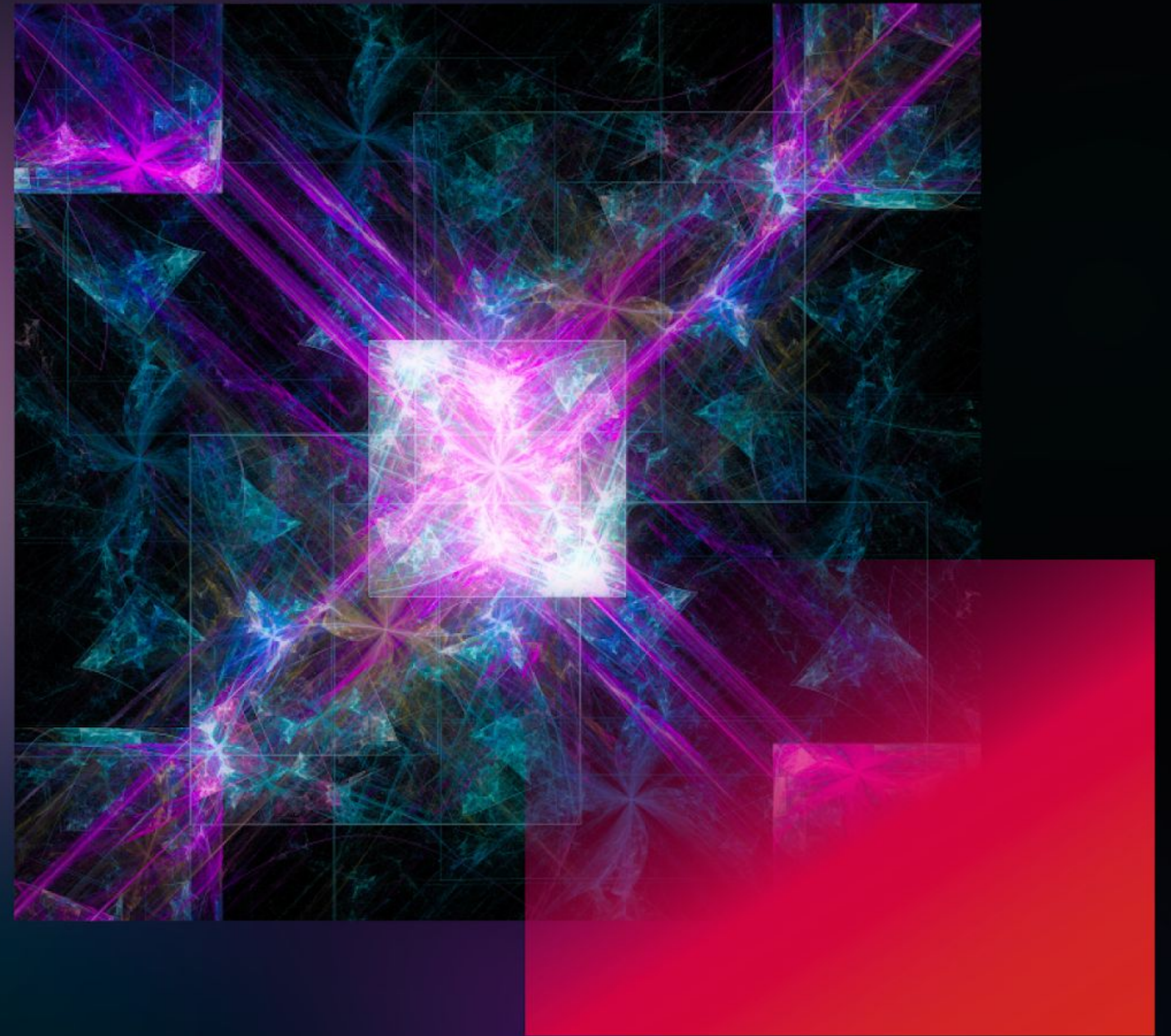


Rochester Security Summit 2023

What Cyberattackers See: Top Tips for Minimizing Your Identity Attack Surface





What Cyberattackers See: Top Tips for Minimizing your Identity Attack Surface

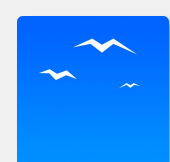


Eric Woodruff

Product Technical Specialist

Microsoft Security MVP

IDPro Certified Identity Professional
(CIDPRO)



@ericonidentity.c
om



/in/msfthike
r



ericonidentity.c
om



@msft_hik
er

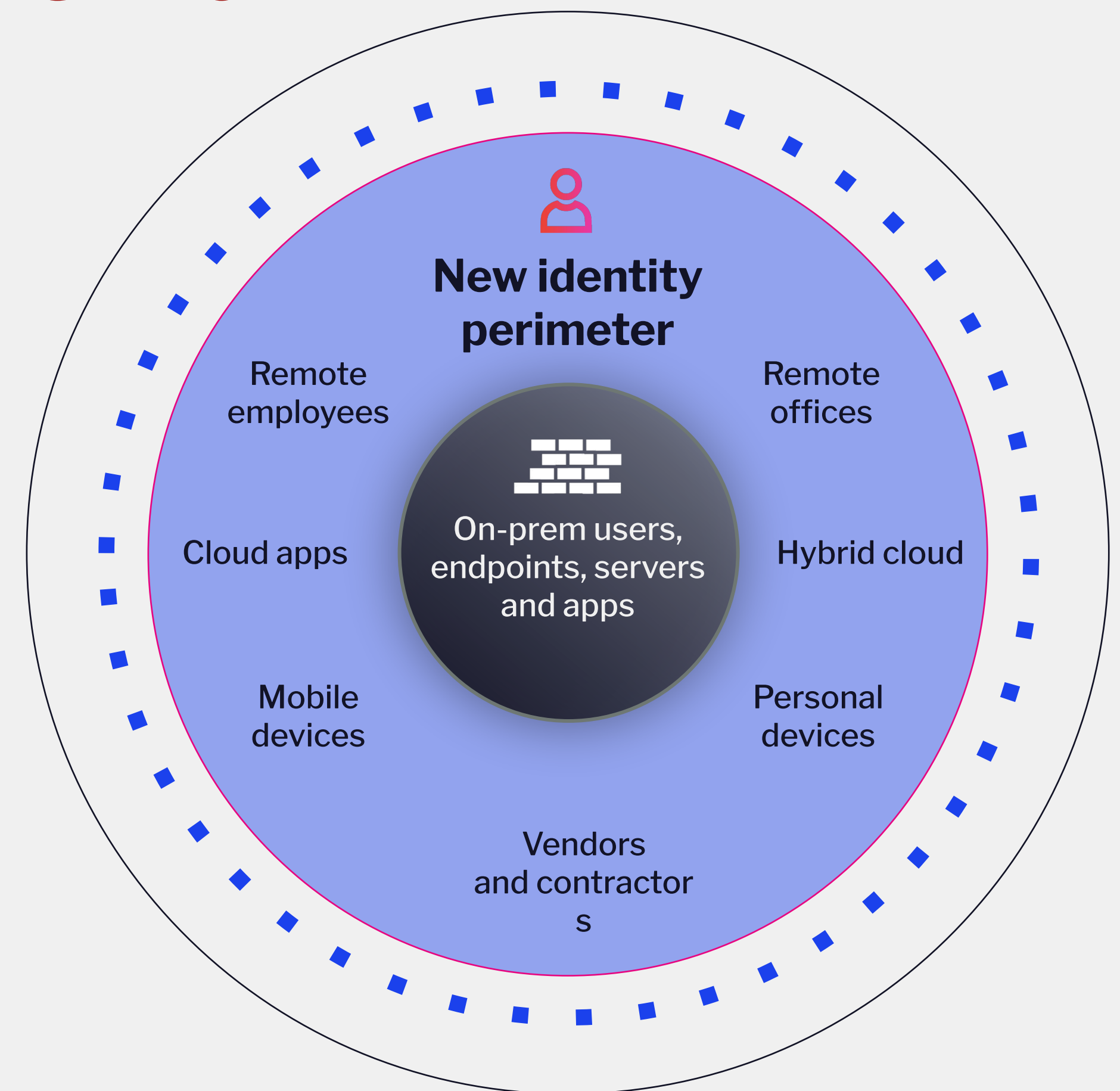


@ericonidentity@infosec.excha
nge

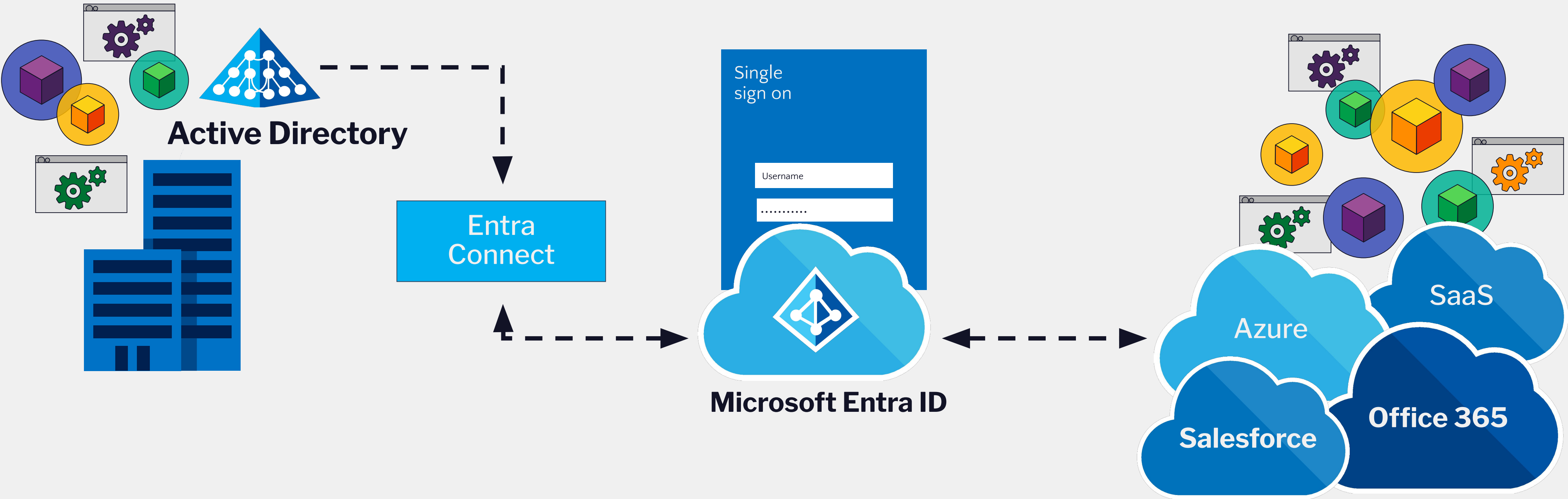
Addivitijis est amoris et caritatis
preferentia

Identity has become **fundamental**

1. Keeping legacy environments secure
2. Enabling digital transformation
3. Is the ❤️ of Zero Trust



The Complexities of Hybrid Identity



If Active Directory isn't secure, **nothing is**





... attacks like ransomware are the second stage, predicated by an identity compromise.

Microsoft



**Attackers are targeting Active Directory
and the identity infrastructure with
phenomenal success.**

Gartner

Results of an **attack** on Active Directory

Active Directory can't be trusted

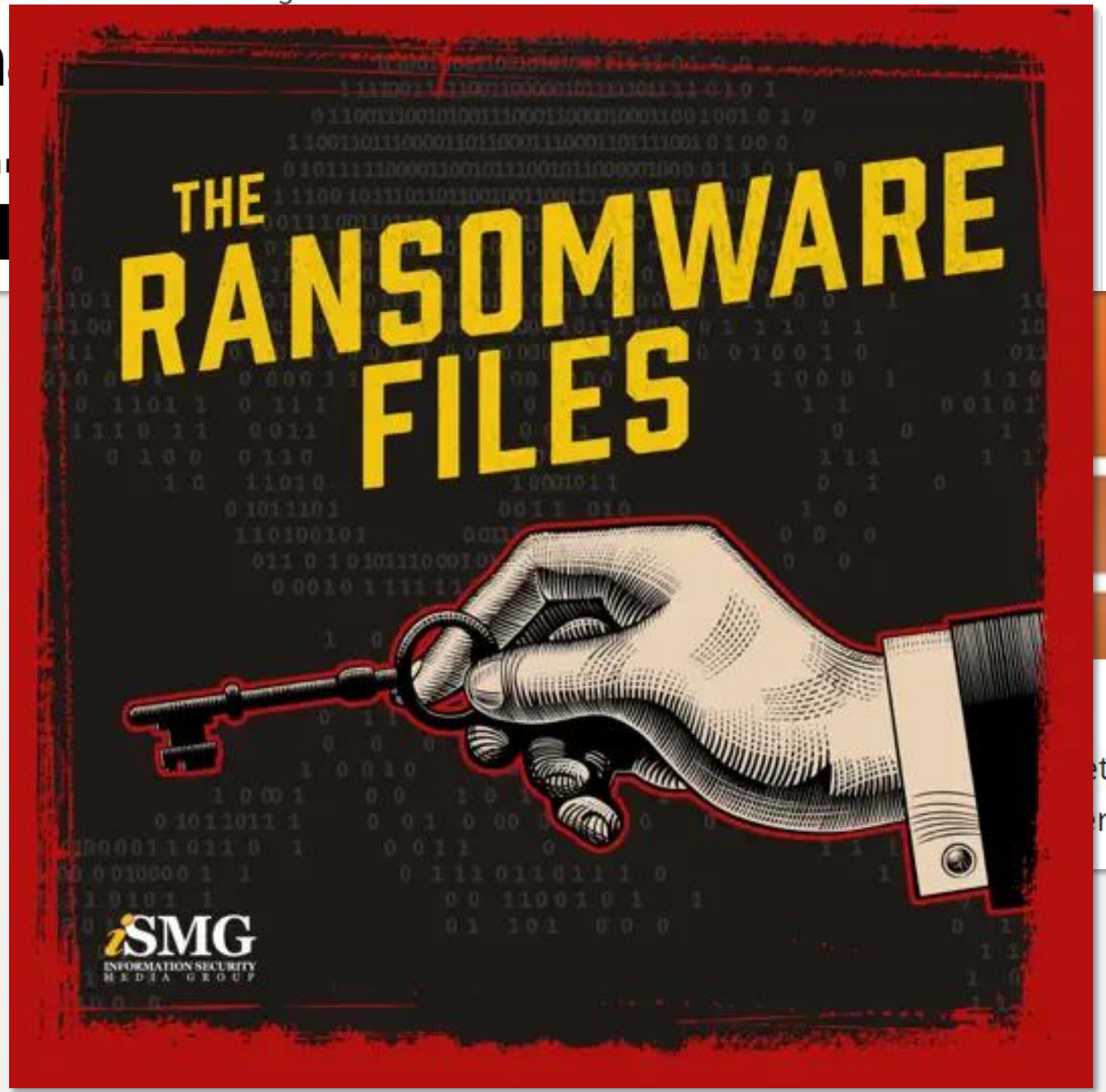
- Malware on Domain Controller restores
- Backdoor accounts after eviction
- Owning one Domain Controller owns the entire directory

← Ads by Google

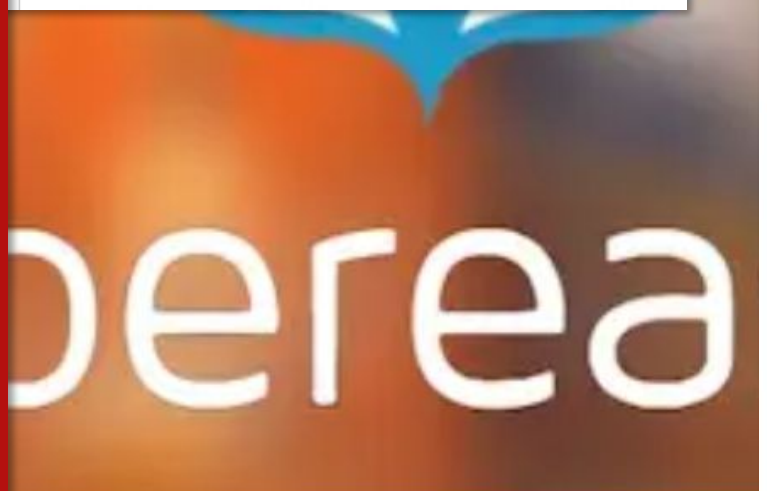
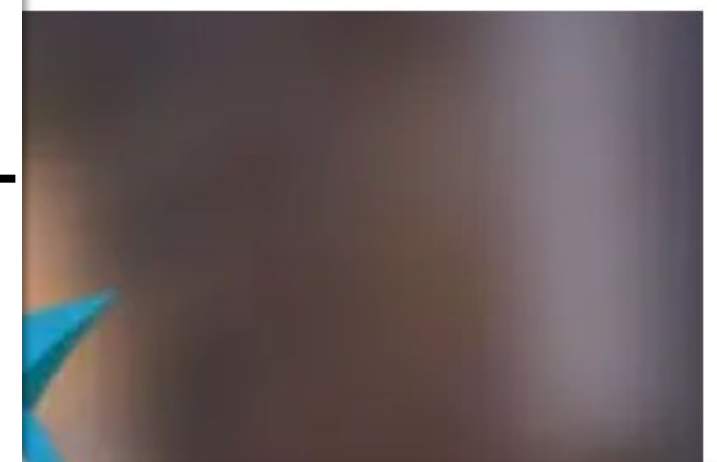
Stop seeing this ad Why this ad? ▸

Business >> Casinos & Gaming

An \$4 cycl



ve Directory Domain in



trator compromised the Active Dire
ral movement in fewer than 60 min

Multinational tech firm ABB hit by Black Basta ransomware attack

By Lawrence Abrams

May 11, 2023 05:05 PM 0



Swiss multinational company ABB, a leading electrification and automation technology provider, has suffered a Black Basta ransomware attack, reportedly impacting business operations.

To what extent would your company be impacted if an attack took out Active Directory?

1. Minimal impact (can recover AD quickly)
2. Some impact
3. Significant impact
4. Catastrophic impact
5. 🙄

Improving
Active
Directory
Security



Implement strong
identity processes

Improving
Active
Directory
Security



Implement Active Directory Forest Trust Security

- Ensure SID filtering is active across all trusts between forests
- Consider using selective authentication

Improving
Active
Directory
Security



Secure Kerberos

- Reset the KRBTGT account password annually
- Remove SPNs assigned to administrators
- Eliminate unconstrained delegation

Improving
Active
Directory
Security

4

Deter Lateral Movement

- Implement LAPS on all servers and clients
- Limit Local Administrator group membership

Improving
Active
Directory
Security



Secure privileged users and groups

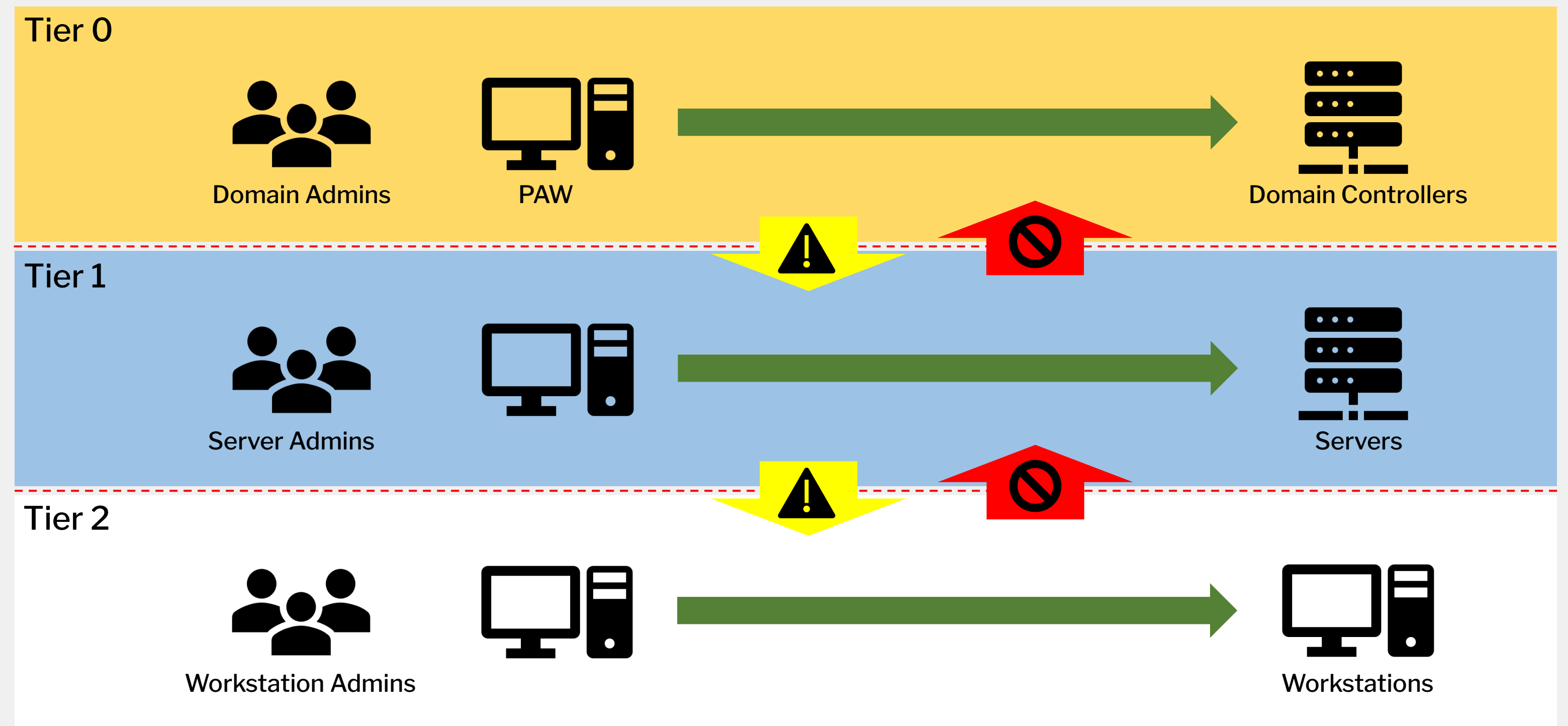
- Limit privileged service accounts
- Monitor for permission changes on AdminSDHolder object

Improving
Active
Directory
Security

6

**Harden privileged
access**

Improving Active Directory Security

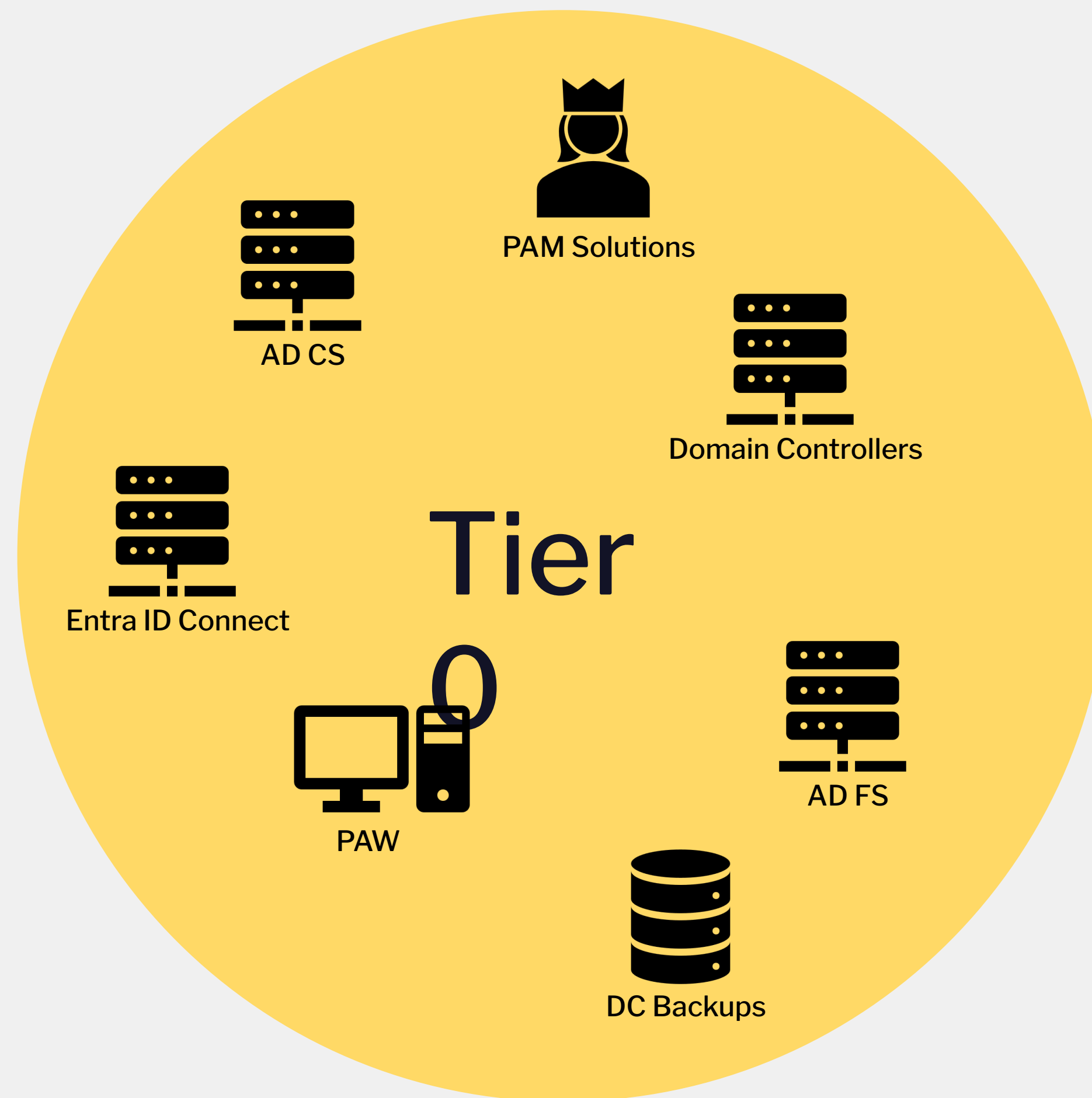


Improving
Active
Directory
Security



Secure Tier 0 dependencies

Improving Active Directory Security



Improving
Active
Directory
Security



Harden domain controllers

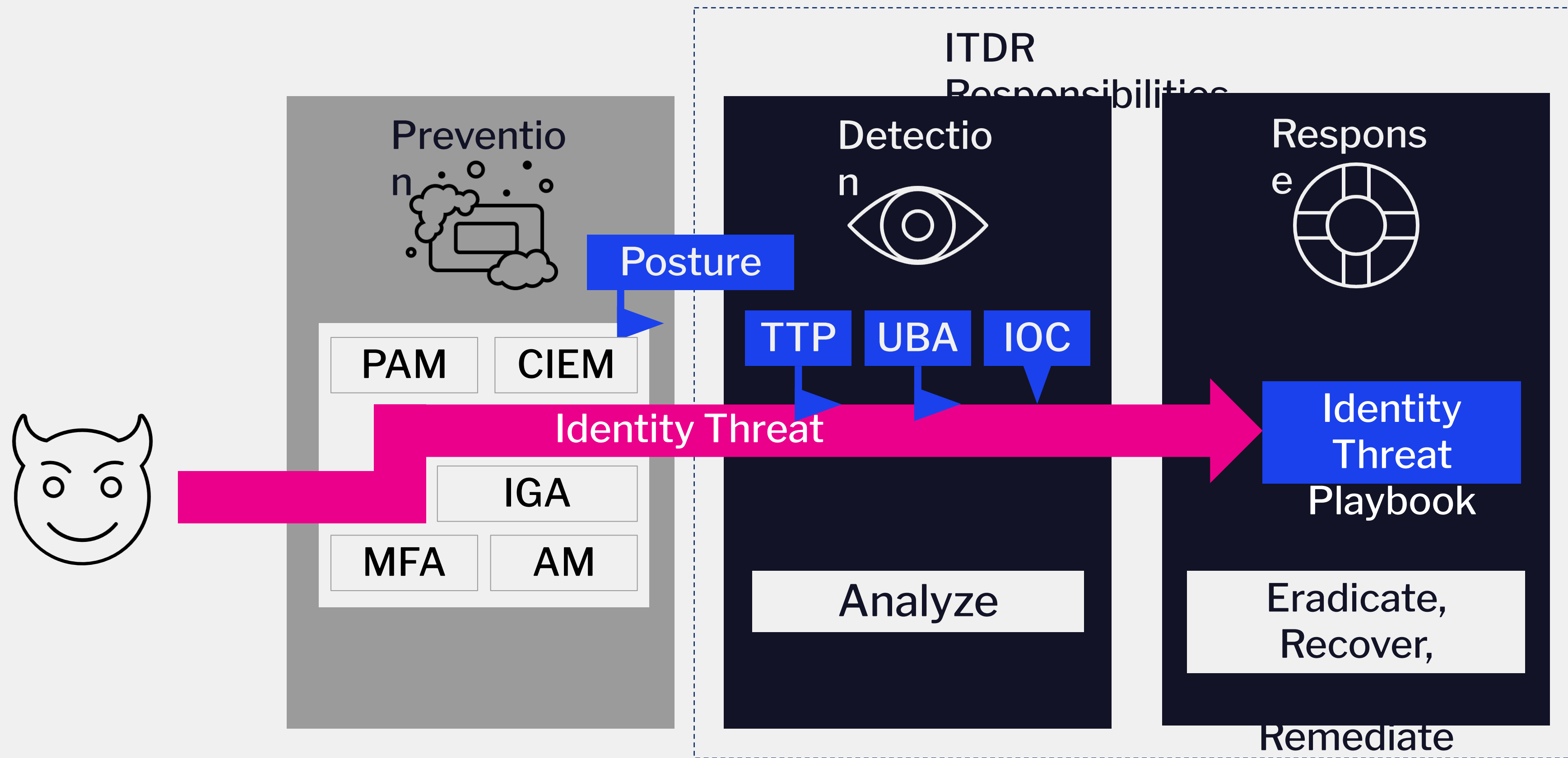
- Remove unnecessary roles and agents
- Consider using server core
- Apply hardening policies

Improving
Active
Directory
Security



**Monitor for unusual
activity**

Improving Active Directory Security



Gartner ITDR Model

Improving
Active
Directory
Security

10

Backup Active
Directory... and
ensure you can
recover

How frequently is your Active Directory DR process tested?

1. During an actual production recovery
2. Every 1-2 years
3. Every 6-12 months
4. DR plan created but never tested
5. No Active Directory DR plan exists
6. 🙄

Active
Directory DR
Backup and
Recovery



Backup every
domain, especially
the root

Active
Directory DR
Backup and
Recovery

2

**Backup two or more
DCs per domain**

Active
Directory DR
Backup and
Recovery

3

Test your backups
regularly

Active
Directory DR
Backup and
Recovery

4

Use supported
backup methods

Active
Directory DR
Backup and
Recovery

5

Ensure backups are
malware free

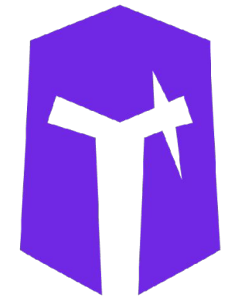
Active
Directory DR
Backup and
Recovery



**Keep offline or air
gaped copies**

Preparing for Active Directory Recovery

1. Know your AD topology
2. Know your DNS topology
3. Minimize OS versioning differences
4. Know the Microsoft AD Forest Recovery Guide



purple knight

powered by  semperis

Perform an AD Security Assessment

Purple Knight is a free AD, Entra ID, and Okta security assessment tool

SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 07/12/22 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Azure AD tenant, or both.

Active Directory forest: Purple Knight queried the Active Directory environment and ran a series of security indicator scripts against domains within the selected forest (see Appendix 1 – Domains list for a full list of the domains included in the assessment).

Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering Active Directory and Azure AD security weaknesses, this assessment report provides valuable insight into the overall security posture across your hybrid identity environment and presents opportunities to minimize the attack surface and stay ahead of the ever-changing threat landscape.

[View Appendix 1 - Domains list](#)



ACTIVE DIRECTORY



AZURE AD

Forest	f4.lab
No. of Domains	1
Duration	00:00:24.9367601
Run by	F4\Administrator

Indicators	
Evaluated	97
Not selected	1
IOEs found	39
Passed	58
Failed to run	0
Not Relevant	1
Canceled	0

Tenant	Semperis F4 Hybrid
Application ID	dde0a18cd-cb2d-4ff3-95ce-8ee909df8e13
Duration	00:00:04.4430073
Run by	F4\Administrator

Indicators	
Evaluated	10
Not selected	0
IOEs found	6
Passed	4
Failed to run	0
Not Relevant	0
Canceled	0

Understand your AD Attack Paths

Forest Druid is a free AD, Entra ID, and Okta security assessment tool

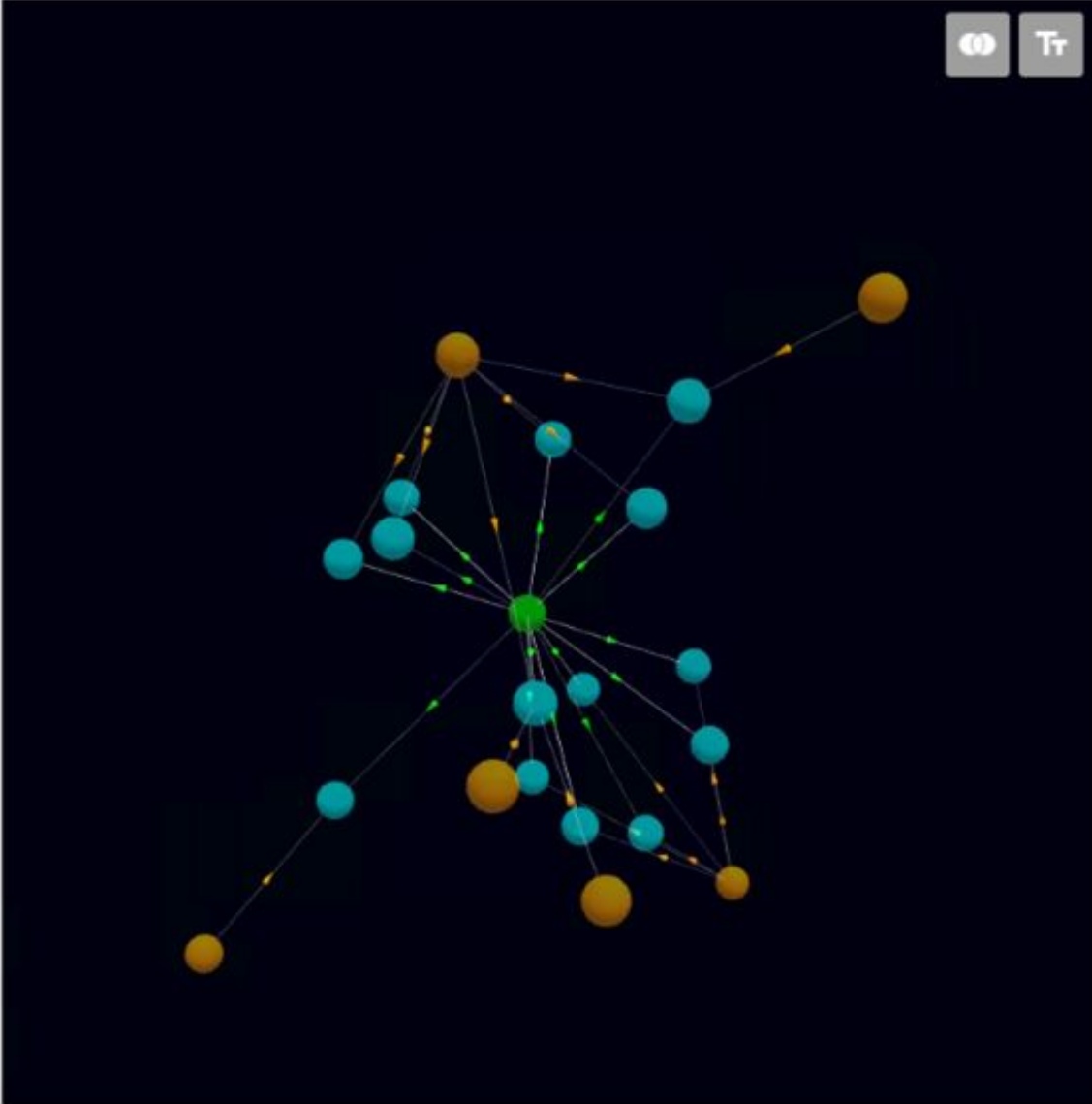
Unclassified privilege escalation relationships: 17

Only Privilege Escalation No target filtering

Classify as: TIER 0 RISKY EXPORT Legend: Default Tier 0 Tier 0 Risky

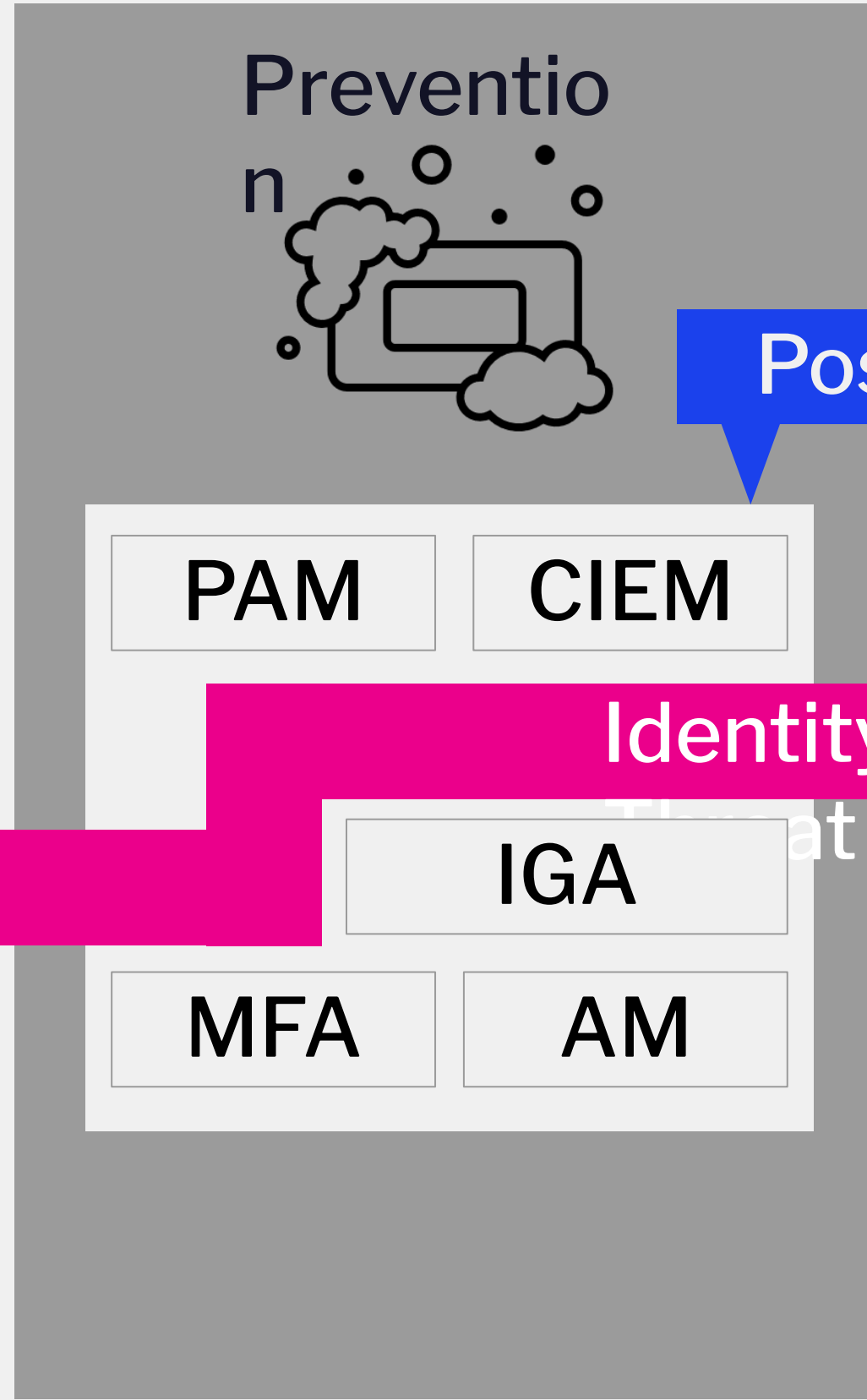
<input type="checkbox"/>	Name	Type	Relation	Target Name	Target Type
<input type="checkbox"/>	Builtin	builtinDomain	Contains	Administrators	group
<input type="checkbox"/>	Users	container	Contains	Domain Admins	group
<input type="checkbox"/>	ForeignSecurityPrincipals	container	Contains	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	foreignSecurityPrincipal
<input type="checkbox"/>	Users	container	Contains	Domain Controllers	group
<input type="checkbox"/>	F127-D02-DC02	computer	PrimaryGroup	Domain Controllers	group
<input type="checkbox"/>	F127-D02-DC01	computer	PrimaryGroup	Domain Controllers	group
<input type="checkbox"/>	Users	container	Contains	krbtgt	user
<input type="checkbox"/>	Builtin	builtinDomain	Contains	Account Operators	group
<input type="checkbox"/>	Users	container	Contains	f127d02admin	user
<input type="checkbox"/>	Users	container	Contains	Group Policy Creator Owners	group
<input type="checkbox"/>	Users	container	Contains	Read-only Domain Controllers	group
<input type="checkbox"/>	NT AUTHORITY\SYSTEM	undefined	Owner	DnsAdmins	group
<input type="checkbox"/>	Users	container	Contains	DnsAdmins	group
<input type="checkbox"/>	Builtin	builtinDomain	Contains	Server Operators	group
<input type="checkbox"/>	Builtin	builtinDomain	Contains	Print Operators	group
<input type="checkbox"/>	Builtin	builtinDomain	Contains	Backup Operators	group
<input type="checkbox"/>	Builtin	builtinDomain	Contains	Remote Desktop Users	group

1-17 of 17



Questions

?



Posture

