

WHAT'S NEW IN AZURE ACTIVE DIRECTORY?

IGNITE 2020 RECAP

Thomas Naunheim
6th October 2020



THOMAS NAUNHEIM

*Cloud Solutions Architect
Koblenz, Germany*



@Thomas_Live



www.cloud-architekt.net





IGNITE 2020 FOCUS

IDENTITY TODAY

AZURE AD ENHANCEMENTS
(FOR ZERO TRUST)

IDENTITY FEATURE UPDATES IN
AZURE AND SECURITY PRODUCTS

IDENTITY TRENDS AND FEATURES
(OF TOMMORROW)



AZURE AD ENHANCEMENTS (FOR ZERO TRUST)

SECURE REMOTE ACCESS



IDENTITY ATTACKS IN TIMES OF WORK FROM HOME / COVID-19

Attacks in August 2020:

9M high-risk enterprise sign-in attempts flagged

2M compromised accounts detected

5.8B attacker-driven sign-ins detected

300% increase in attacks over the past year



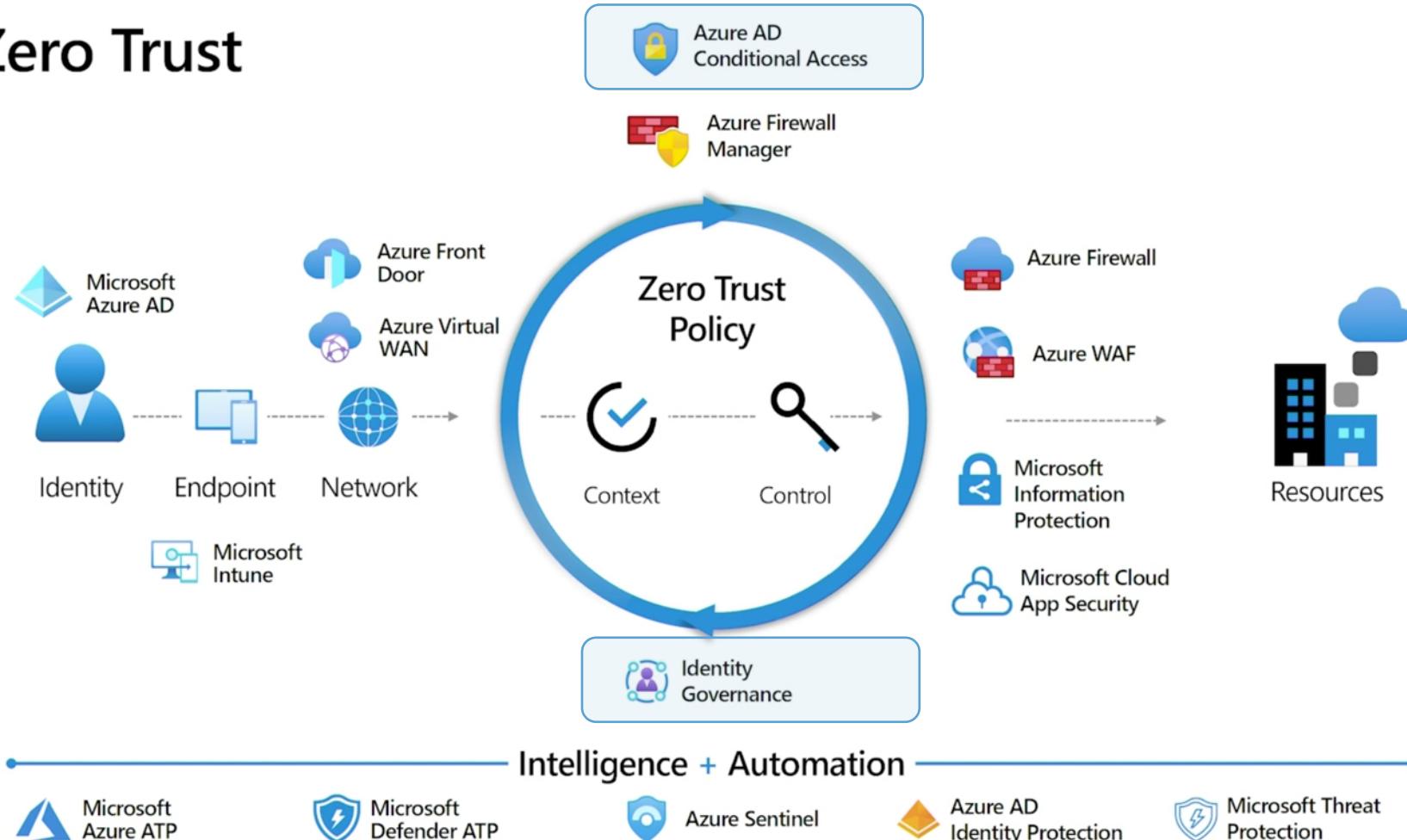
AZURE AD MONTHLY ACTIVE USERS

SHIFT TO CLOUD AUTHENTICATION

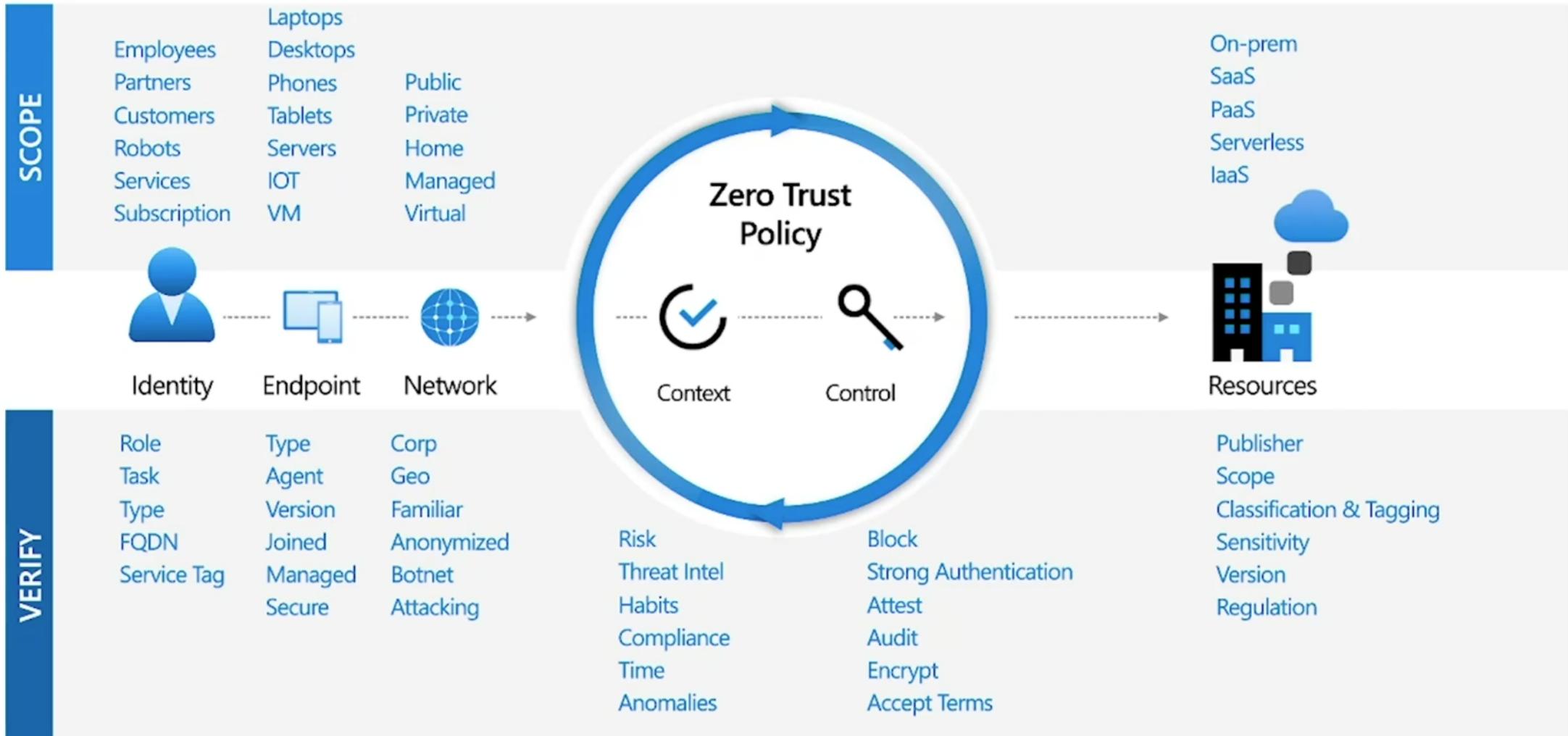
Source: ["Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity"](#)

NEVER TRUST, ALWAYS VERIFY

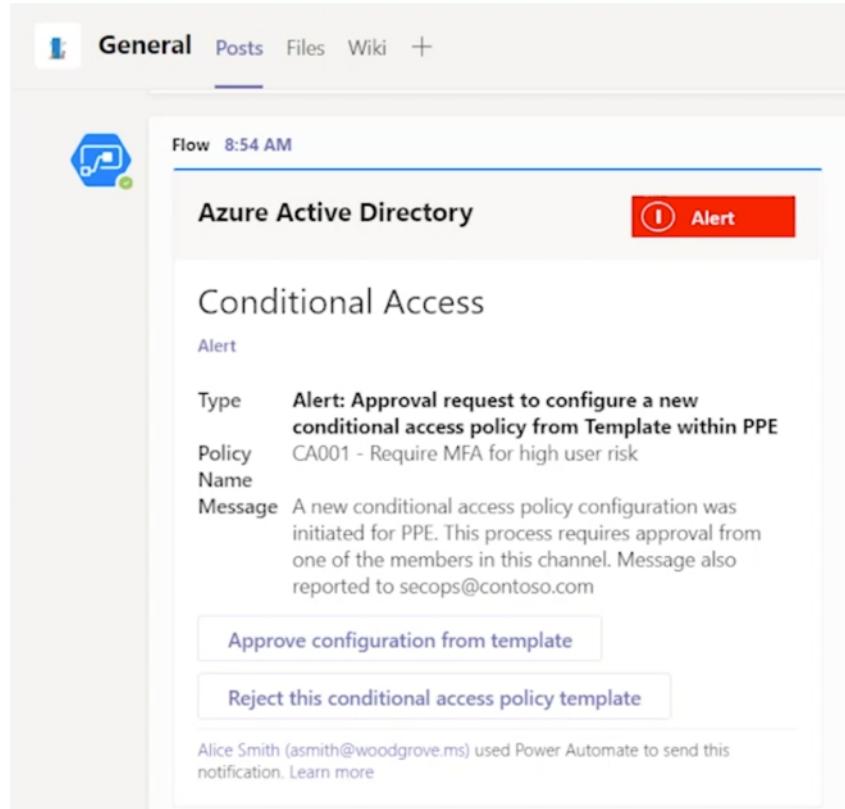
Zero Trust



SECURING IDENTITY WITH ZERO TRUST (ZT)



CONDITIONAL ACCESS AS ZT POLICY ENGINE



AUTOMATION VIA (GRAPH) API

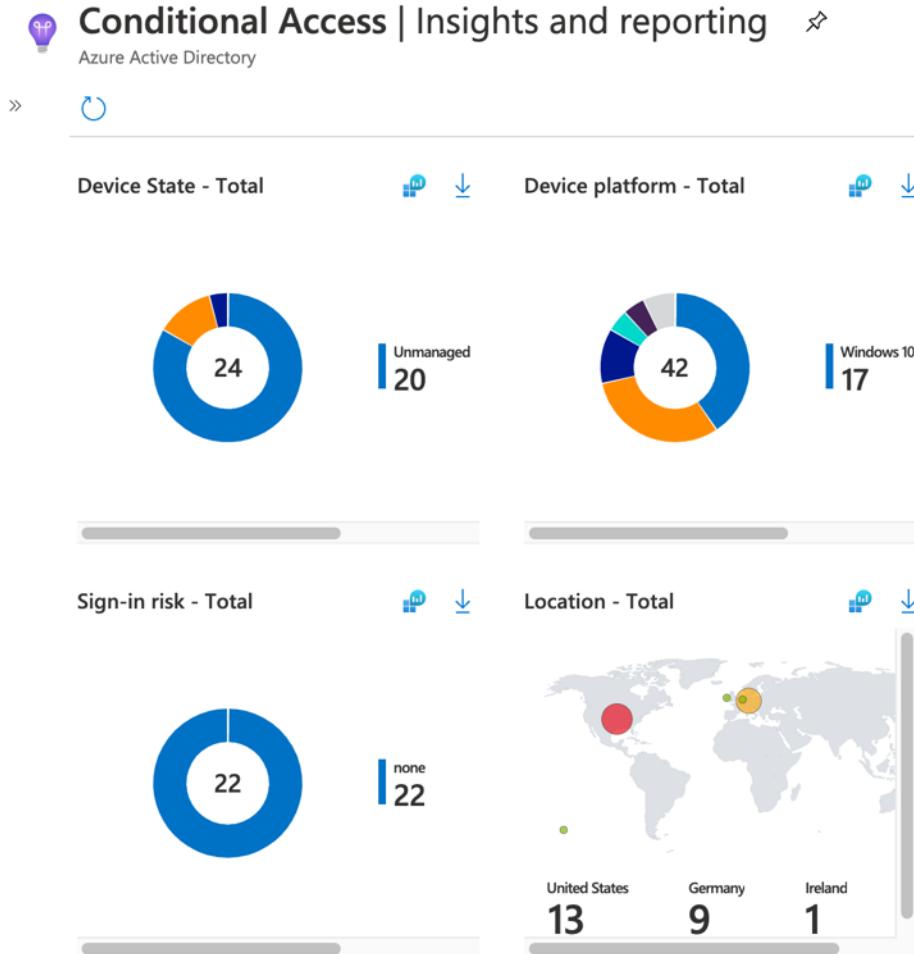
Conditional Access API in GA and
Samples for "Conditional Access as Code" by Microsoft:

- [GitHub Repo includes Samples](#)
- [Microsoft Docs: “Management of Lifecycle via API”](#)

ZT ENGINE FOR ALL TYPES OF USERS

- CA Policies and Identity Protection for Azure AD B2C / Azure AD “External Identities” (B2X)
 - Consideration of [Monthly Active User \(MAU\) Billing](#)

CONDITIONAL ACCESS AS ZT POLICY ENGINE



ADVANCED REPORTING AND INSIGHTS

Reporting and Analyses that helps to understand impact of CA Policies in your environment:

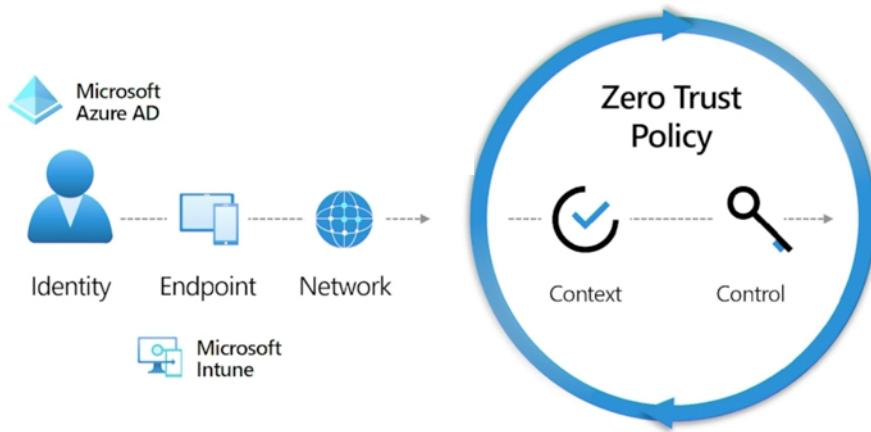
- Detailed Insights and Reporting
- Block legacy authentication in your organization

CONDITIONAL ACCESS POLICIES

Insights and Automation

LIVE DEMO

CONTINUOUS ACCESS EVALUATION (CAE)

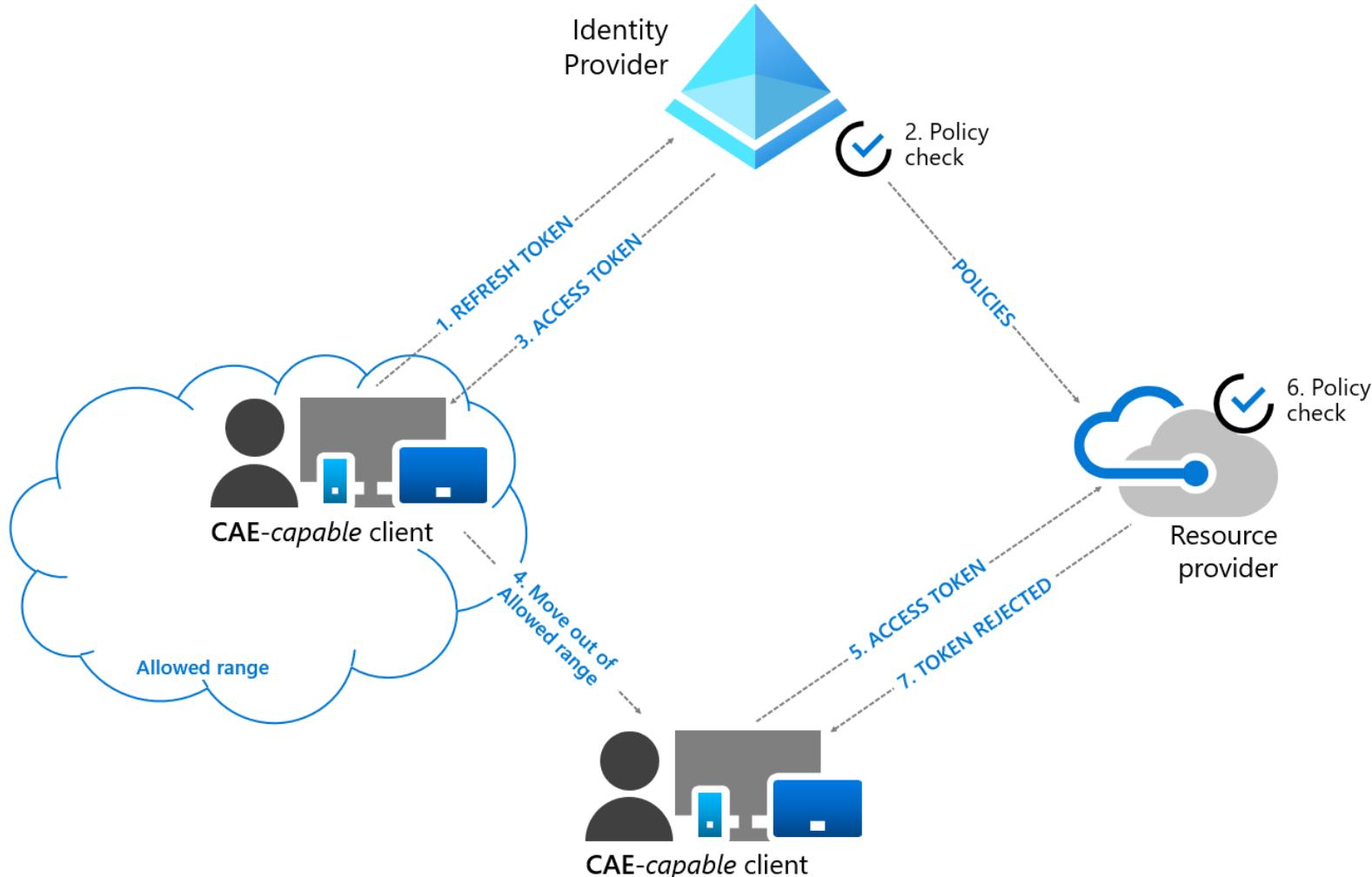


“ALWAYS VERIFY” EVALUATION/RESPONSE

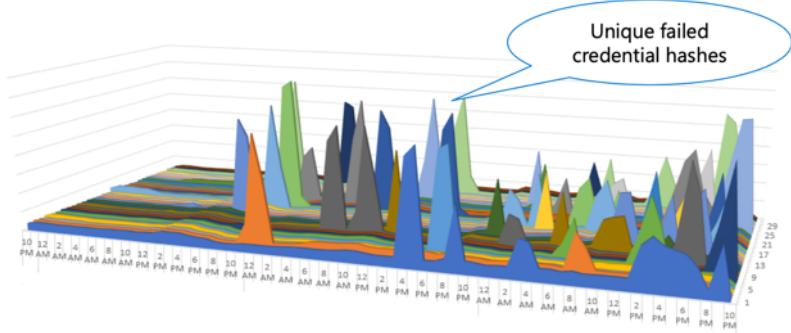
Reduce the lag between condition changes and policy (re)enforcement:

- Critical Event Evaluation (Examples):
 - Revocation all refresh tokens for a user (by Admin)
 - Client IP Address changes (outside of “Trusted Network”)
 - ...
- Current scenarios in public preview (resource provider support)
 - Exchange Online, SharePoint

CONTINUOUS ACCESS EVALUATION (CAE)



IDENTITY PROTECTION



Unusual activity

To let us know whether an unusual sign-in was safe, you can choose This was me or This wasn't me.



PASSWORD SPRAY ATTACKS

- 80 million attacks a day / 230% increase (this year)
- New Risk Type: “Smart Password Spray Detection”

GENERAL ENHANCEMENTS

- End User Feedback Integration
- Advanced APIs and Integration
- Session: The science behind Identity Protection

FINE-GRANTED POLICIES

- User-Risk as Condition, Password Change as Control

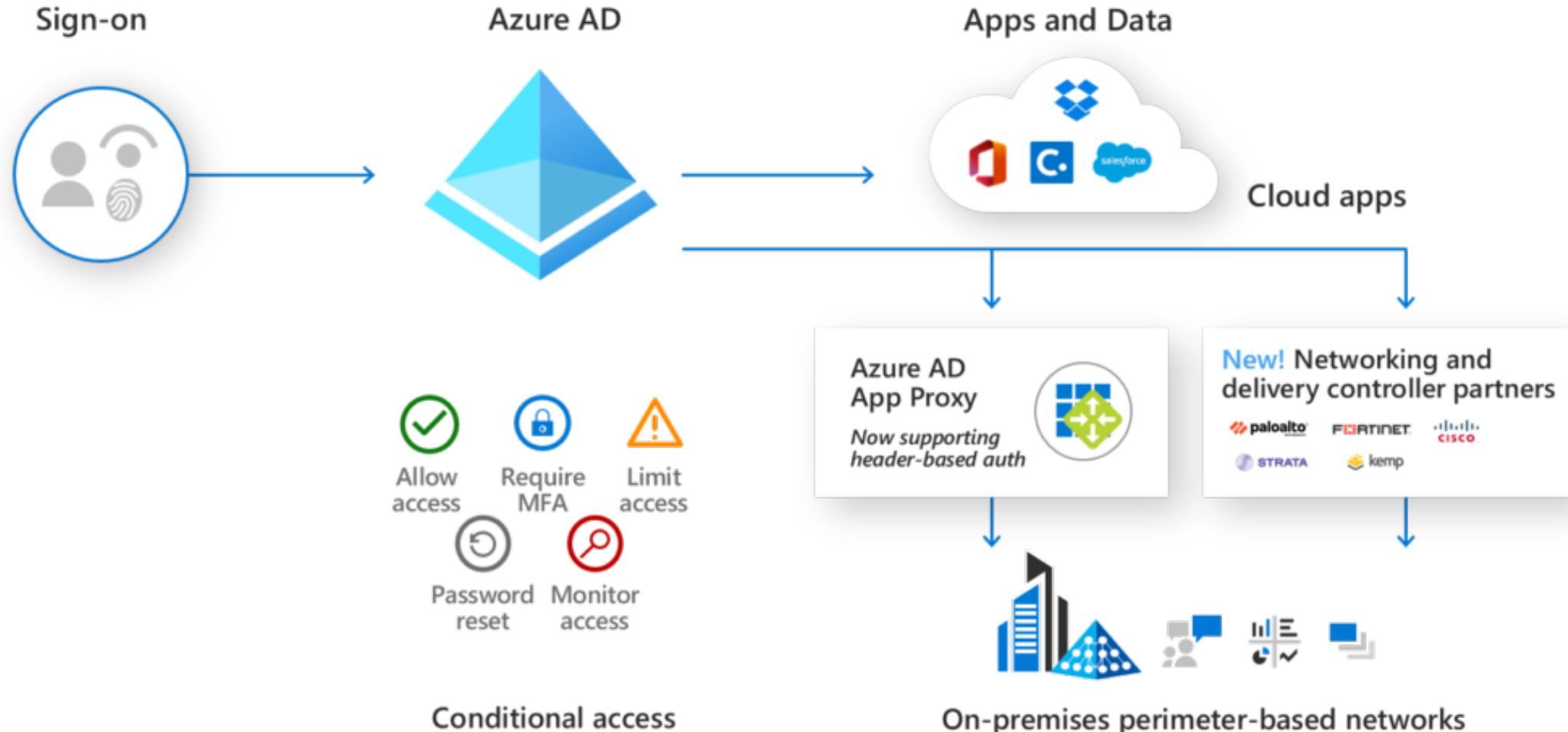
PROTECT YOUR DATA FROM MALICIOUS APPS

User Consent Policies / Report Suspicious Apps

Publisher Verification

LIVE DEMO

SECURE HYBRID ACCESS PARTNERS



SECURE HYBRID ACCESS PARTNERS



SUPPORT OF LEGACY ON-PREMISES APPS

Dashboard >

 Oracle EBS | Single sign-on 

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators (Pre...)
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

« Select a single sign-on method [Help me decide](#)

 **Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

 **SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

 **Password-based**
Password storage and replay using a web browser extension or mobile app.

 **Linked**
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

 **Windows Integrated Authentication**
Allows the Application Proxy Connectors permission in Active Directory to impersonate users to the published application.

 **Header-based**
Give users access and single sign-on to applications that use headers for authentication.

ADOPTION OF 3RD PARTY APPS

"UPGRADE TO THE CLOUD FOR IDENTITY – DECOMMISSION ON-PREMISES SYSTEMS"

- Session: "Save money by securing access to all your apps with Azure AD"
 - Integrating all your apps with Azure AD (<https://aka.ms/FiveStepAppIntegration>)
 - ADFS to Azure AD App Migration Tools

Summary

✓ This application is ready to migrate to Azure AD

We've detected on-premises settings for this relying party that can be migrated to a new Azure AD enterprise application. You won't be redirected to it until you say so.

- No additional WS-Federation endpoints were found.
- AllowedAuthenticationClassReferences is not set up.
- AlwaysRequireAuthentication is not set up.
- AutoUpdateEnabled is not set up.
- No Additional Claim Providers were configured.
- Relying Party is not set to encrypt claims.
- Relying Party is not set to encrypt name ID

Stats	Numbers	%
Total Number of Applications	73	
Applications that can't be migrated	13	17.81%
Application with Warnings	16	21.92%
Applications that can be migrated	44	60.27%
Percentage of apps that can be migrated	60.27%	

ENTERPRISE SSO PLUG-IN FOR APPLE DEVICES (IOS/IPADOS)

- Seamless SSO experience (across all apps by supporting Apple Enterprise SSO feature)

AZURE AD IMPROVEMENTS FOR ZERO TRUST AND BEST PRACTICES

ADOPTION OF 3RD PARTY APPS

Home > rcdemos inc. > Enterprise applications > ServiceNOW >

ServiceNOW | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan Diagnose and solve problems

Manage Properties Owners Users and groups Single sign-on Provisioning Self-service

Security Conditional Access Permissions Token encryption

Activity Sign-ins Usage & insights (Preview) Audit logs

Upload metadata file Change single sign-on mode Test this application Got feedback?

3 SAML Signing Certificate

Status Active
Thumbprint 5D370B727333C23CF24FB5AA57A27BEAEC771E68
Expiration 9/4/2021, 2:32:48 AM
Notification Email Missing
App Federation Metadata Url <https://login.microsoftonline.com/db9bd5e1-b037...>
Download Download Federation Metadata XML

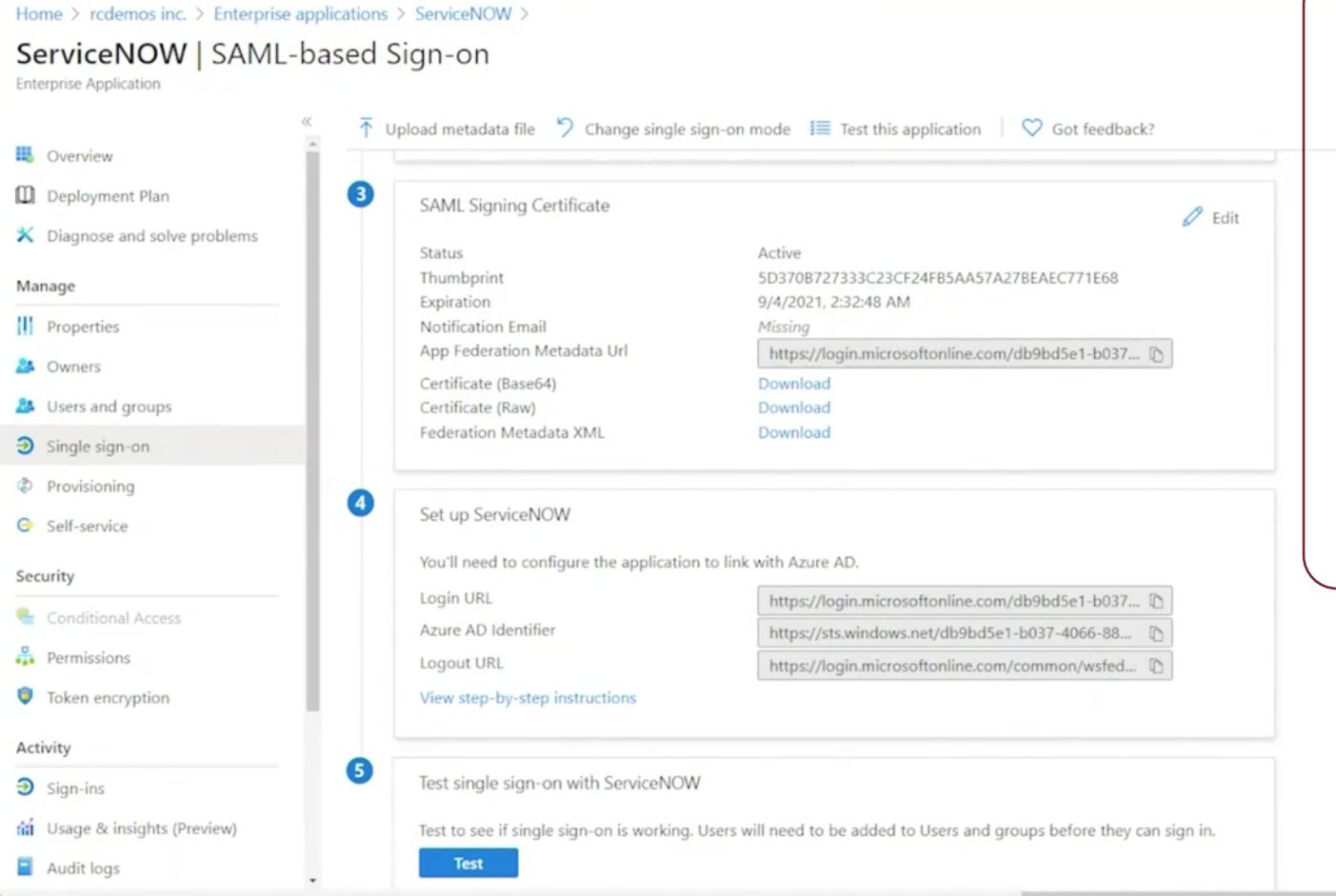
4 Set up ServiceNOW

You'll need to configure the application to link with Azure AD.

Login URL <https://login.microsoftonline.com/db9bd5e1-b037...>
Azure AD Identifier <https://sts.windows.net/db9bd5e1-b037-4066-88...>
Logout URL <https://login.microsoftonline.com/common/wsfed...>
[View step-by-step instructions](#)

5 Test single sign-on with ServiceNOW

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.
[Test](#)



Configure sign-on

Automatically Configure ServiceNow
Azure AD can automatically configure ServiceNow for single sign-on. Simply provide the information below and click "Configure Now". Or, check "Manually configure single sign-on" to learn how to perform the configuration manually.

ServiceNow Instance Name * Admin Username * Admin Password *

Make this the default identity provider for ServiceNow

Configure Now

Manually configure single sign-on

PRIVILEGED ACCESS MANAGEMENT

NEW FEATURES IN AZURE AD PIM & DIRECTORY ROLES

- Session: “Get to least privilege in Azure Active Directory and Microsoft 365 using RBAC and PIM”
 - Custom Roles for Enterprise Applications
 - Privileged Access Groups (PAG)
 - GA and Improvements of Administrative Units (AUs)
 - **Roadmap of Features in preview and development**

FUTURE INVESTMENTS IN RBAC

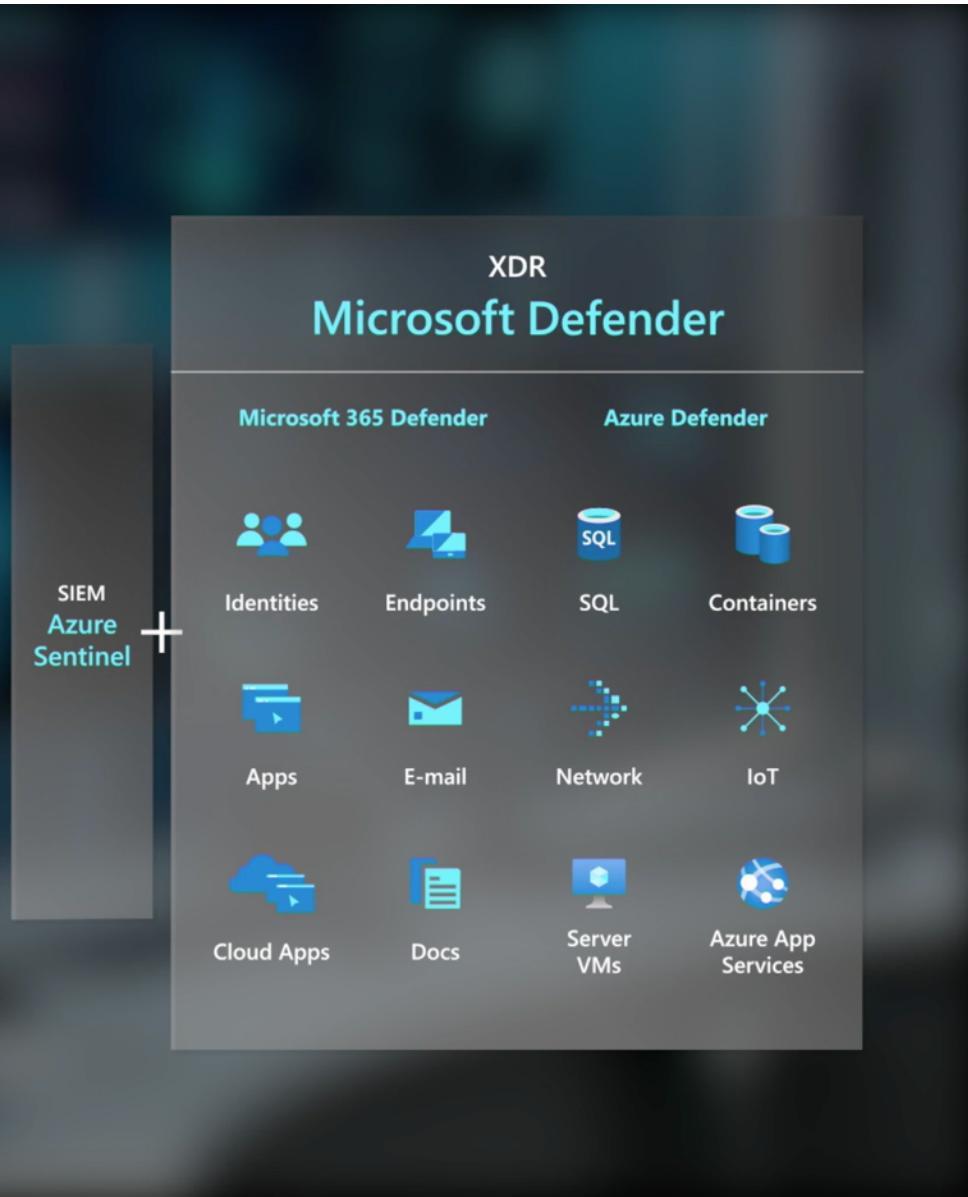
- Survey (<https://aka.ms/azureadrbacsurvey>)
 - Unified RBAC API (across S&C, Exchange, MCAS,..)
 - Scenarios of Protected AUs for sensitive Resources

A black and white abstract background featuring a globe, binary code (0s and 1s), and various geometric shapes like circles and lines.

IDENTITY FEATURE UPDATES IN AZURE AND SECURITY PRODUCTS

INTEGRATION IN SECURITY STACK

“MINOR” CHANGES WITH GREAT BENEFITS



AZURE KEYVAULT

introduced Azure AD RBAC with Granular (Object-Level) Permissions

MICROSOFT DEFENDER FOR IDENTITY (AZURE ATP)

integrated Directory Event Logs from Azure ATP Portal

AZURE AD SIGN-IN REPORTS

included Non-Interactive, Managed Identities and Service Principals

NEW IDENTITY AUDIT AND HUNTING FEATURES

Enhancement of Azure AD Audit Logs

Directory Events in Microsoft 365 Security

Entity Behavior in Azure Sentinel

LIVE DEMO

IDENTITY FEATURE UPDATES IN AZURE AND SECURITY PRODUCTS

ENTITY BEHAVIOR

Dashboard > Azure Sentinel >

Scotty

Selected workspace: 'secops-la' (Preview)

X

Guides & Feedback



Scotty



Identity

Azure AD Object ID User Principal Name
24de71e4-7eeef-421a-918d-
ac27bc59ff05 Scotty@ad.cloud-architekt.net

Security identifier Department
S-1-5-21-118446976-
1435061091-3912829123-8602 --

Manager

--

Contact info

Office Location City
-- --
Country Mobile Phone
-- --
State Email
-- scotty@ad.cloud-architekt.net

Entity link

https://portal.azure.com/#asset/Microsoft_Azure_Security_Ins...

Investigate

Overview

Search

Time range : 10/4/2020, 11:51:48 AM - 10/5/2020, 11:51:48 AM

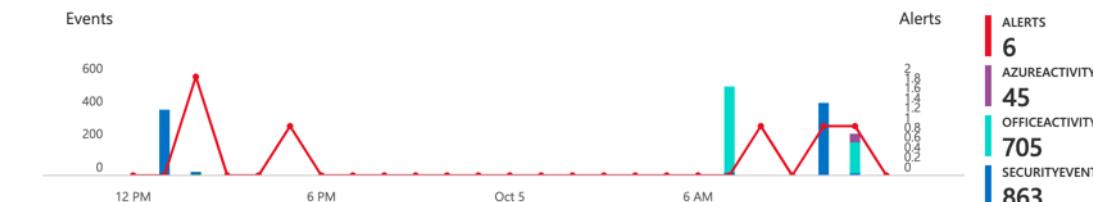
Timeline content : All

Alerts : All

Activities : All

Severity : All

Events and alerts over time



Alerts and activities timeline

An event log was cleared

Detected by Azure Security Center | 10/5/2020, 11:08:34 AM

Machine logs indicate a suspicious event log clearing operation by user: 'AD\scotty' in Machine: 'CL2-VM'. The Security log shows multiple entries of 'Event ID 4648' being cleared. This is a common indicator of privilege abuse or lateral movement. Related incident: 1155

Suspicious additions to sensitive groups

Detected by Azure Advanced Threat Protection | 10/5/2020, 10:52:43 AM

Scotty added backdoor to the sensitive Account Operators (Members can administer domain user and group accounts) group. This is a high-risk activity as it grants full control over user accounts. Related incident: 1153

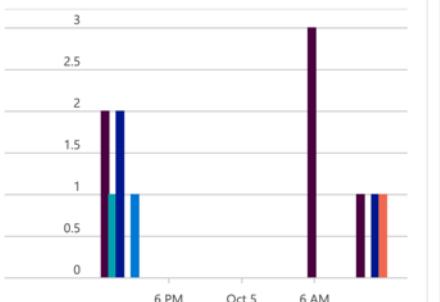
Attempt to bypass conditional access rule in Azure AD

Detected by Azure Sentinel | 10/5/2020, 8:14:24 AM

Insights

Action	Most Recent	Count
Change password	2020-10-04T12:00:00Z	1
4724	2020-10-05T09:00:00Z	1
4723	2020-10-04T12:00:00Z	1
Change user pa...	2020-10-05T09:00:00Z	3
Update user	2020-10-04T12:00:00Z	1
Update user	2020-10-04T12:00:00Z	1
Update user	2020-10-05T09:00:00Z	6
Update user	2020-10-05T09:00:00Z	7

Actions by type

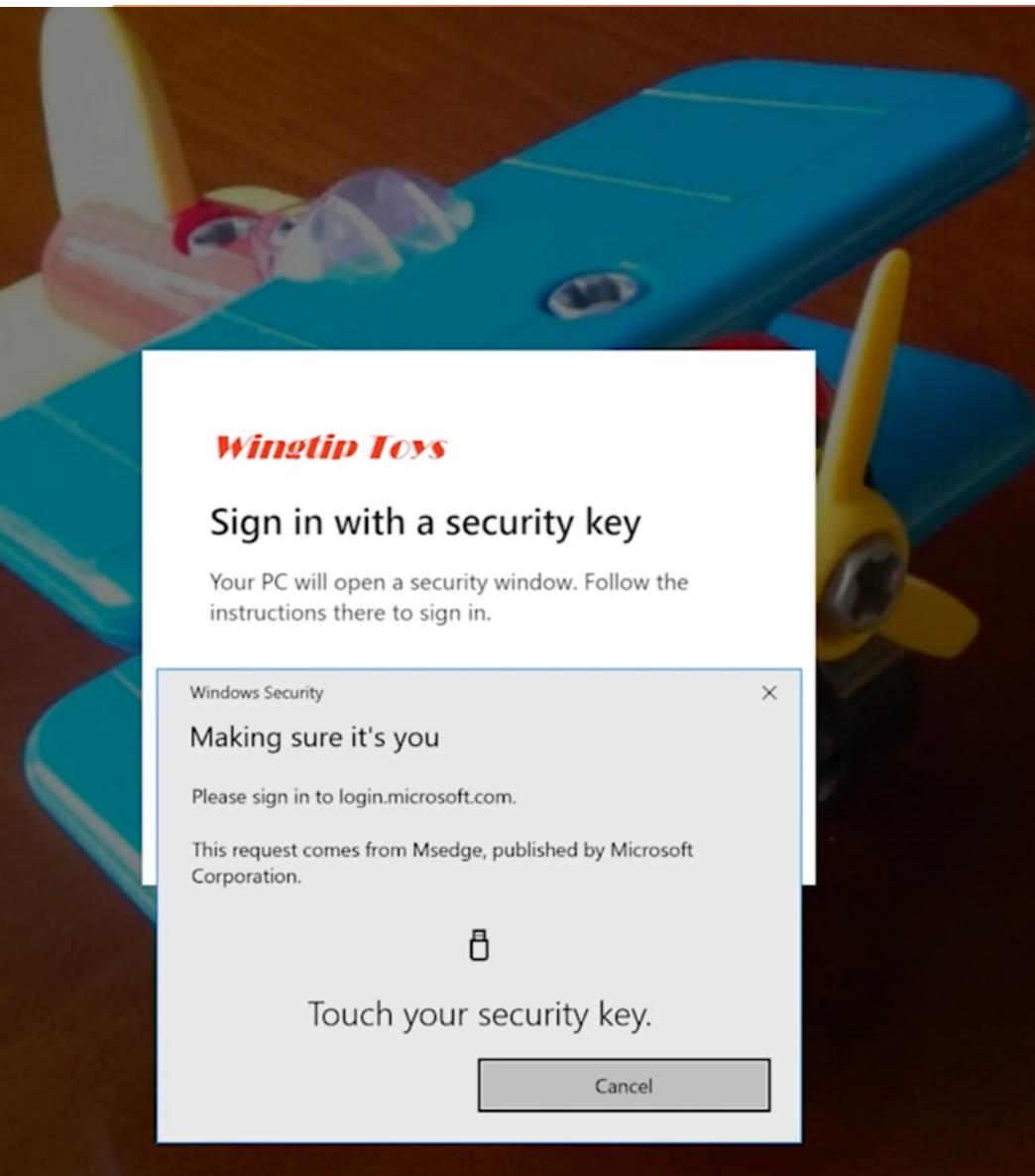




IDENTITY TRENDS AND FEATURES (OF TOMMORROW)

FUTURE OF IDENTITY

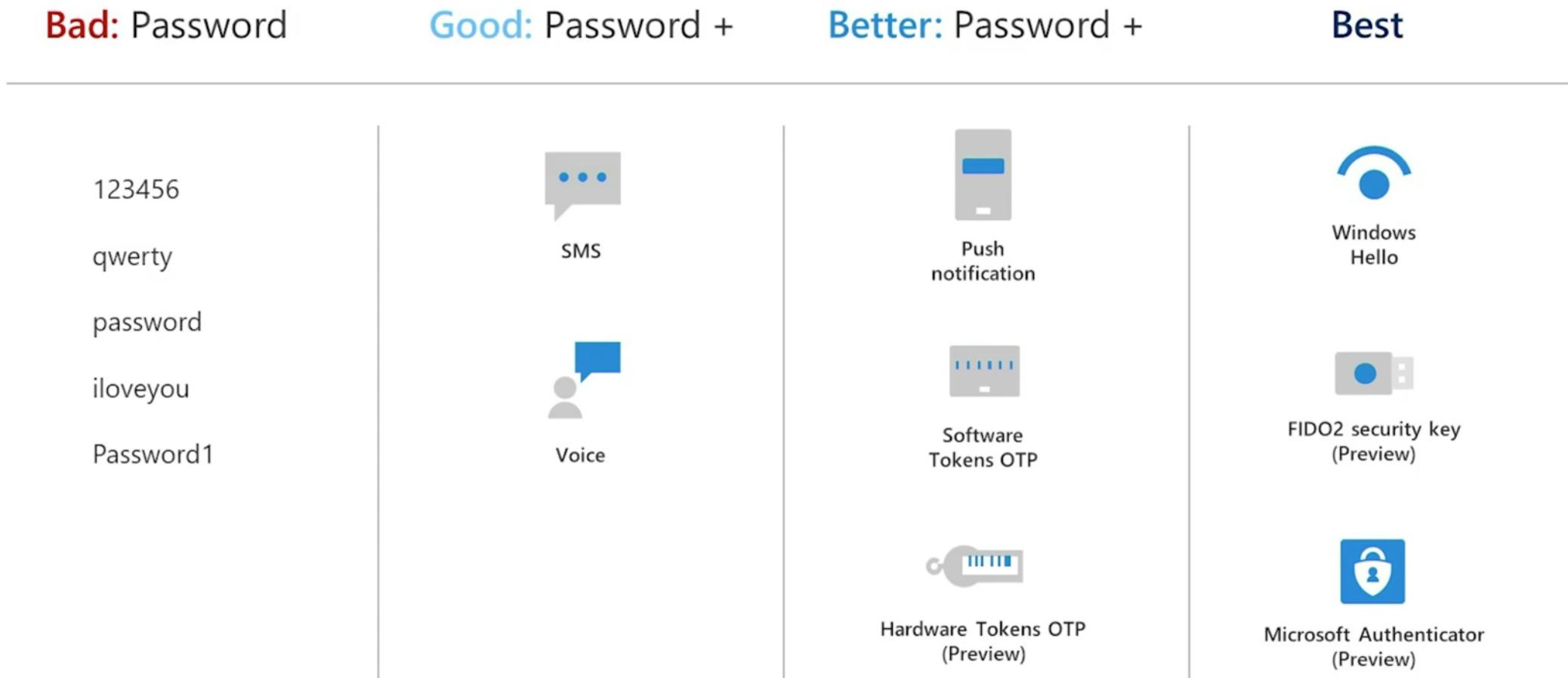
PASSWORD-LESS LOGIN



"REFRESH" OF CURRENT PUBLIC PREVIEW:

- Prompt user based on what they used last
- Advanced API Support (Policies for Authentication Methods, Read and Delete Credentials)
- Choose your right password-less option:
<http://aka.ms/passwordlesswizard>
- Session: ["The state of Passwordless in the enterprise"](#)

PASSWORD-LESS LOGIN



OWN YOUR DIGITAL IDENTITY



"DECENTRALIZED IDENTIFIERS ARE CORE TO THE FUTURE OF IDENTITY SYSTEMS"

W3C Standard "Decentralized Identifiers (DIDs)"

- Pilot with United States Department Defense (DOD)
- Digital information validation feature as part of MilGears educational program

VERIFIABLE CREDENTIALS PREVIEW BY AZURE AD

- Overview, Tutorials and Code Samples
- Issue Credentials by using various Azure Services (AAD Premium, KeyVault, Blob Storage and Node(JS) Server)
- Managing "Digital Cards" in "Authenticator App"

THANK YOU



@Thomas_Live



Thomas@Naunheim.net

www.cloud-architekt.net