

Secureworks®

# Consequences of Trust in Azure Active Directory

---

@DrAzureAD@infosec.exchange

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

<https://aadinternals.com>



**Dr Nestori Syynimaa**

Senior Principal Security Researcher

Secureworks® CTU™

*Twitter/Mastodon:*

*@DrAzureAD@infosec.exchange*



Secureworks®

# AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
  - <https://github.com/gerenios/aadinternals>
  - <https://aadinternals.com/aadinternals>
- MITRE ATT&CK
  - <https://attack.mitre.org/software/S0677/>



## Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

---

# Contents

- Concept of Trust
- Introduction to Azure AD
- Consequences of Trust in Azure AD
  - Paula's top 10, #8: Trusting solutions without knowing how to break them

Secureworks®

# Concept of Trust

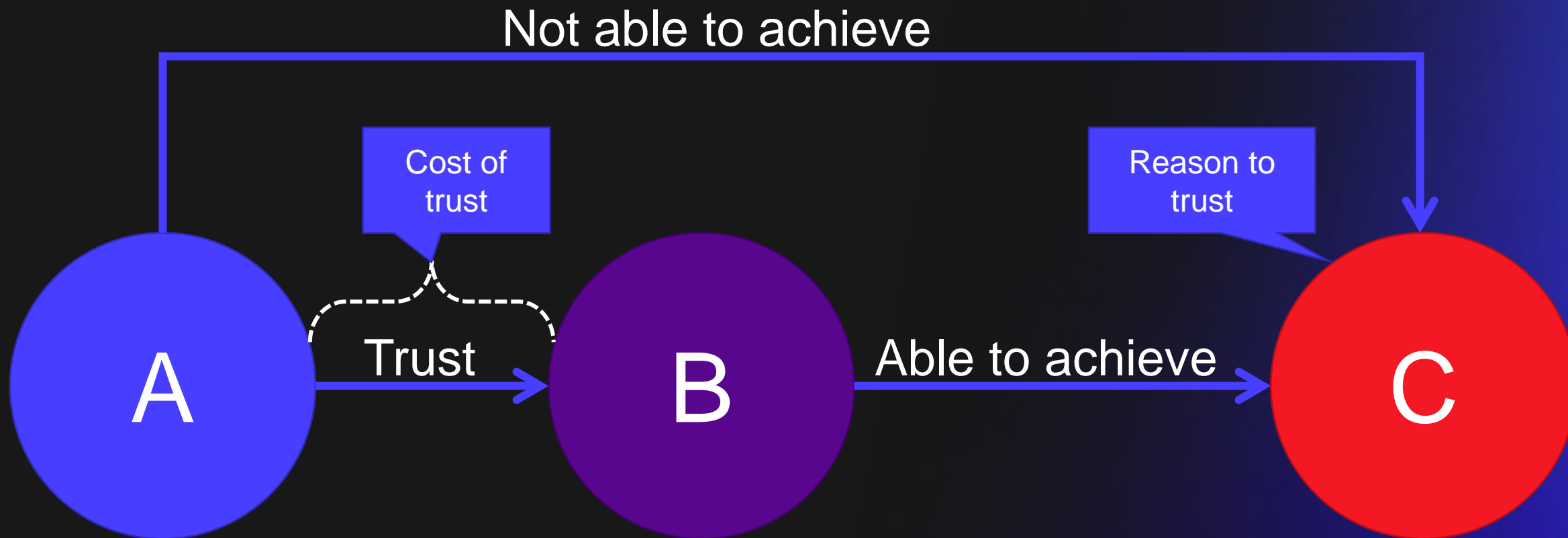
---

# Trust

- a) acceptance of dependency in
- b) the absence of information about the other's reliability in order to
- c) create an outcome otherwise unavailable

Barbalet, Jack. (2009). A characterization of trust, and its consequences. *Theory and Society*, 38(4), 367-382. doi:10.1007/s11186-009-9087-3

# Basis of trust



# Trust assessment framework

- Reason to trust = *Why*
- Cost of trust
  - Level of control or power = *What*
  - Guardrails = *Constraints*
- *Best Practices*



Secureworks®

# Azure Active Directory

---

---

# Azure Active Directory

- Cloud based Identity and Access Management (IAM) solution
- Used by Microsoft Azure & Microsoft 365 + thousands 3<sup>rd</sup> parties

# Usage statistics

<b>Fortune 500</b>		
Has Azure AD Tenant	441	88 %
Has federated domains ( <i>n</i> =441)	293	68 %
Uses Seamless SSO ( <i>n</i> =441)	118	27 %

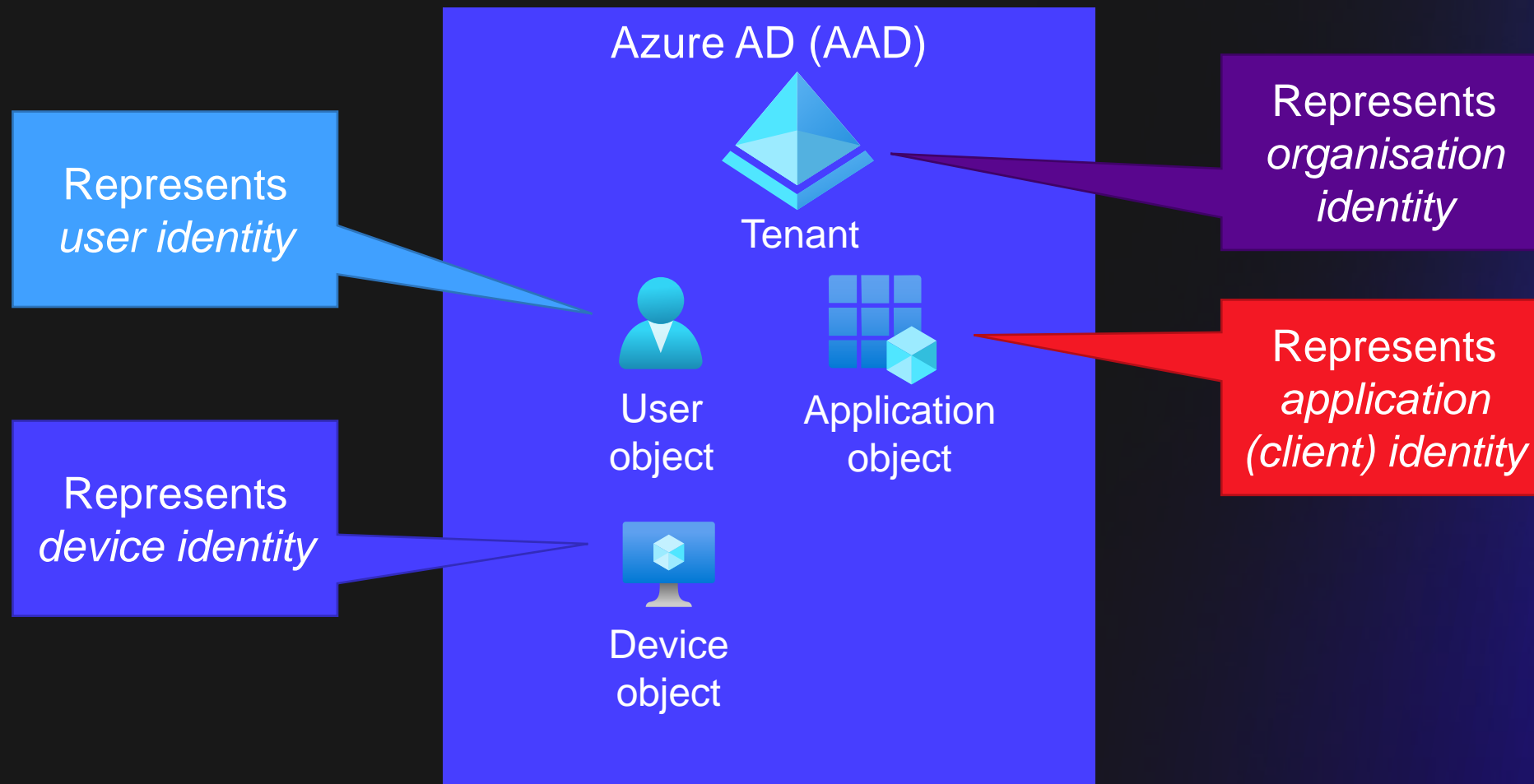
<b>Finland 500</b>		
Has Azure AD Tenant	492	98 %
Has federated domains ( <i>n</i> =492)	160	35 %
Uses Seamless SSO ( <i>n</i> =492)	191	39 %

<b>Top Universities (<i>n</i>=2000)</b>		
Has Azure AD Tenant	1892	95 %
Has federated domains ( <i>n</i> =1892)	293	28 %
Uses Seamless SSO ( <i>n</i> =1892)	258	14 %

<b>Estonian municipalities (<i>n</i>=79)</b>		
Has Azure AD Tenant	67	85 %
Has federated domains ( <i>n</i> =67)	13	19 %
Uses Seamless SSO ( <i>n</i> =67)	1	1 %

<b>Finnish municipalities (<i>n</i>=302)</b>		
Has Azure AD Tenant	301	100 %
Has federated domains ( <i>n</i> =301)	78	26 %
Uses Seamless SSO ( <i>n</i> =301)	94	31 %

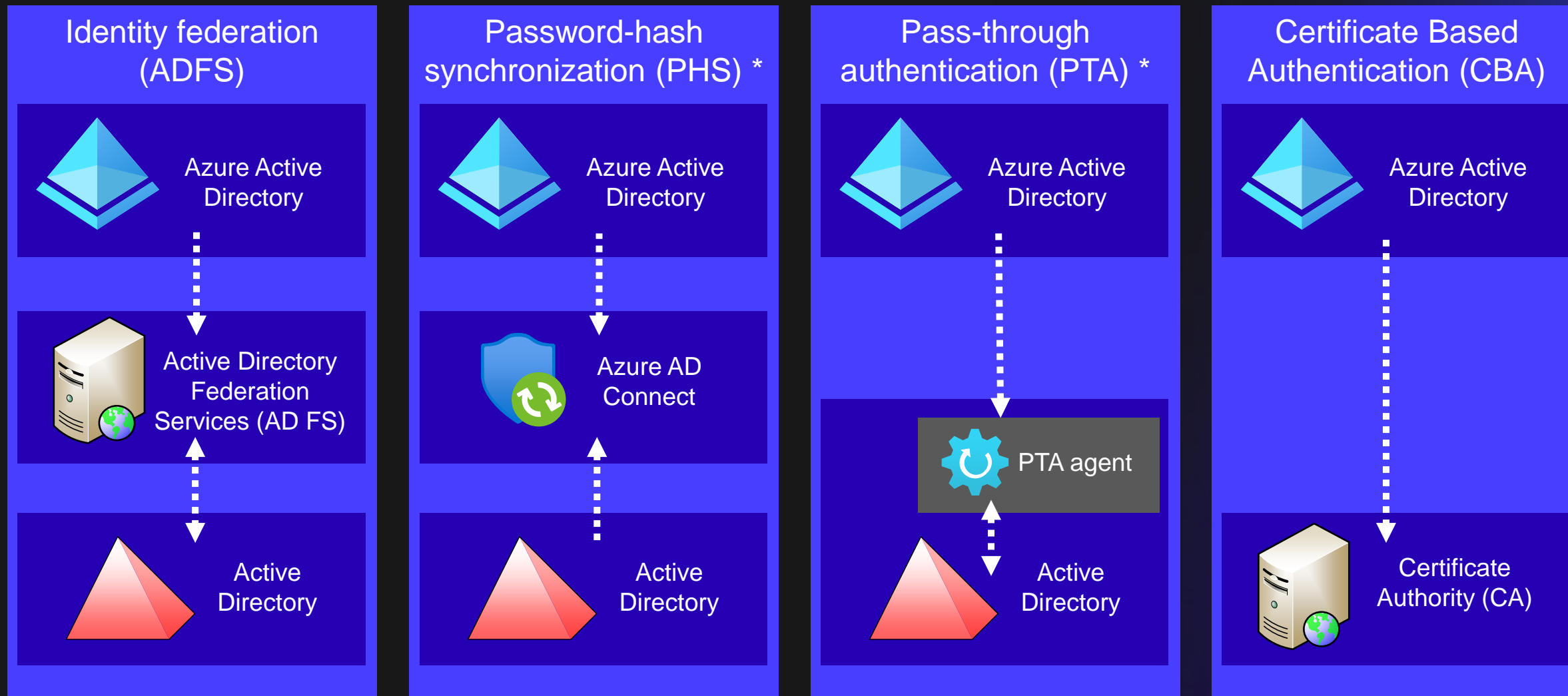
# Azure AD identities



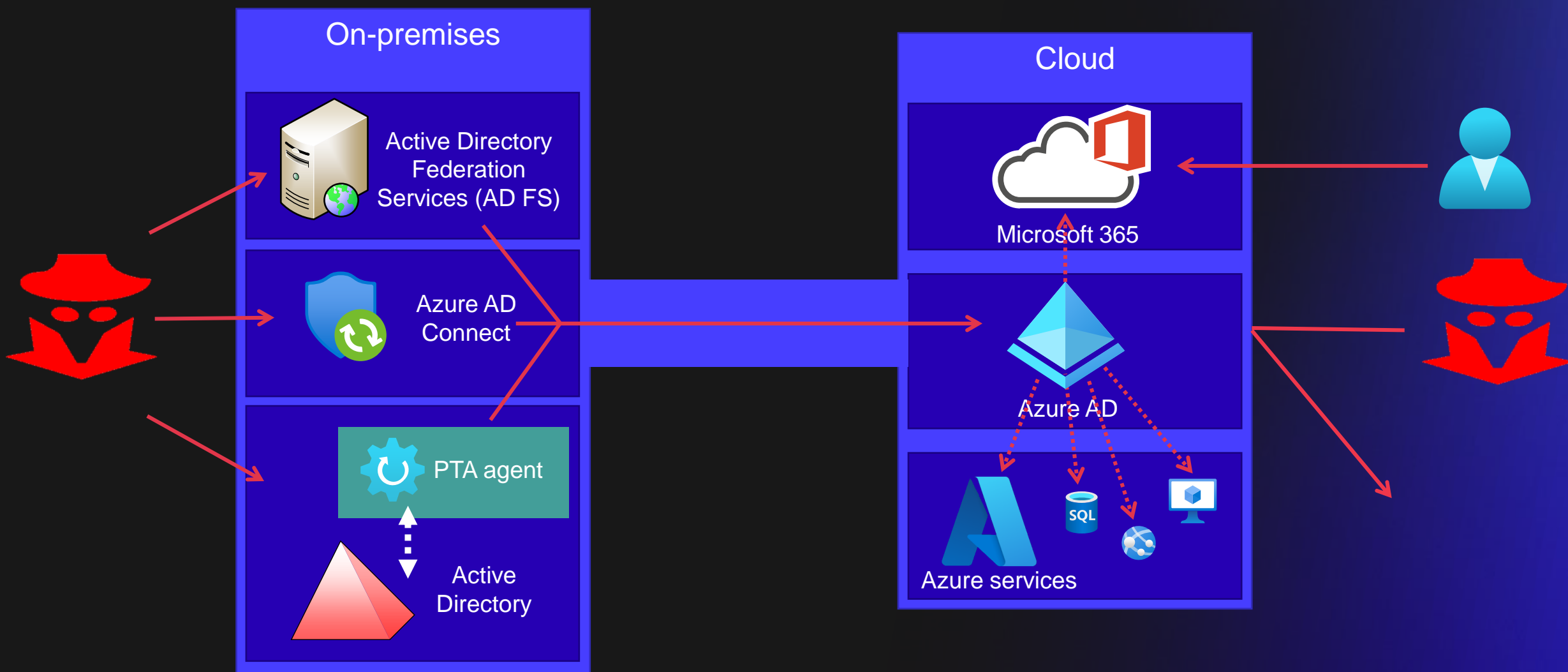
# Proof of identity

Proof of identity	User	Device	App/client
Username + password (ROPC)	X		X
Authenticator	X		
FIDO2	X		
Kerberos ticket (Seamless SSO)	X		
SAML token (federated identity)	X		
Primary Refresh Token (PRT)	X	X	
Refresh token	X	X	
Windows Hello for Business	X	X	
Certificate	X	X	X

# Hybrid Authentication Options

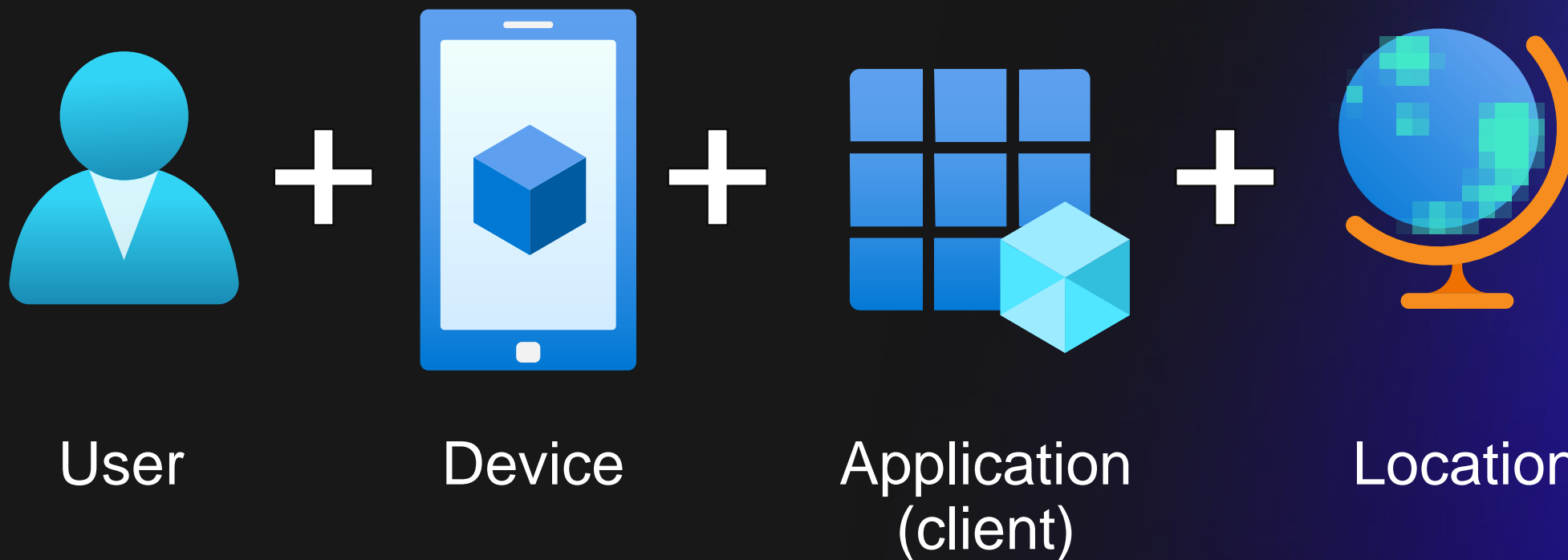


# (Hybrid) Cloud Security



# Conditional Access

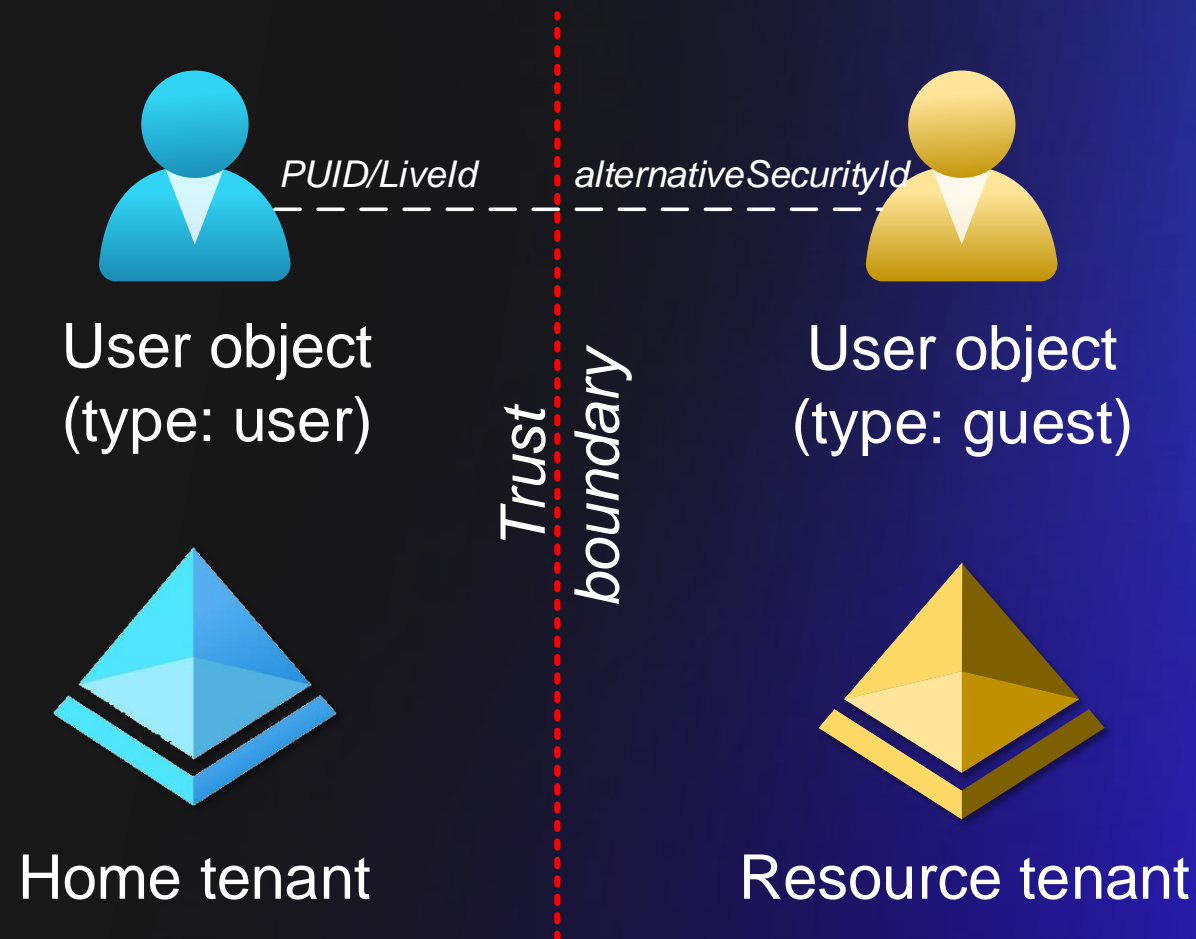
- Grant / block access based on conditions
- Outside signals:





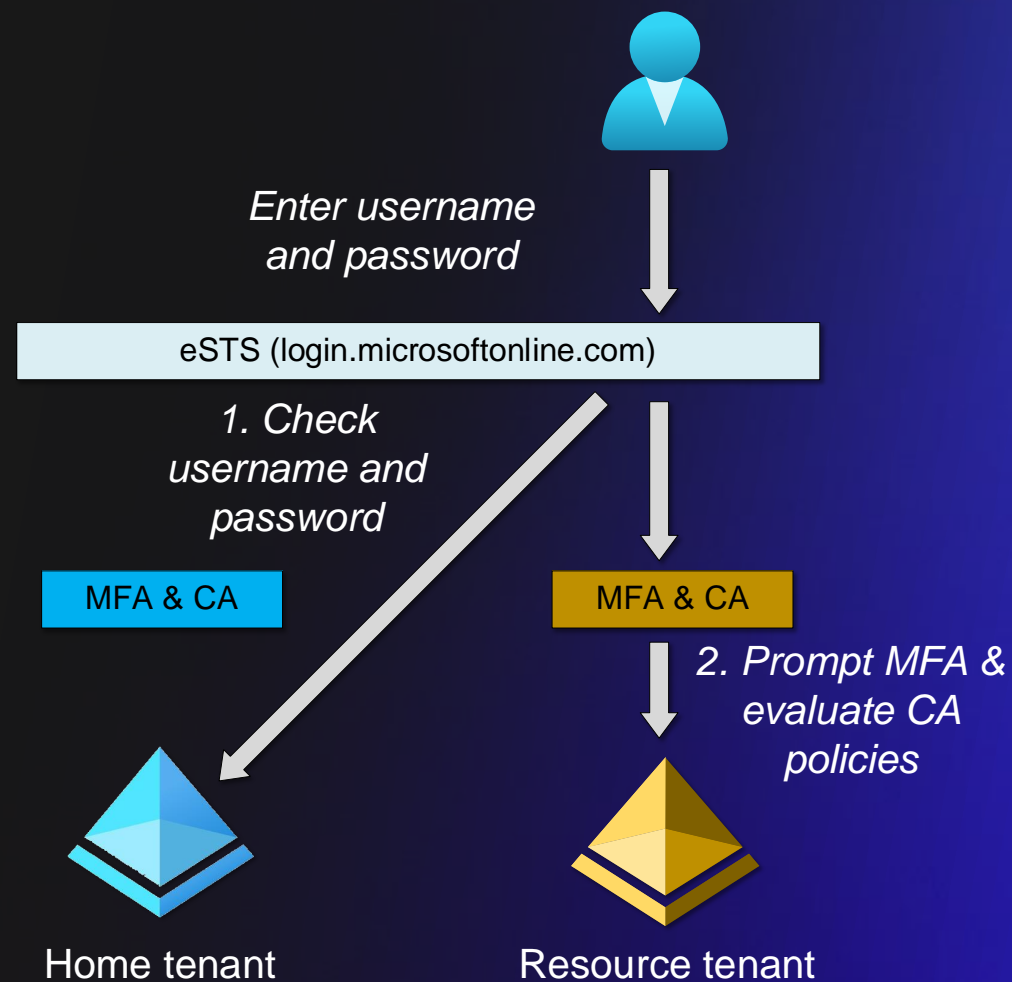
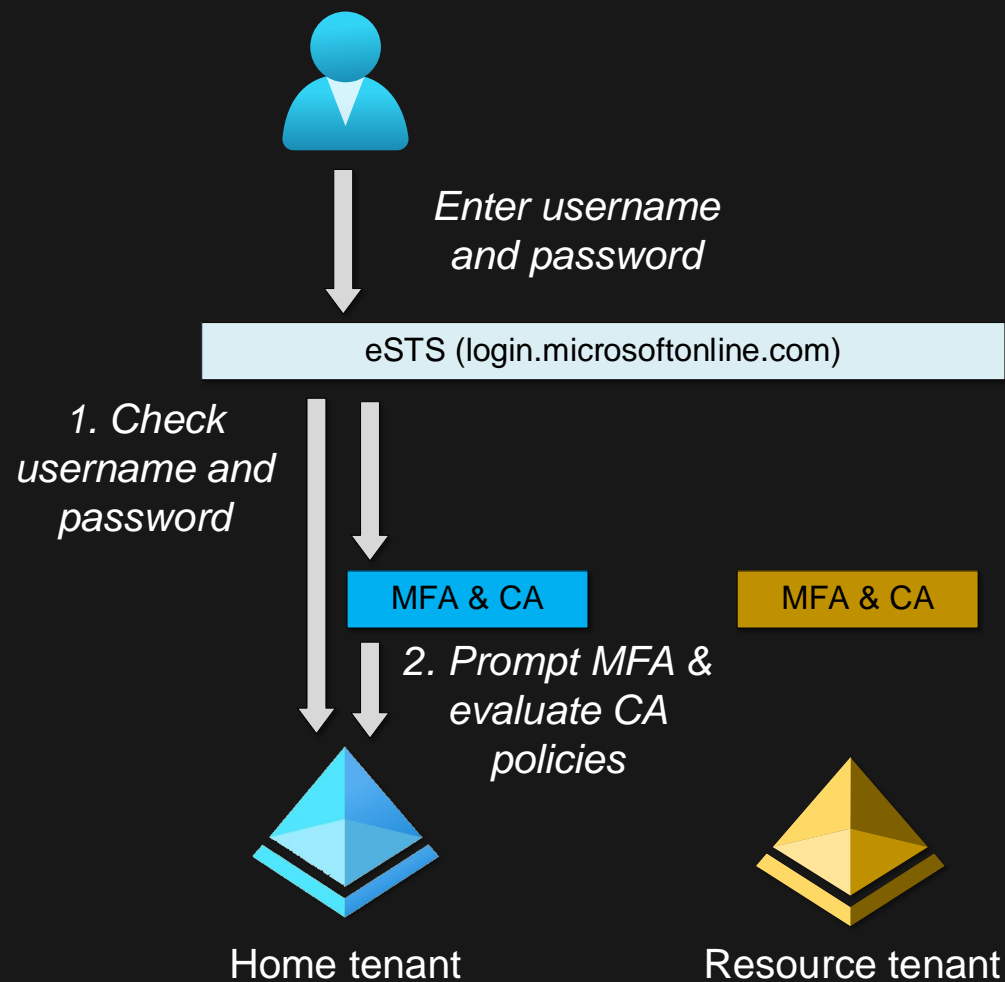
# Home & Resource tenants

- Home Tenant = your tenant
- Resource Tenant = tenant where you are a guest



<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/multi-tenant-user-management-introduction#terminology>

# MFA & CA evaluation



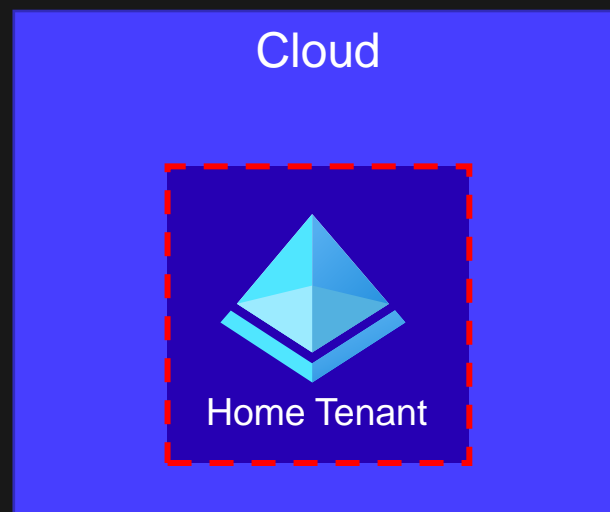
Secureworks®

# Consequences of Trust in Azure AD

---

# Internal Trust

- Trust boundary = Home Tenant

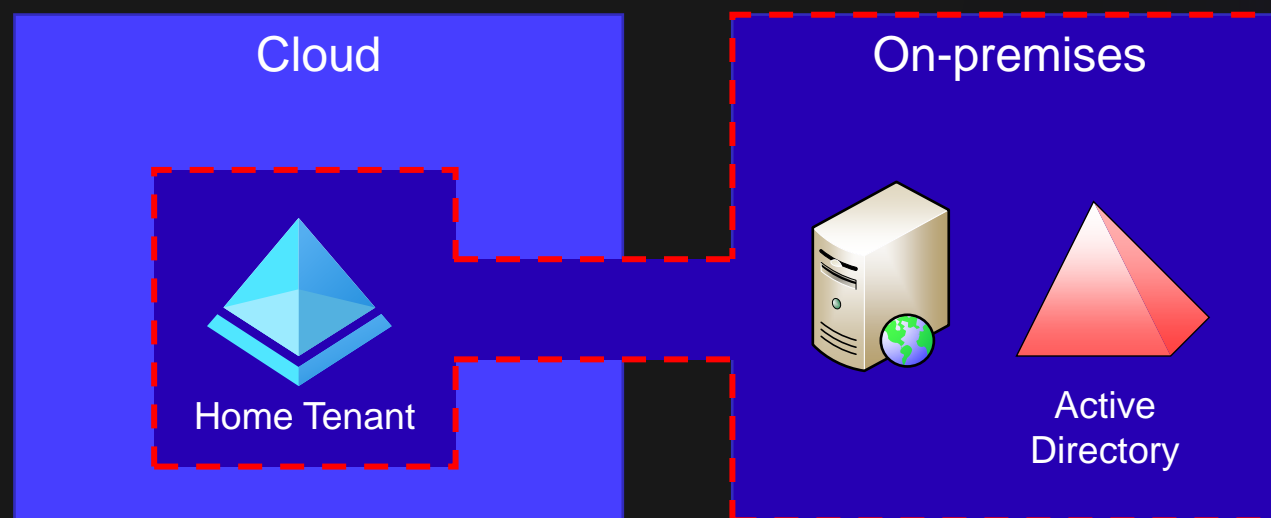


# Internal Trust

Trust	Why	What	Constraints	Best Practices
Users	Access services	Permissions, Roles	AuthN, AuthZ, CA	Least-Privilege
Administrators	To perform administrative tasks	Permissions, Roles	AuthN, AuthZ, CA	Least-Privilege
Apps	To perform activities	Permissions, Roles	AuthN, AuthZ	Least-Privilege
Devices	Access services	(H)AADJoin	AuthZ, CA	Zero Trust (only allow admins to join)

# Hybrid Trust

- Trust boundary = Home Tenant + on-premises Hybrid components

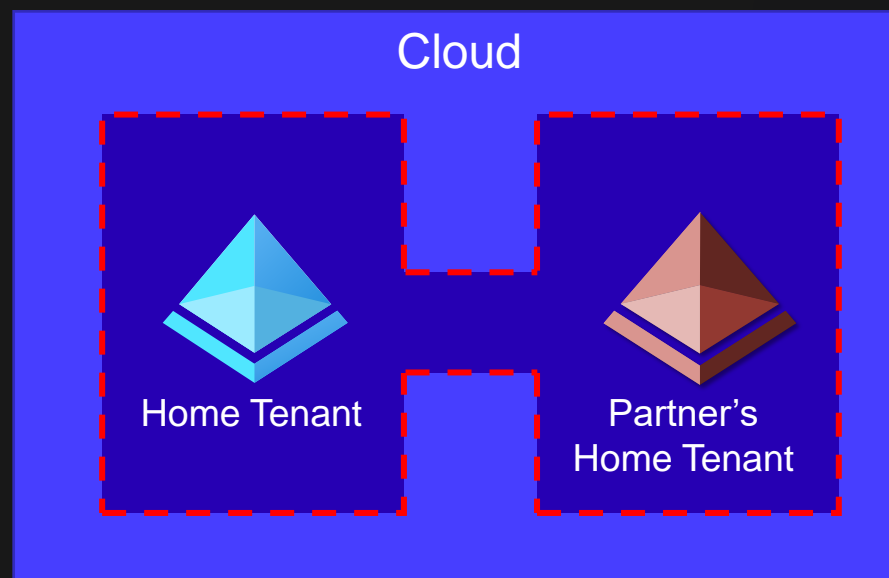


# Hybrid Trust

Trust	Why	What	Constraints	Best Practices
Azure AD Connect	Synchronise objects from on-prem AD to Azure AD	Roles	AuthZ, CA	Tier-0, Least-Privilege
AD FS	Identity Federation, ease of use	Certificate(s)	CA, Tenant settings	Tier-0, HSM, do not trust IdP MFA claims
PTA	Login using on-prem credentials	Certificate	CA	Tier-0, <i>don't use</i>
SSSO	Ease of use	Kerberos	AuthN, CA	Use PRT based SSO
CBA	Strong authentication	Certificate	AuthZ, CA	CRL

# Partner Trust

- Trust boundary = Home Tenant + partner's Home Tenant





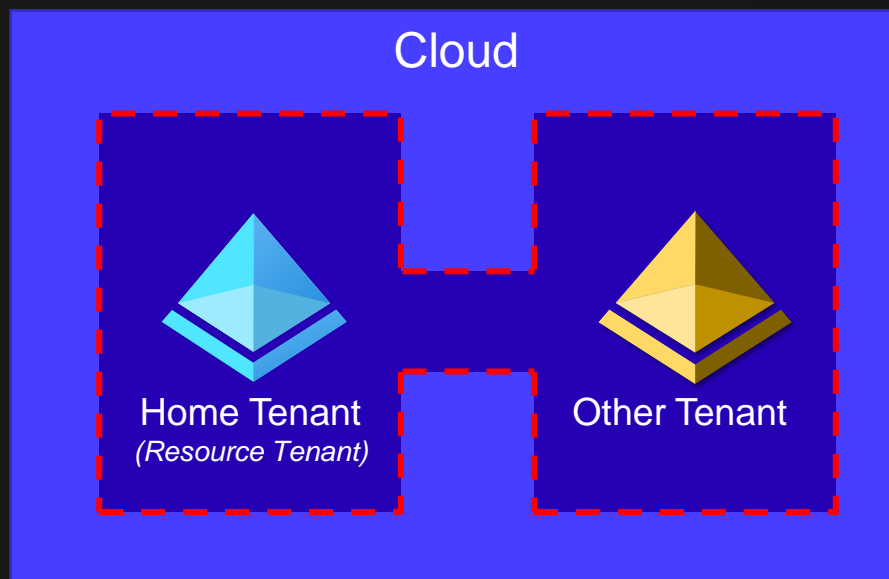
# Partner Trust

Trust	Why	What	Constraints	Best Practices
DAP <sup>1</sup>	Allow partner to perform administrative tasks	Roles (Global / Helpdesk admin) to all partner's users	Accept or deny the partner organisation	<b>Do not use!</b> Use GDAP or dedicated admin accounts.
GDAP <sup>2</sup>	Allow partner to perform administrative tasks	Roles	Accept or deny per user	Least-privilege, use dedicated admin accounts.

1. [Delegated Admin Permissions](#)
2. [Granular Delegated Admin Permissions](#)

# Cross-tenant Trust

- Trust boundary = Home Tenant + Other Tenant



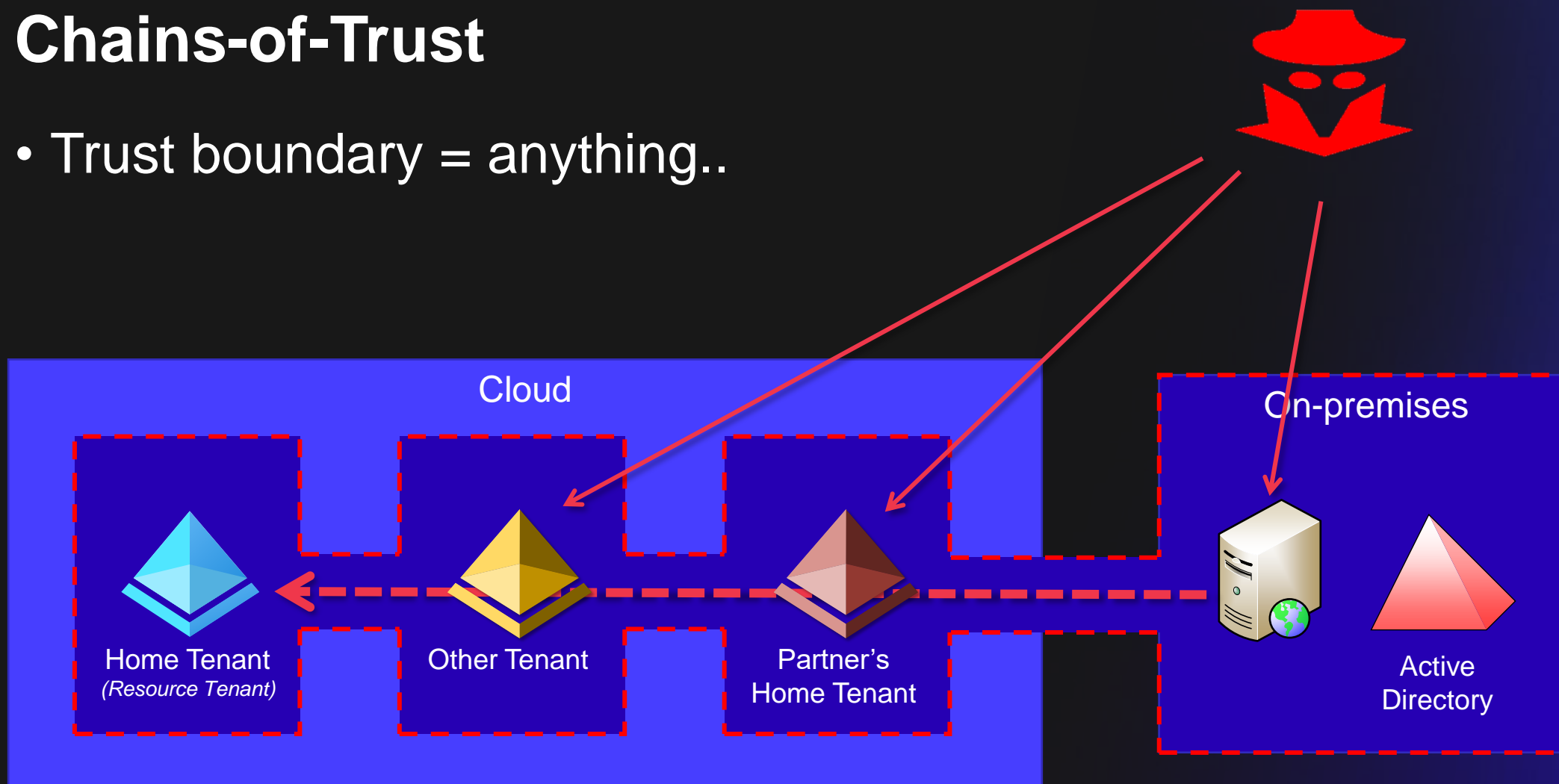
# Cross-tenant Trust

Trust	Why	What	Constraints	Best Practices
Cross-tenant access settings	Ease cross-tenant access	Trust other tenant's MFA, device compliance, and HAADJ status	Per tenant configuration	Use only with M&A
Cross-tenant synchronisation	Ease cross-tenant collaboration	Sync home tenant users to resource tenant(s) as guests	Per tenant configuration	Use only with M&A

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/cross-tenant-access-overview>

# Chains-of-Trust

- Trust boundary = anything..



Secureworks®

# Summary

---

## Summary

- There are a lot of new features introduced to Azure AD
- Apply best practices
- Evaluate the ***cost of trust*** of each used feature on regular basis!
- Evaluate available ***constraints*** and apply accordingly
- Audit trusts of your partners and trusted tenants
- Admin rights != Human rights\*

\* *Sami Laiho*

Secureworks®