

Secureworks®

ICEIS 2022

24th International Conference on Enterprise Information Systems

Online Streaming 25 - 27 April, 2022

Exploring Azure Active Directory Attack Surface: Enumerating Authentication Methods with Open-Source Intelligence Tools

@DrAzureAD

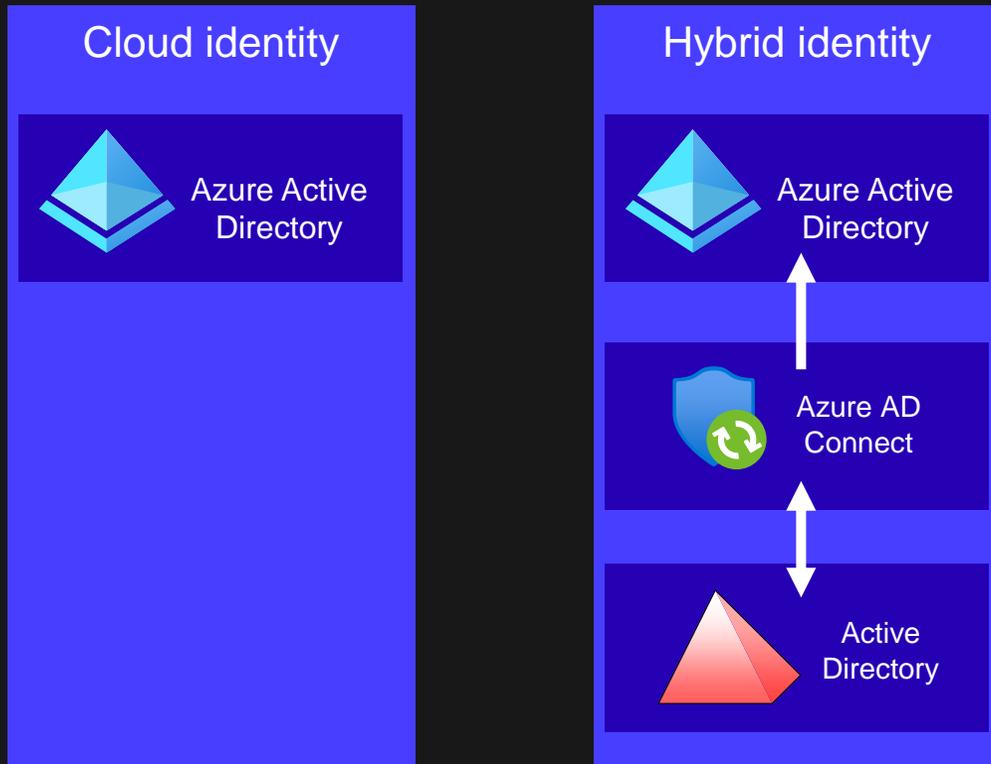
<https://linkedin.com/in/nestori>

Contents

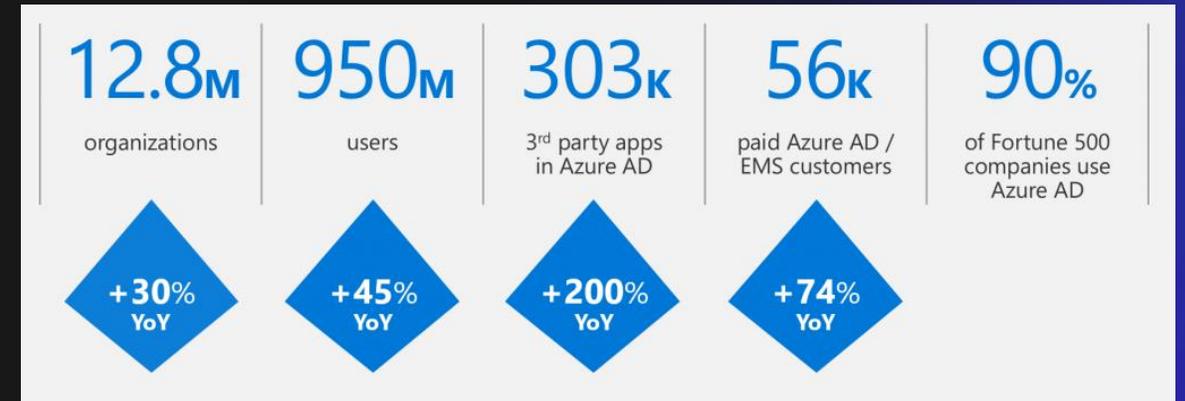
- Introduction
- Methodology
- Results

Introduction

- Azure Active Directory (Azure AD) is Microsoft's cloud-based Identity and Access Management (IAM) system
- Identity options:

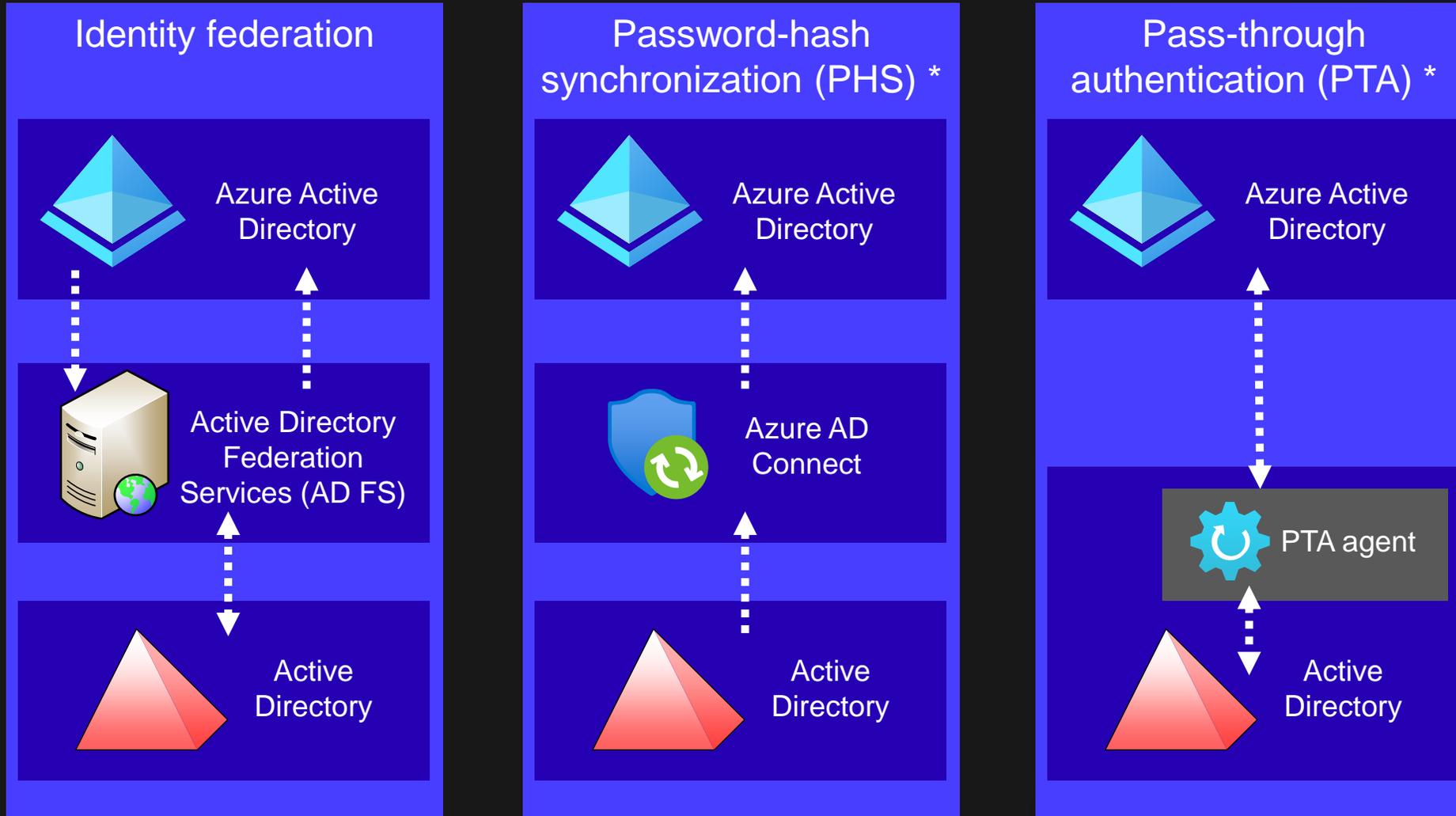


Source: Secureworks



Source: Microsoft / Simons (2017)

Hybrid identity options & known attack vectors



* Supports seamless single sign-on

Source: Secureworks

Research Questions

- What is the Azure AD adoption rate?
- Which authentication methods organisations are using?
- What other information is openly available?

Methodology

- Datasets:
 - 2019: Fortune 500 companies
 - 2022: Top 2000 universities
- Extracted information with AADInternals
 - Azure AD Tenant Id (adoption rate)
 - Directory Synchronisation status (hybrid identity)
 - Seamless Single-Sign-On (sso #1)
 - Federated Domains (sso #2)
 - Tenant Organisation information (administrator name & phone number)

Azure AD Adoption rate

Organisation type		
Fortune 500 (<i>n</i> =500)	441	88 %
Top 2000 Universities (<i>n</i> =2000)	1892	95 %

Directory Synchronisation

Organisation type		
Fortune 500 (<i>n</i> =441)	420	84 %
Top 2000 Universities (<i>n</i> =1892)	1042	52 %

Seamless SSO

Organisation type		
Fortune 500 (<i>n</i> =441)	118	27 %
Top 2000 Universities (<i>n</i> =1892)	258	14 %

Domains Registered

Organisation type		
Fortune 500 (<i>n</i> =441)	432	98 %
Top 2000 Universities (<i>n</i> =1892)	1884	100 %

Average number of domains:

Organisation type	
Fortune 500	77
Top 2000 Universities	17

Federated Domains

Organisation type		
Fortune 500 (<i>n</i> =432)	293	68 %
Top 2000 Universities (<i>n</i> =1884)	535	28 %

Average number of federated domains:

Organisation type	
Fortune 500	18
Top 2000 Universities	6

Both SSOs

Organisation type		
Fortune 500 (<i>n</i> =441)	11	2.49 %
Top 2000 Universities (<i>n</i> =1892)	9	0.48 %

Tenant Organisation Information

Organisation type		
Fortune 500 (<i>n</i> =432)	434	98 %
Top 2000 Universities (<i>n</i> =1884)	1463	77 %

With phone number:

Organisation type		
Fortune 500 (<i>n</i> =432)	383	87 %
Top 2000 Universities (<i>n</i> =1884)	1059	56 %

Conclusion

- What is the Azure AD adoption rate?
 - Azure AD adoption rate is high
- Which authentication methods organisations are using?
 - ~60 percent of Fortune 500 organisations still use identity federation (AD FS)
- What other information is openly available?
 - Open-source intelligence (OSINT) can be used for reconnaissance
 - Microsoft now prevents querying directory synchronisation & organisation information

Thank you!

Questions?