RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **CSCS-R06**

The Road to Cloud Is Paved with On-Prem Integrations

Dr. Nestori Syynimaa

Senior Principal Security Researcher
Secureworks® CTU
@DrAzureAD

Disclaimer

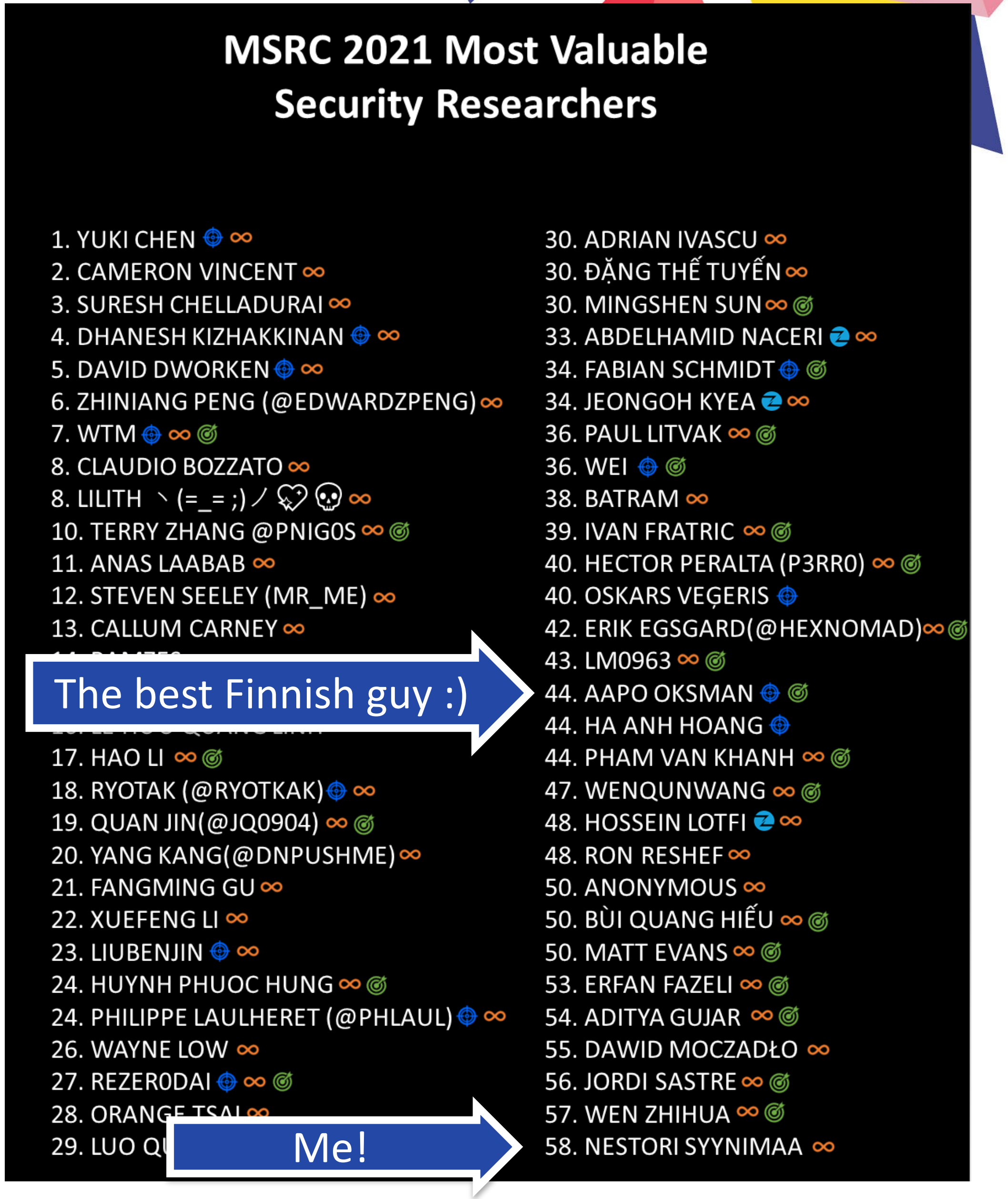
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Introduction

About the speaker

- Dr. Nestori Syynimaa (@DrAzureAD)
- Senior Principal Security Researcher @Secureworks CTU
- Creator of AADInternals toolkit
- Microsoft MCT
- Microsoft MVP x2
- Microsoft MVR



MSRC 2021 Most Valuable Security Researchers

1. YUKI CHEN ⊕ ∞
2. CAMERON VINCENT ∞
3. SURESH CHELLADURAI ∞
4. DHANESH KIZHAKKINAN ⊕ ∞
5. DAVID DWORKEN ⊕ ∞
6. ZHINIANG PENG (@EDWARDZPENG) ∞
7. WTM ⊕ ∞ ◎
8. CLAUDIO BOZZATO ∞
8. LILITH ヽ(=_=;)ノ 💖 💀 ∞
10. TERRY ZHANG @PNIG0S ∞ ◎
11. ANAS LAABAB ∞
12. STEVEN SEELEY (MR_ME) ∞
13. CALLUM CARNEY ∞
17. HAO LI ∞ ◎
18. RYOTAK (@RYOTKAK) ⊕ ∞
19. QUAN JIN(@JQ0904) ∞ ◎
20. YANG KANG(@DNPUSHME) ∞
21. FANGMING GU ∞
22. XUEFENG LI ∞
23. LIUBENJIN ⊕ ∞
24. HUYNH PHUOC HUNG ∞ ◎
24. PHILIPPE LAULHERET (@PHLAUL) ⊕ ∞
26. WAYNE LOW ∞
27. REZER0DAI ⊕ ∞ ◎
28. ORANGE TSAI ∞
29. LUO QU
30. ADRIAN IVASCU ∞
30. ĐẶNG THẾ TUYẾN ∞
30. MINGSHEN SUN ∞ ◎
33. ABDELHAMID NACERI ⓩ ∞
34. FABIAN SCHMIDT ⊕ ◎
34. JEONGOH KYEA ⓩ ∞
36. PAUL LITVAK ∞ ◎
36. WEI ⊕ ◎
38. BATRAM ∞
39. IVAN FRATRIC ∞ ◎
40. HECTOR PERALTA (P3RR0) ∞ ◎
40. OSKARS VEĢERIS ⊕
42. ERIK EGSGARD(@HEXNOMAD) ∞ ◎
43. LM0963 ∞ ◎
44. AAPO OKSMAN ⊕ ◎
44. HA ANH HOANG ⊕
44. PHAM VAN KHANH ∞ ◎
47. WENQUNWANG ∞ ◎
48. HOSSEIN LOTFI ⓩ ∞
48. RON RESHEF ∞
50. ANONYMOUS ∞
50. BÙI QUANG HIẾU ∞ ◎
50. MATT EVANS ∞ ◎
53. ERFAN FAZELI ∞ ◎
54. ADITYA GUJAR ∞ ◎
55. DAWID MOCZADŁO ∞
56. JORDI SASTRE ∞ ◎
57. WEN ZHIHUA ∞ ◎
58. NESTORI SYYNIMAA ∞

The best Finnish guy :)

Me!

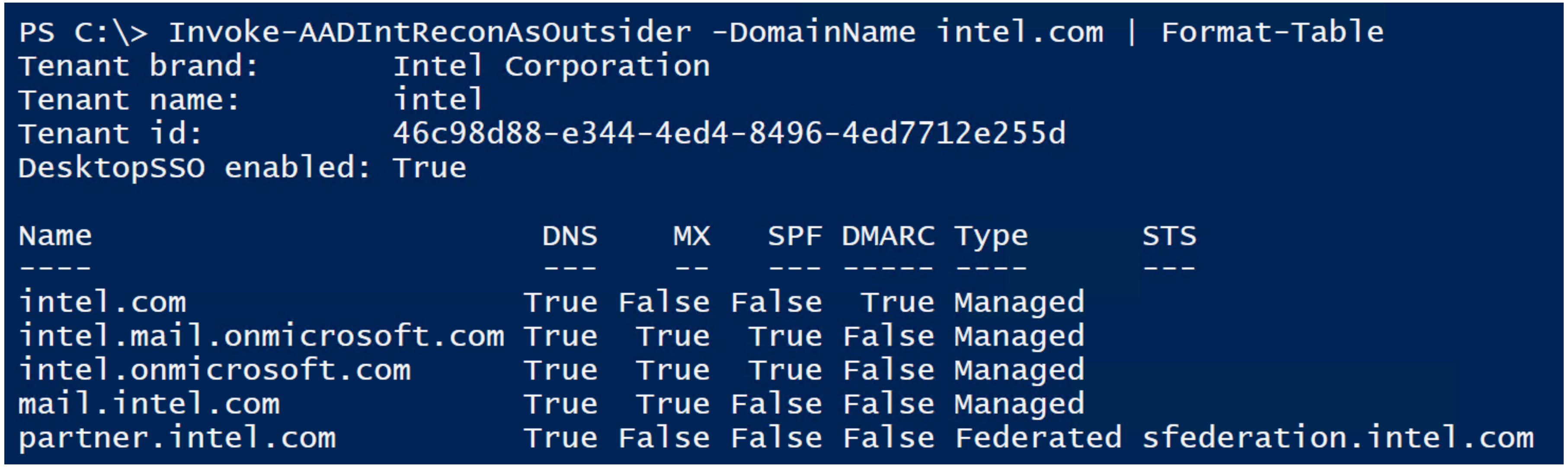
Contents

- Azure Active Directory authentication options
- On-prem integrations and threats of each option
- Hardening / mitigation techniques

- To make points:
  - Live demos w/ AADInternals 😮
  - Interactive demos w/ audience 😲

Azure Active Directory OSINT

- Azure AD APIs can be used to fetch OSINT for any tenant
- Presentation statistics based on OSINT for Fortune 500 companies and top 2000 universities*



```
PS C:\> Invoke-AADIntReconAsOutsider -DomainName intel.com | Format-Table
Tenant brand:       Intel Corporation
Tenant name:        intel
Tenant id:          46c98d88-e344-4ed4-8496-4ed7712e255d
DesktopSSO enabled: True

Name                        DNS    MX   SPF DMARC Type      STS
----                        ---    --   --- ----- ----      ---
intel.com                  True False False  True Managed
intel.mail.onmicrosoft.com True  True  True False Managed
intel.onmicrosoft.com      True  True  True False Managed
mail.intel.com             True  True False False Managed
partner.intel.com          True False False False Federated sfederation.intel.com
```

* Syynimaa, Nestori. (2022). *Exploring Azure Active Directory Attack Surface - Enumerating Authentication Methods with Open-Source Intelligence Tools*. Paper presented at the ICEIS - 24th International Conference on Enterprise Information Systems, Apr 25-27.

Azure AD Adoption Rate Statistics

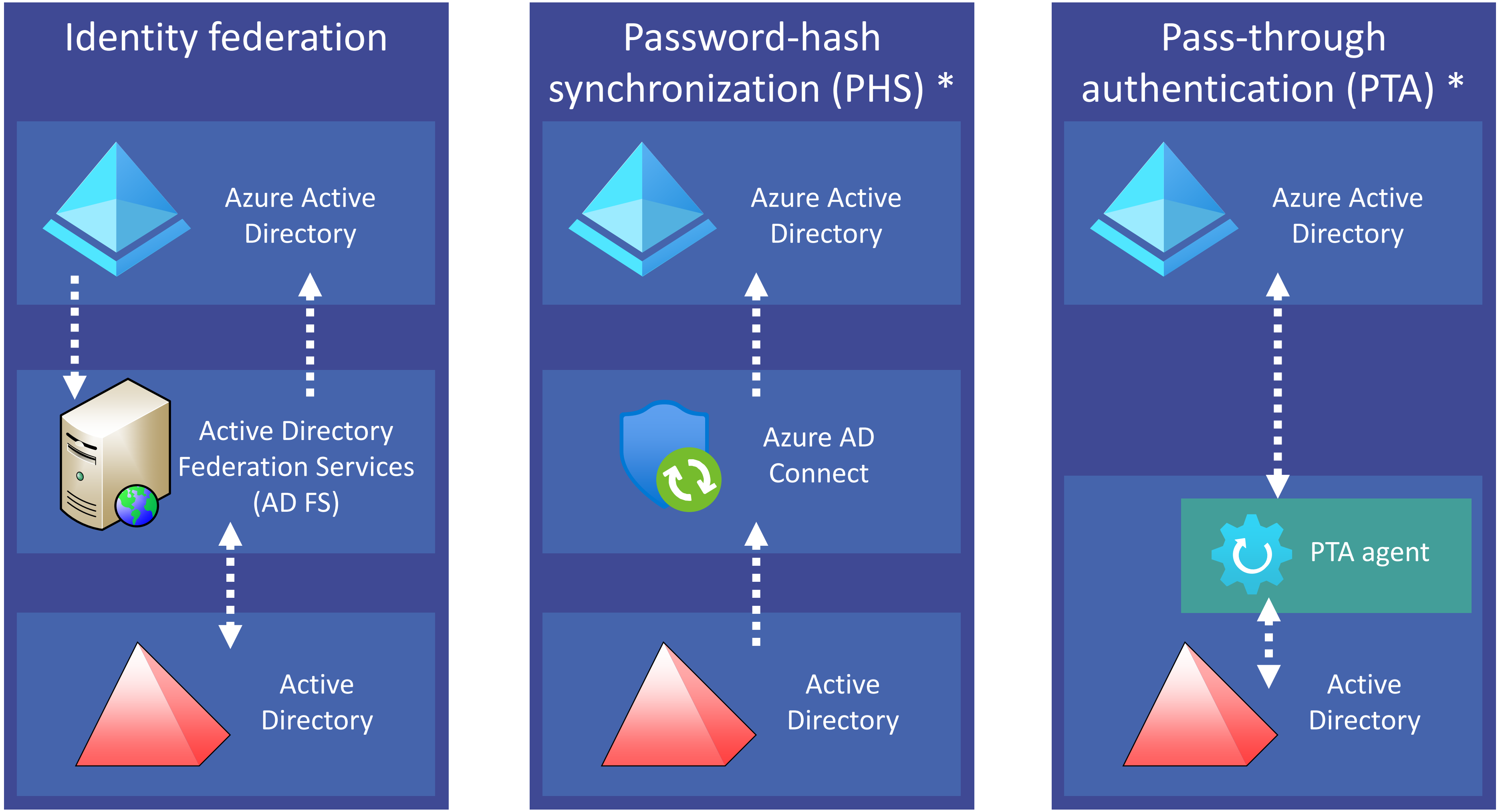
Fortune 500		
Has Azure AD tenant	441	88 %
No Azure AD tenant	59	12 %

Top 2000 Universities		
Has Azure AD tenant	1892	95 %
No Azure AD tenant	108	5 %

RSAConference2022

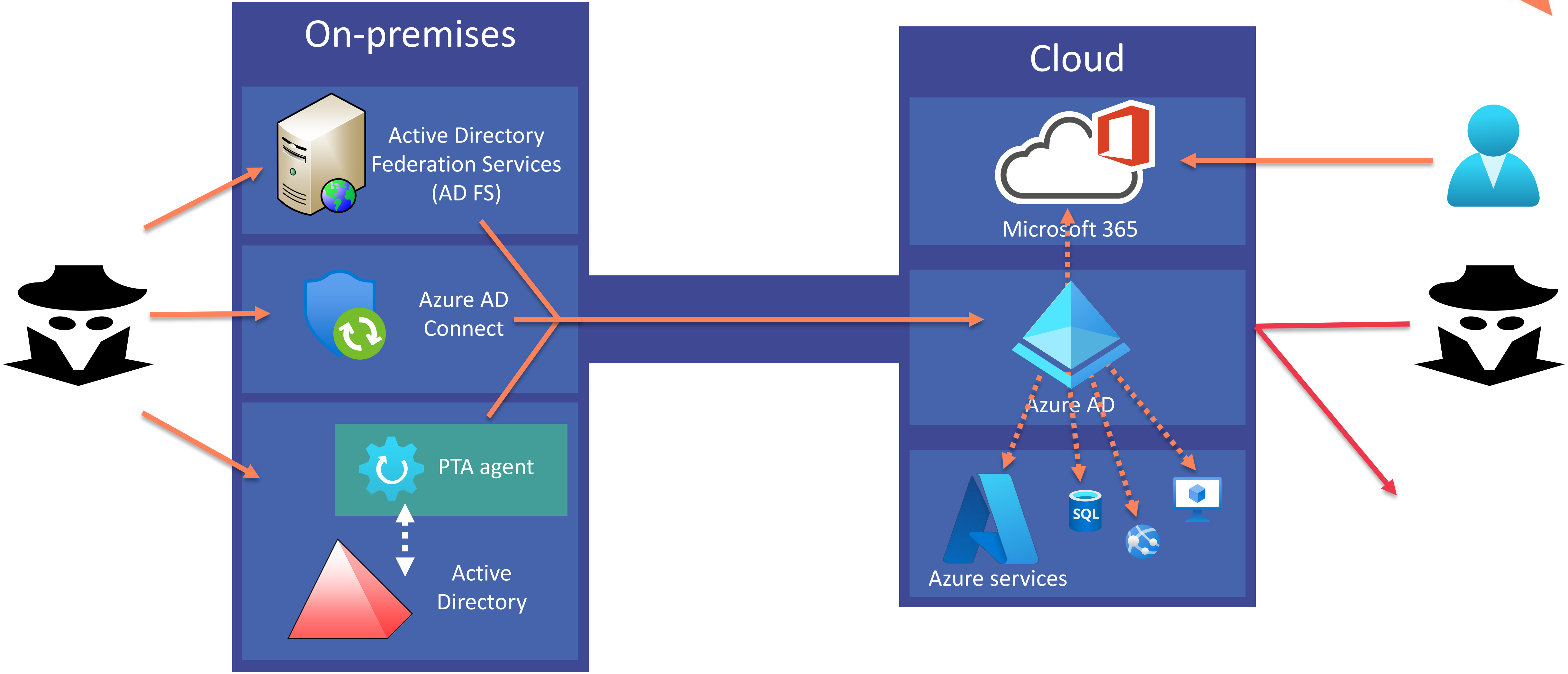
Azure AD Cloud & Hybrid Identities

Azure AD Hybrid Authentication Options



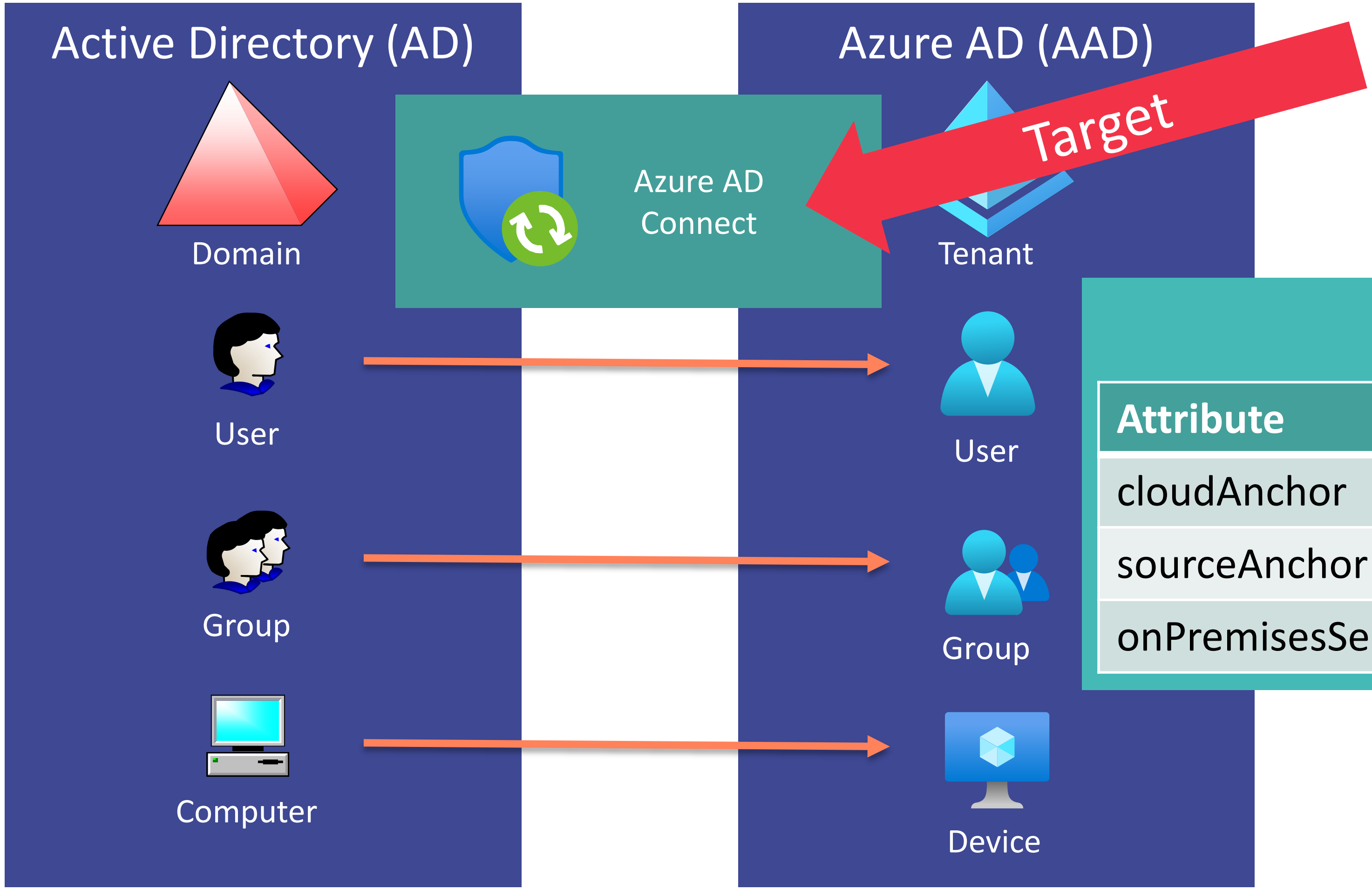
* Supports seamless single sign-on

(Hybrid) Cloud Security



Hybrid Cloud Threats and Mitigations

Directory Synchronization



Azure AD Object

Attribute	Description
cloudAnchor	<object type>_<object id>
sourceAnchor	B64(on-prem AD object GUID)
onPremisesSecurityIdentifier	on-prem AD object SID

Azure AD Synchronization Statistics

Fortune 500 (*n*=441)		
Enabled	411	93 %
Enabled (errors)	9	2 %
Disabled	*13*	*3 %*
Unknown	*8*	*2 %*

Top 2000 universities (*n*=1 892)		
Enabled	929	49 %
Enabled (errors)	63	3 %
Disabled	*895*	*47 %*
Unknown	*5*	*0 %*

Demo

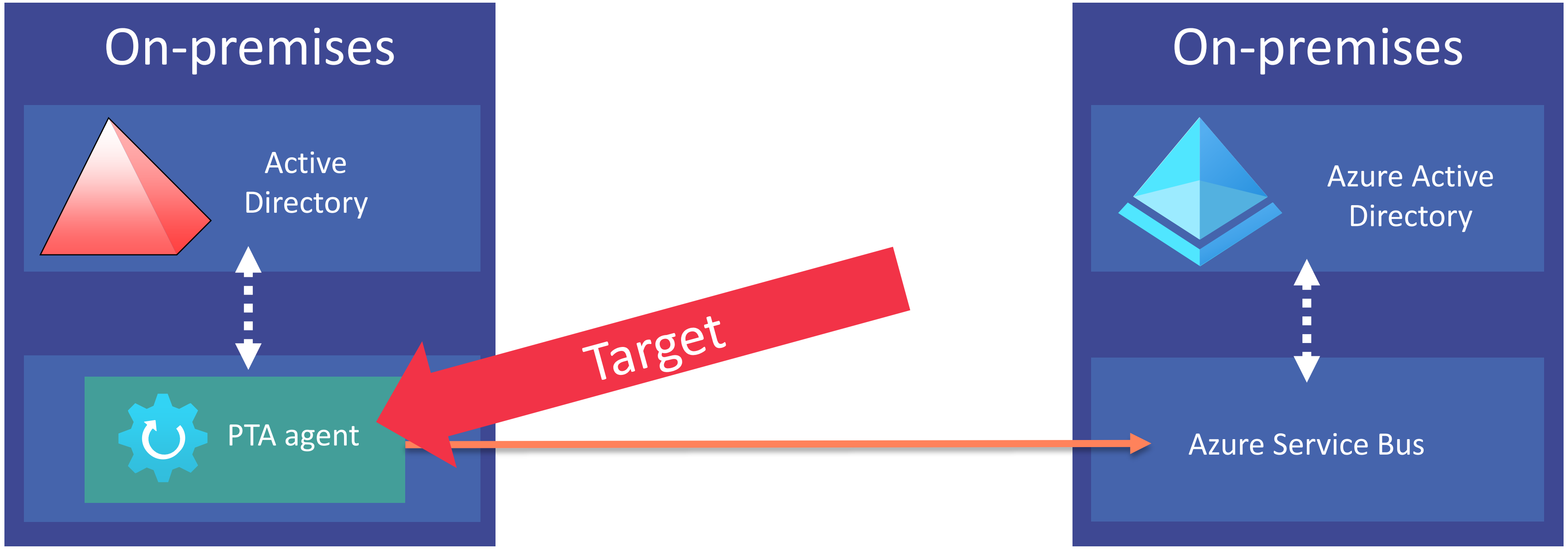
- Dump Azure AD Connect credentials with AADInternals:

  `Get-AADIntSyncCredentials`

Directory Synchronization hardening

- Treat as tier 0 server
- Limit access to server
- Allow synchronization only from dedicated ip-address(es)

Pass-through Authentication (PTA)



Demo

- Create a backdoor and harvest credentials with AADInternals' PTA Spy:

  `Install-AADIntPTASpy`

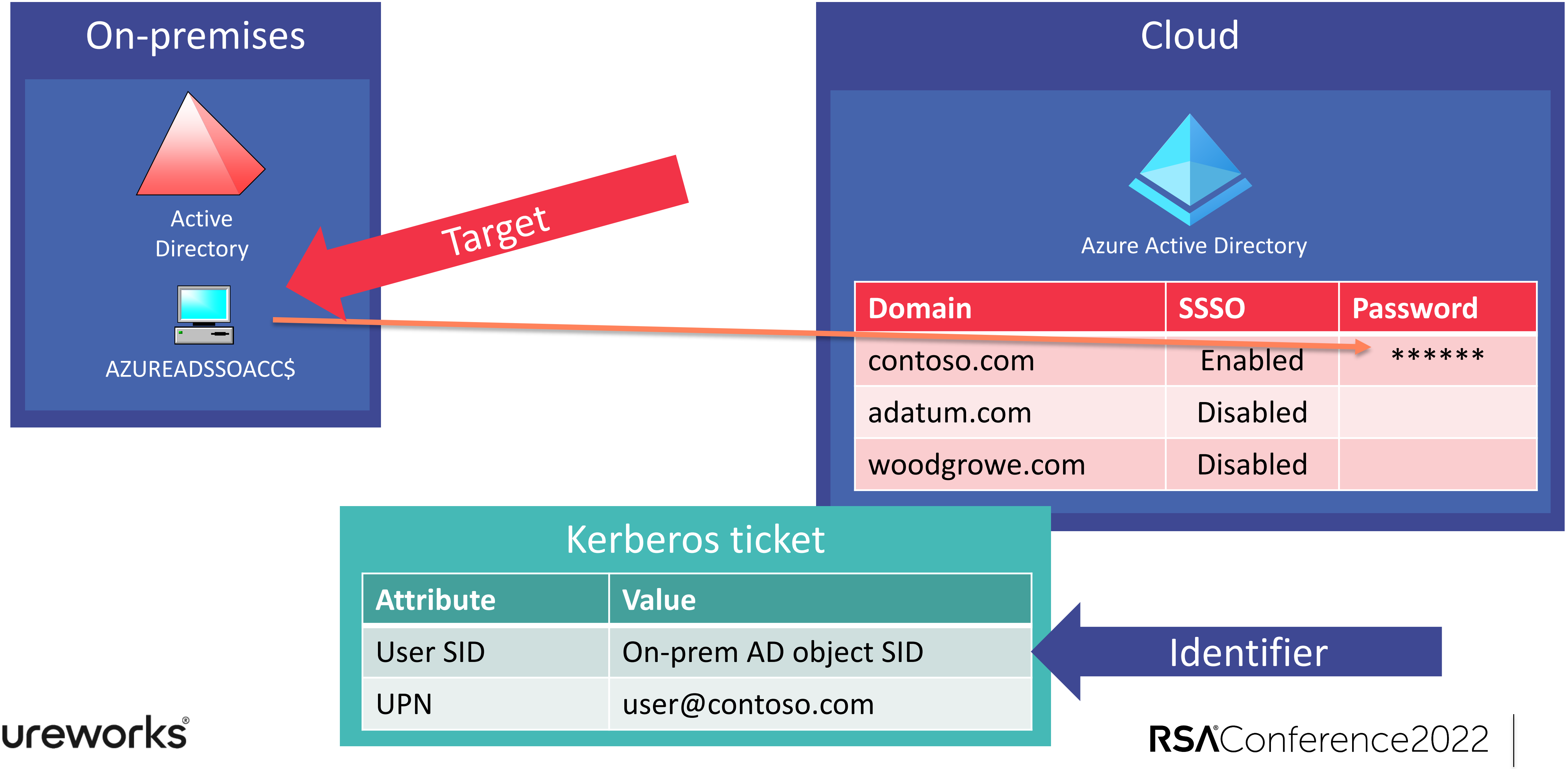
- Audience:

  https://rsac.azurewebsites.net

Pass-through Authentication hardening

- Treat PTA Agent server as Tier 0
- Limit the number of on-prem AD administrators
- Limit the number of Azure AD Global Administrators
- Use Multi-Factor Authentication (MFA)

Seamless Single-Sign-On (aka DesktopSSO)



Domain	SSSO	Password
contoso.com	Enabled	******
adatum.com	Disabled	
woodgrowe.com	Disabled	

Kerberos ticket

Attribute	Value
User SID	On-prem AD object SID
UPN	user@contoso.com

Seamless Single-Sign-On Statistics

Fortune 500 (*n*=441)		
Enabled	118	27 %
Disabled	382	73 %

Top 2000 Universities (*n*=1 892)		
Enabled	258	14 %
Disabled	1 634	86 %

Demo

- Dump AZUREADSSOACC *NTHash* with AADInternals:

  `Get-AADIntDesktopSSOAccountPassword`

- Simulate compromised AZUREADSSOACC:

  `Set-AADIntDesktopSSOEnabled`

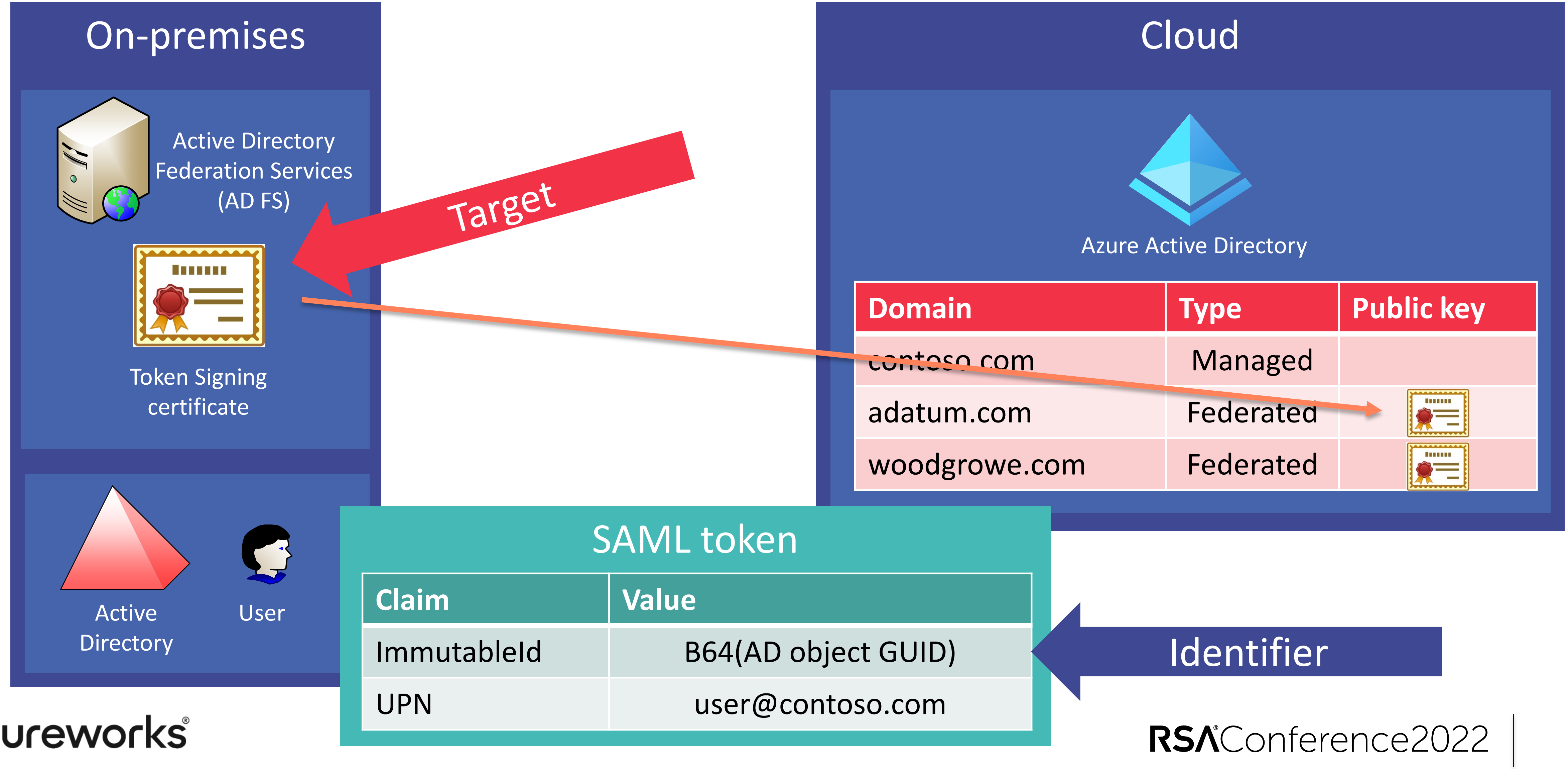
- Audience:

  https://rsac.azurewebsites.net

Seamless Single-Sign-On Hardening

- Limit the number of on-prem AD administrators
- Use Multi-Factor Authentication (MFA)

Identity Federation



Domain	Type	Public key
contoso.com	Managed	
adatum.com	Federated	📜
woodgrowe.com	Federated	📜

SAML token

Claim	Value
ImmutableId	B64(AD object GUID)
UPN	user@contoso.com

Identity Federation Statistics

Fortune 500 (*n*=441)		
Has custom domains	432	98 %
Has federated domains	293	68 %

Averages	
Number of domains	66
Number of federated domains	16

Top Universities (*n*=1892)		
Has custom domains	1 884	99,6 %
Has federated domains	535	28 %

Averages	
Number of domains	17
Number of federated domains	6

Demo

- Dump ADFS token signing certificates with AADInternals:

```
Export-AADIntADFSCertificates
```

- Simulate compromised token signing certificates:

```
Set-MsolDomainFederationSettings
```

- Audience:

  https://rsac.azurewebsites.net

Identity Federation Hardening

- Treat each AD FS server as tier 0 server
- Limit access to AD FS servers
- Close port 80 from all non-AD FS servers
- Limit the number of Azure AD Global Administrators

RSA Conference2022

Call to Action

Call to Action

- Next week:
  - Check OSINT of your own tenant to identify possible weak points
- Next month:
  - Assess the security and risk of current setup
  - Consider different authentication options
- Next two months:
  - Create a hardening and implementation plan
- Next six months:
  - Implement hardening / change authentication

RSA®Conference2022

Summary

Summary

- Hybrid Identity makes cloud easier to use and manage
  - It also means integrations to on-prem services
- Attacking on-prem environment easiest way to breach cloud
  - Protecting your on-prem services is crucial to keep your cloud safe!
- OSINT is the easiest/fastest way to check your tenant for possible attack targets
  - That’s how hackers do it anyways..
- Follow/reach out on Twitter: @DrAzureAD

RSAConference2022

Q&A