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

Azure Meetup BONN

Microsoft® MVP Most Valuable Professional

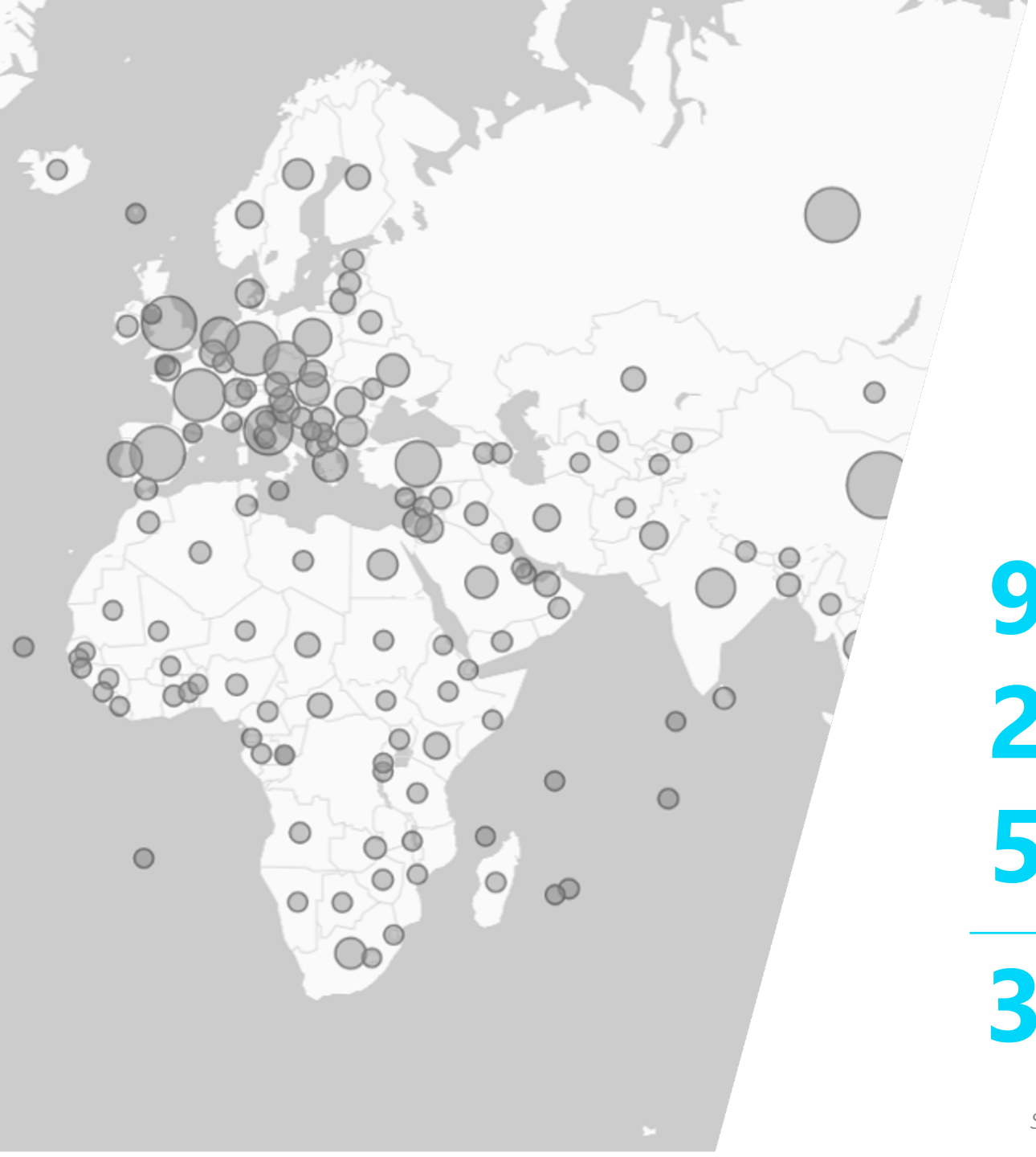
IGNITE 2020 FOCUS

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

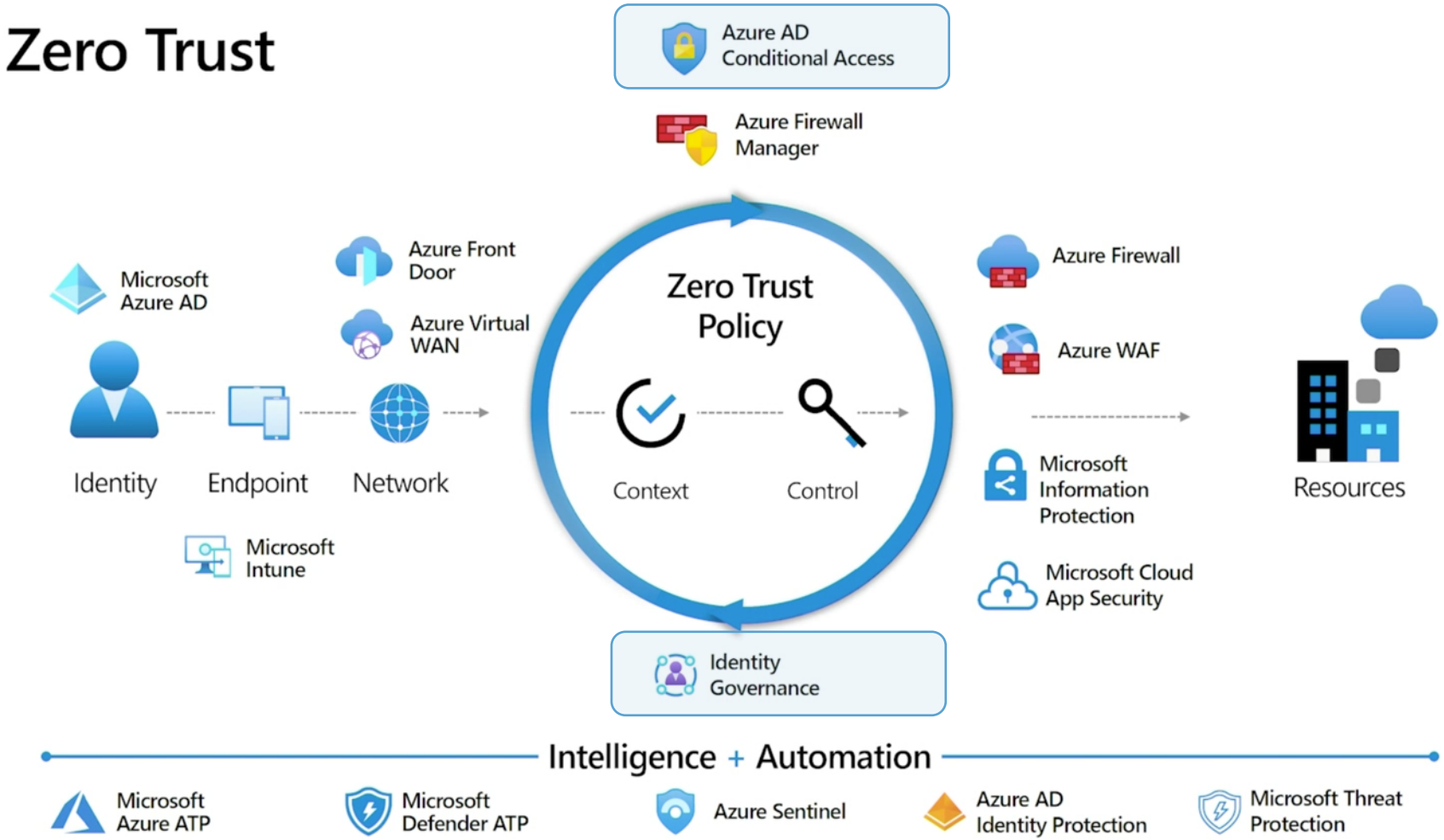
Source: "The science behind Azure Active Directory Identity Protection"

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

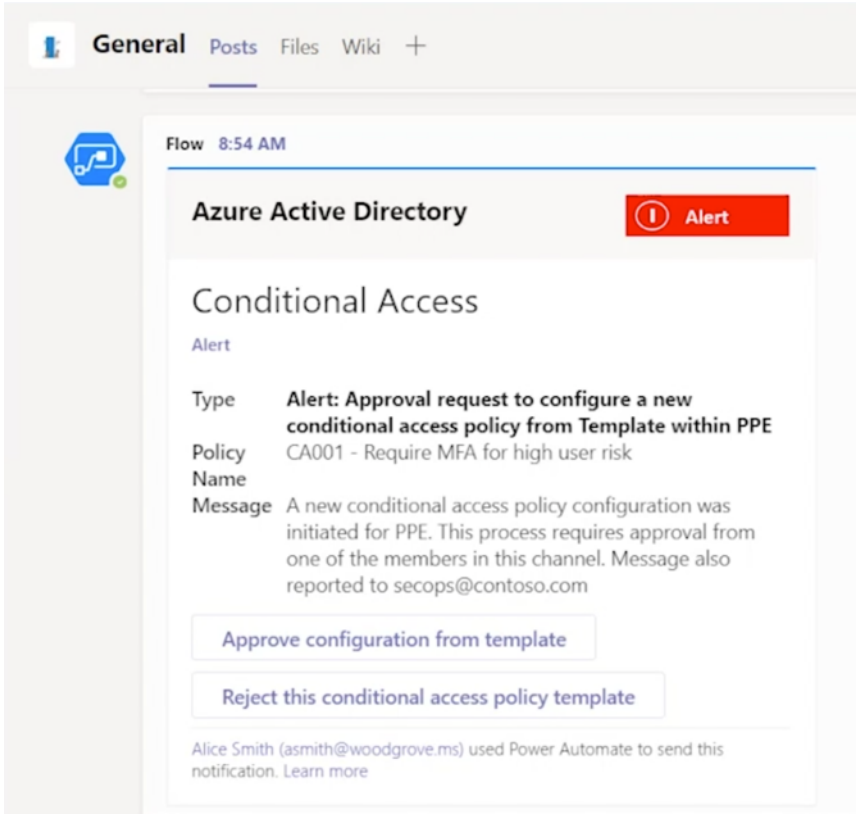


Details: Zero Trust deployment guide for Identity (https://aka.ms/ZTIdentity)

SECURING IDENTITY WITH ZERO TRUST (ZT)

Details: Zero Trust deployment guide for Identity (https://aka.ms/ZTIdentity)

CONDITIONAL ACCESS AS ZT POLICY ENGINE



AUTOMATION VIA (GRAPH) API

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

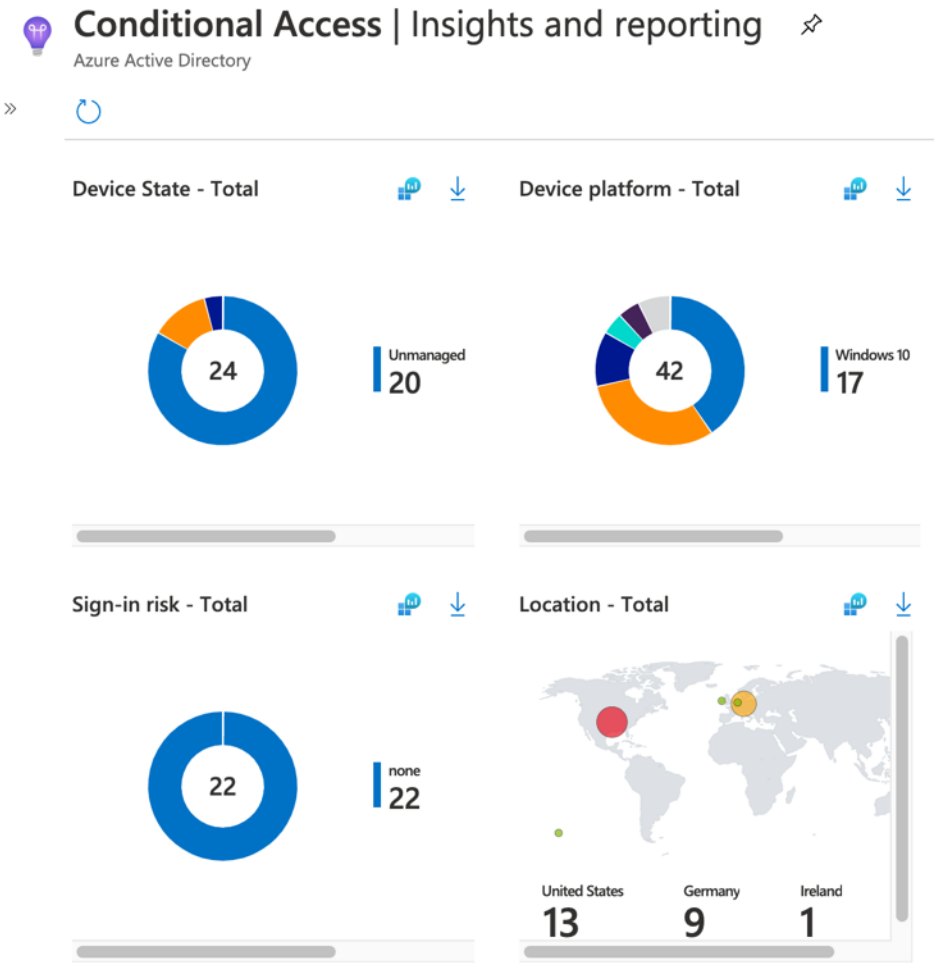
- GitHub Repo includes Samples
- Microsoft Docs: “Management of Lifecycle via API”

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

Image Source: “Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity”

CONDITIONAL ACCESS AS ZT POLICY ENGINE



ADVANCED REPORTING AND INSIGHTS

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

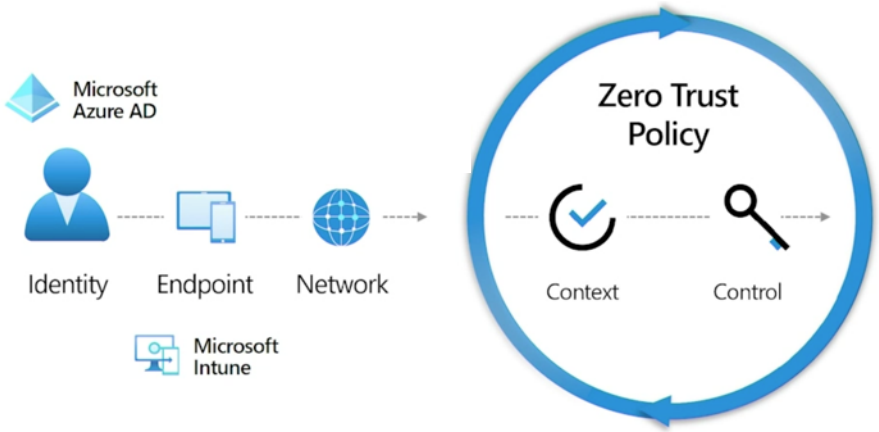
- Detailed Insights and Reporting
- Block legacy authentication in your organization

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

Image Source: "Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity"

CONTINUOUS ACCESS EVALUATION (CAE)

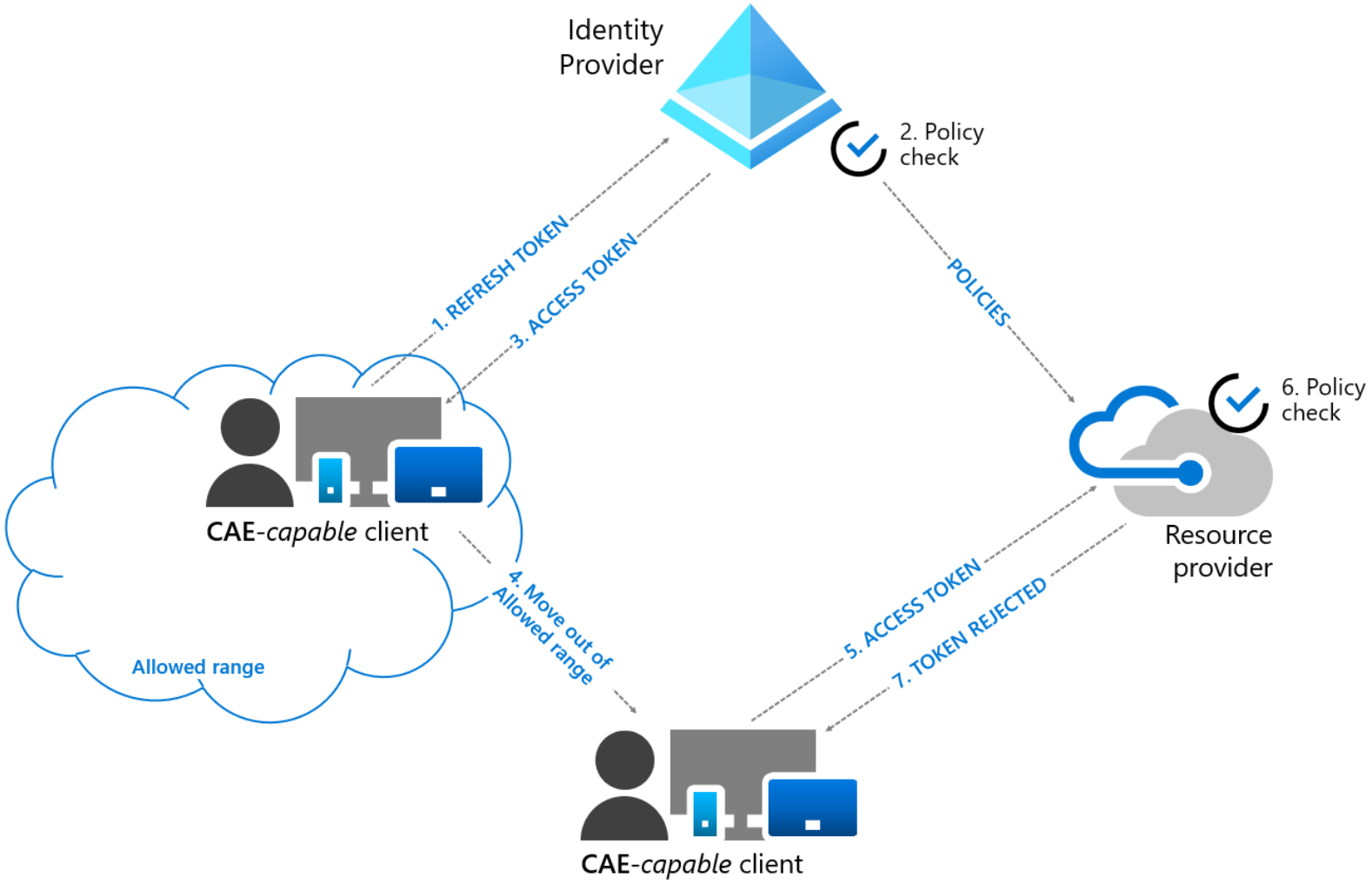
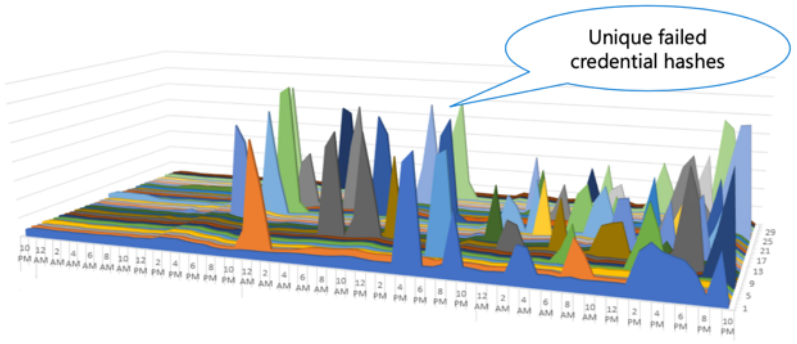
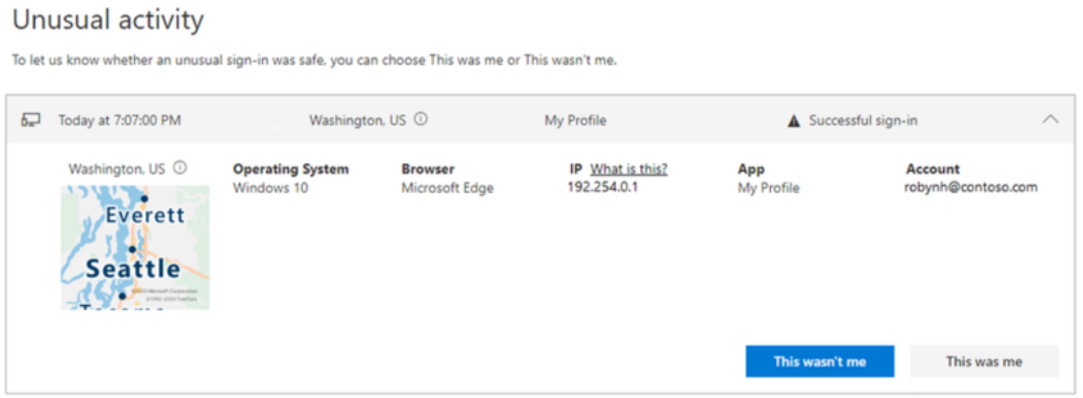


Image Source: "Continuous access evaluation (Microsoft Docs)"

IDENTITY PROTECTION





PASSWORD SPRAY ATTACKS

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

GENERAL ENHANCEMENTS

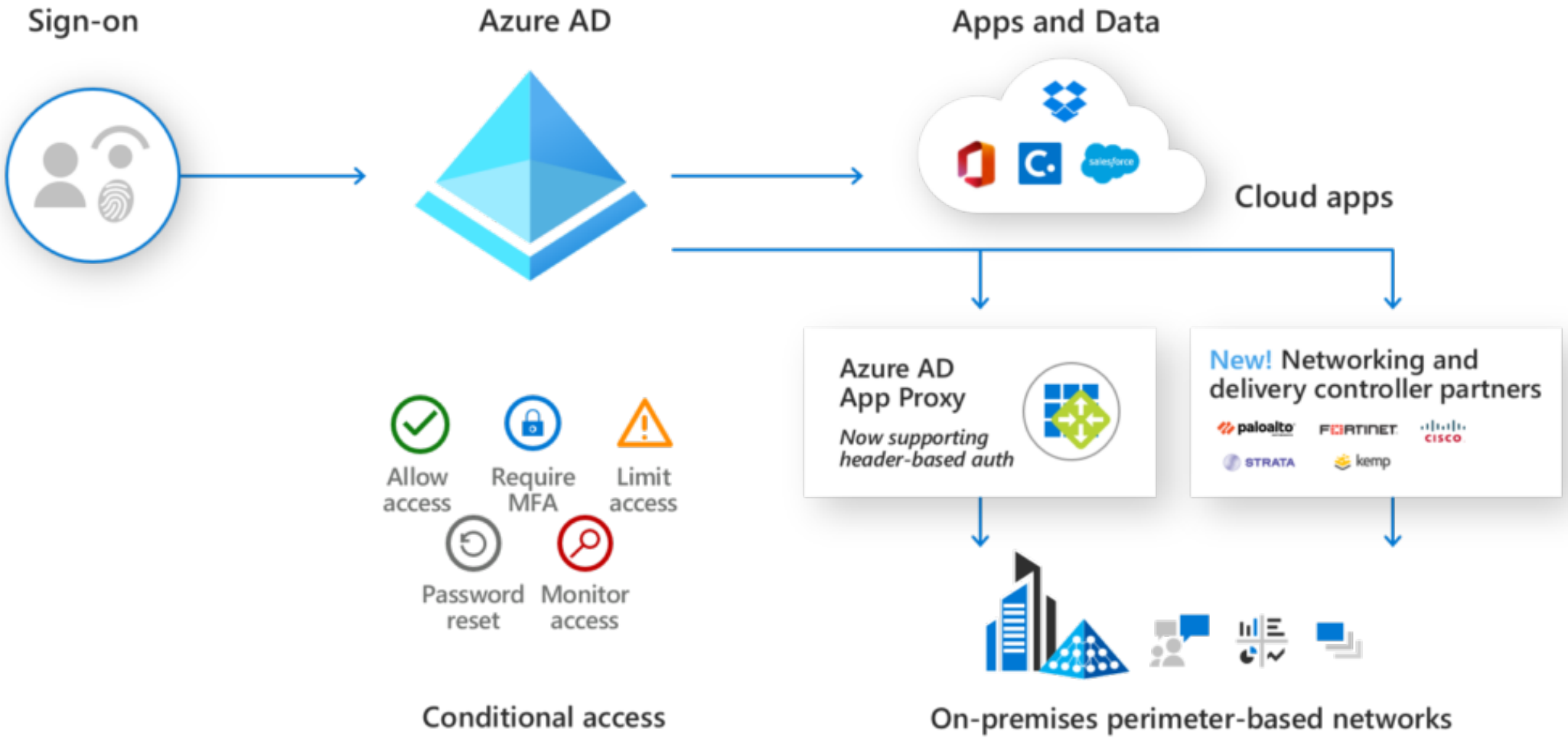
- End User Feedback Integration
- Advanced APIs and Integration
- Session: ”The science behind Identity Protection”

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

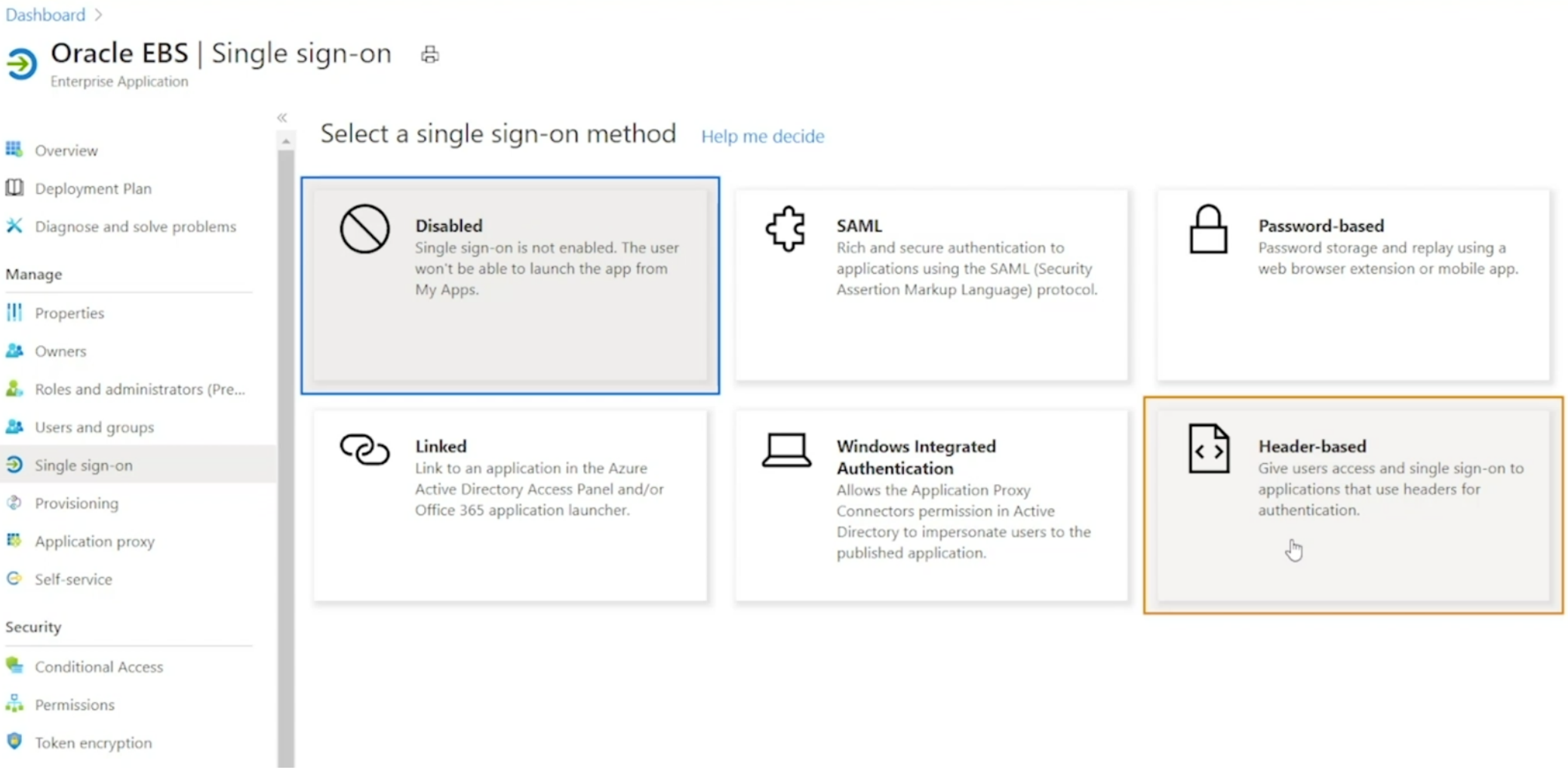


Source: Identity at Microsoft Ignite: Rising to the challenges of secure remote access and employee productivity

SECURE HYBRID ACCESS PARTNERS

Source: "Top 7 Microsoft Identity partnership announcements at Ignite 2020"

SUPPORT OF LEGACY ON-PREMISES APPS

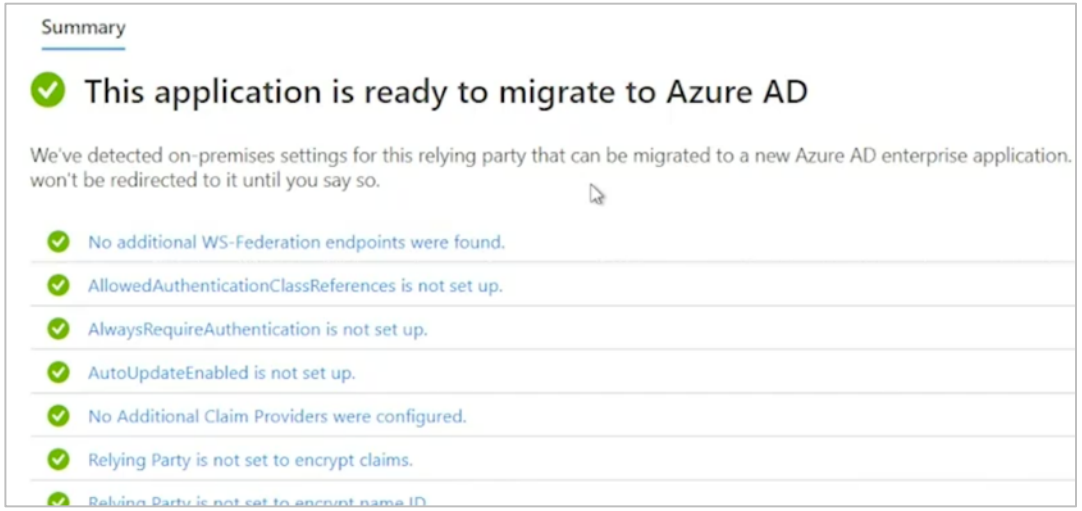


Source: "Azure Active Directory: our vision and roadmap to help you secure remote access and boost employee productivity"

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

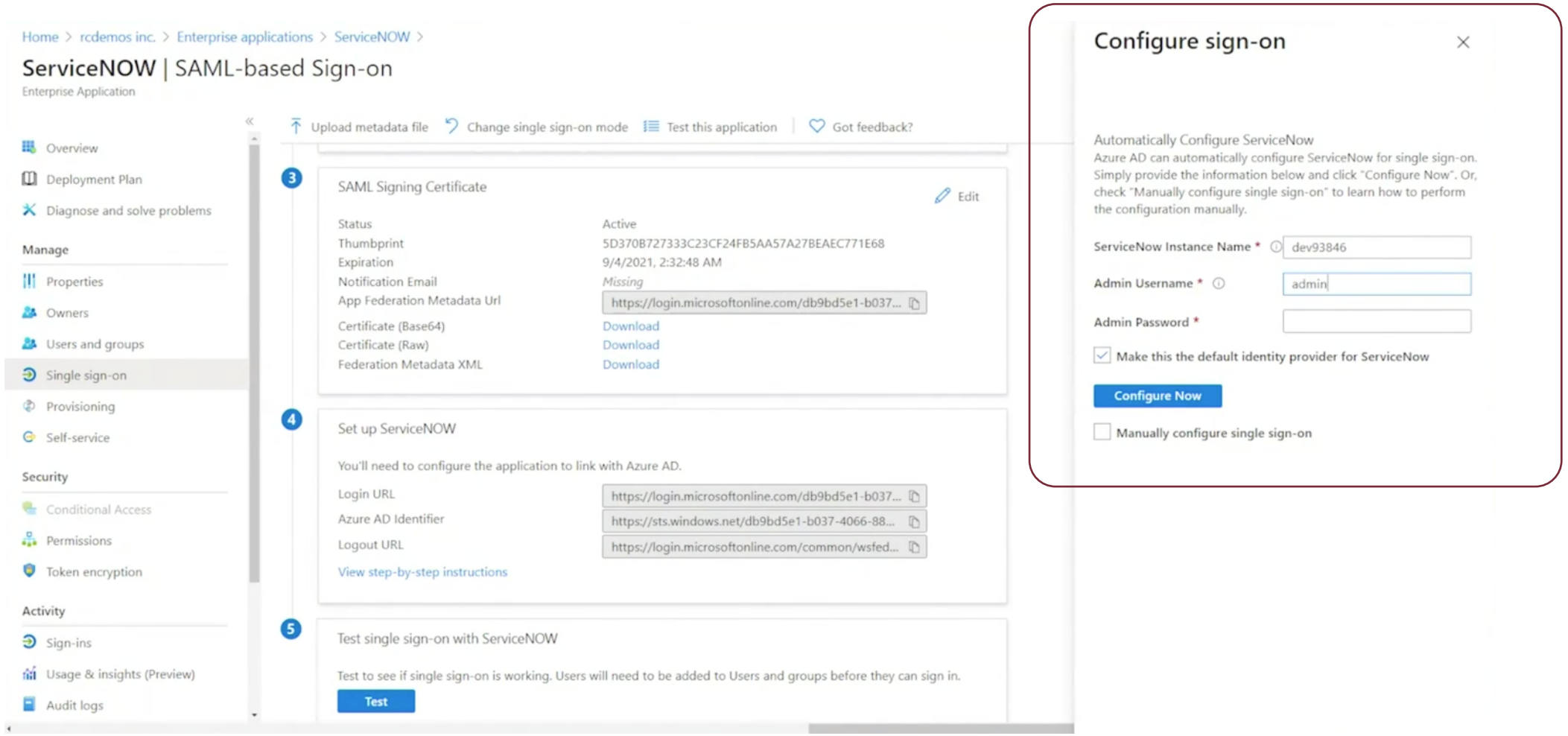


Stats	Numbers	%
Total Number of Applications	73	
Applications that can't be migrated	13	17.81%
Application with Warnings	16	21.92%
Applications that can be migrated	44	60.27%
Percentage of apps that can be migrated	60.27%	

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

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

ADOPTION OF 3RD PARTY APPS



Source: "Save money by securing access to all your apps with Azure AD"

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

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

Image Source: "Achieve resilience with Security, Compliance, and Identity"

NEW IDENTITY AUDIT AND HUNTING FEATURES

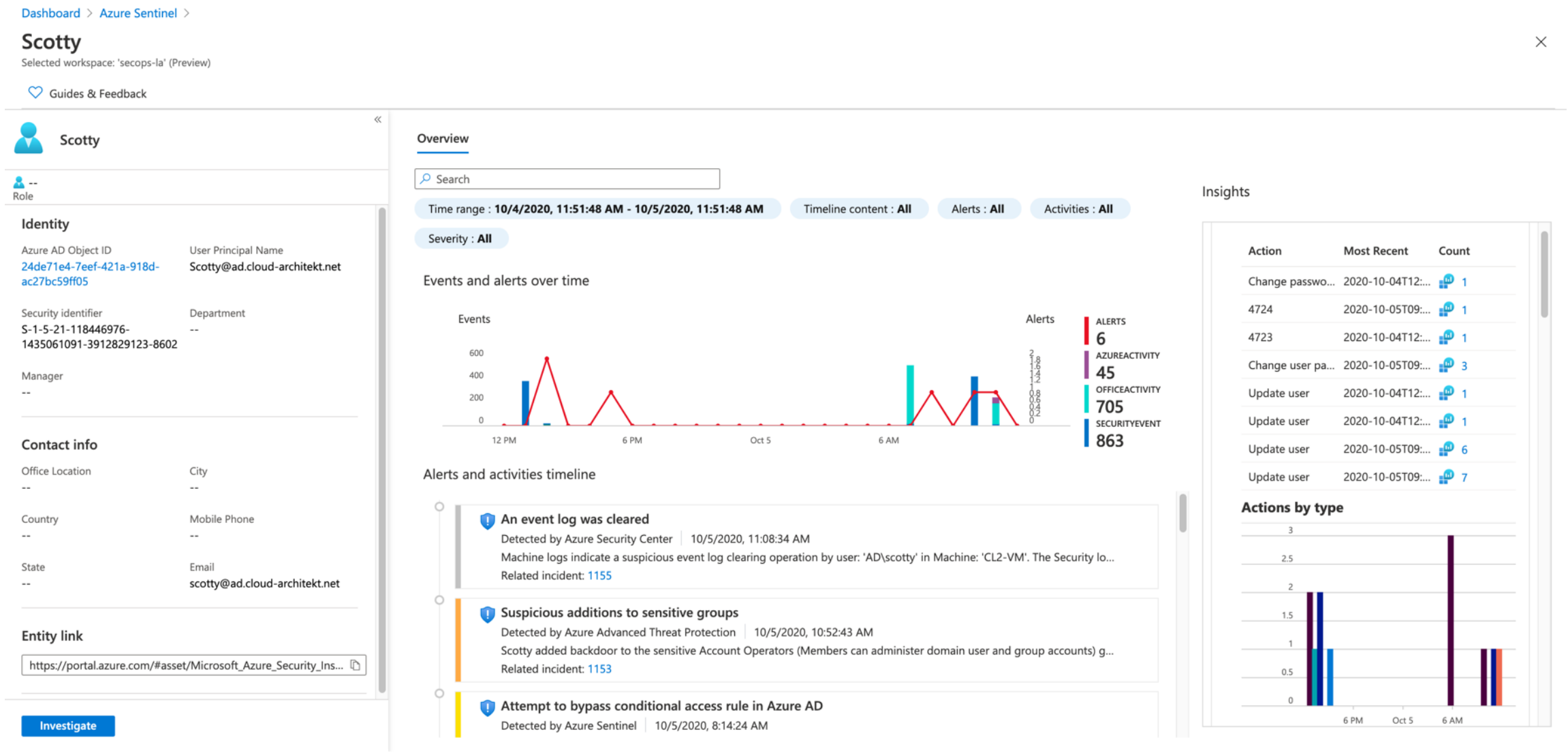
Enhancement of Azure AD Audit Logs

Directory Events in Microsoft 365 Security

Entity Behavior in Azure Sentinel

LIVE DEMO

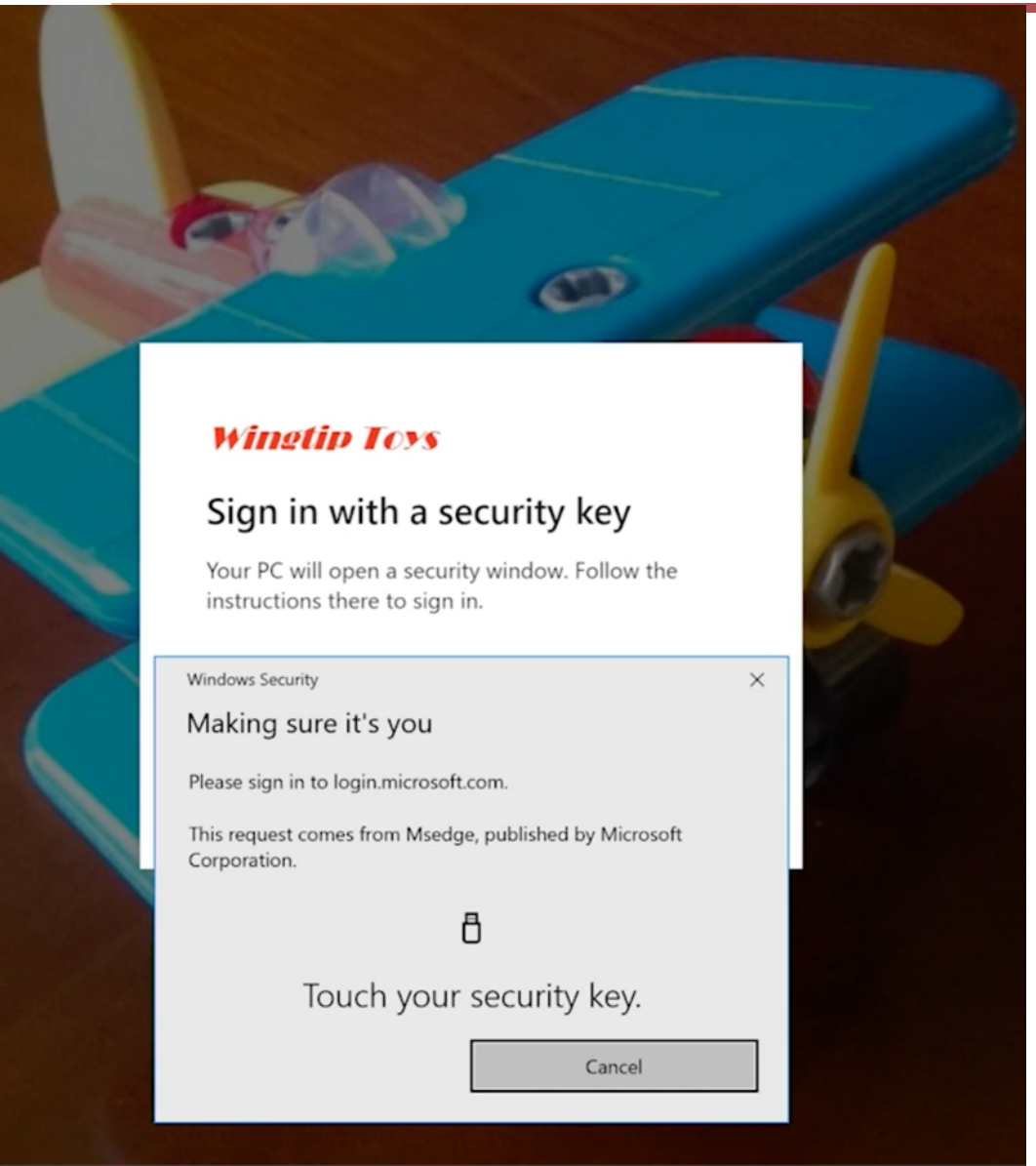
ENTITY BEHAVIOR



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

Bad: Password	**Good:** Password +	**Better:** Password +	**Best**
123456	SMS	Push notification	Windows Hello
qwerty	Voice	Software Tokens OTP	FIDO2 security key (Preview)
password		Hardware Tokens OTP (Preview)	Microsoft Authenticator (Preview)
iloveyou			
Password1			

Source: Winning Azure Active Directory strategies for identity security and governance

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