UI, Logs, Detection
Assign Users to High Value Apps	UI, Logs, Detection	UI, Logs, Detection
Apps with API Scopes	UI, Logs, Detection	UI, Logs, Detection

Upstream Integration

- IPaaS
  - Built in providers
  - External providers
- Web Hooks

IdP Specific Quirks

- Org2Org/Cross Tenant Access
- Self Service Registration
- SsoAcsURLOverride
- Undocumented AWS OAuth Support



THANK YOU!

identiverse

#identiverse