semperis

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

Eric Woodruff

SENIOR SECURITY RESEARCHER

ericw@semperis.com

KKR

INSIGHT PARTNERS

Microsoft Partner

Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell
Microsoft Intelligence Security Association (MISA)

TOP 5 FASTEST-GROWING CYBERSECURITY COMPANIES

3 YEARS IN A ROW OF DOUBLE-DIGIT GROWTH

NAMED TO FORTUNE'S CYBER 60 2024 LIST

2 CONSECUTIVE YEARS ON THE LIST

#14 ON DUN'S 100 2022 RANKING OF BEST STARTUPS

150+ COMBINED YEARS OF MICROSOFT MVP EXPERIENCE

EY HONORS SEMPERIS CEO MICKEY BRESMAN

TOP 10 OF US 100 FASTEST-GROWING VETERAN-OWNED BUSINESSES

semperis

Active Directory and Zero Trust

semperis

I ❤️ Active Directory and Entra ID

semperis

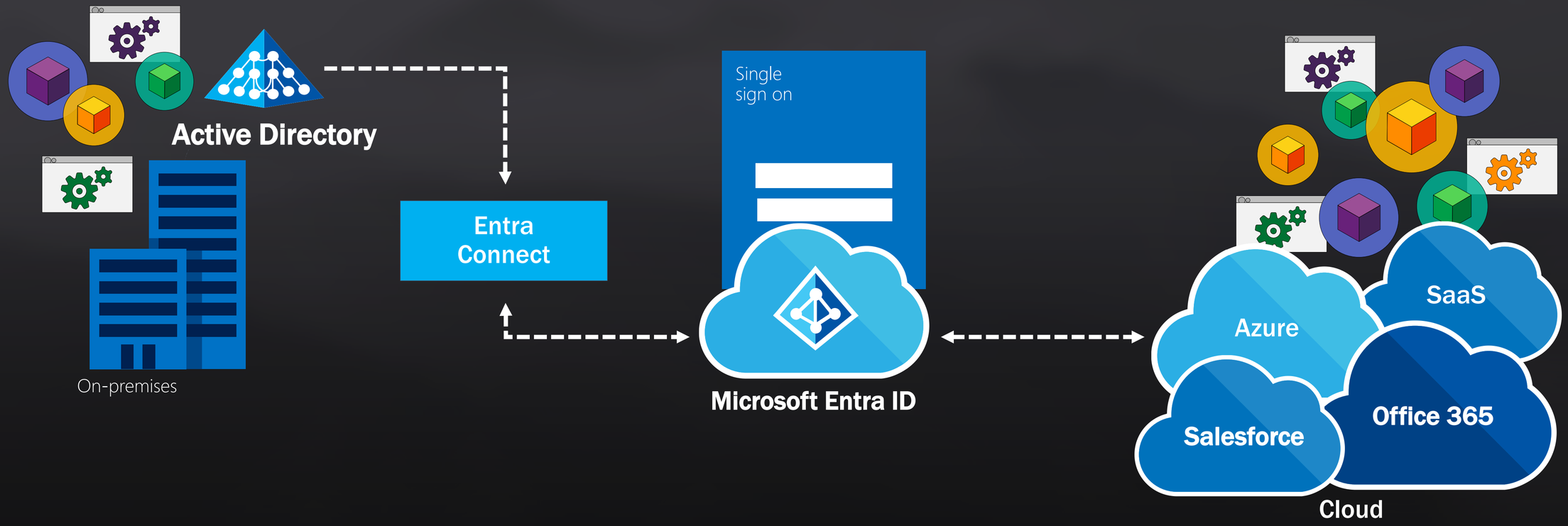
SECURITY CHALLENGES

Protect the shifting & expanding enterprise

1. Keep legacy environments secure
2. Enable digital transformation
3. Security consolidation & automation

semperis

The Complexities of Hybrid Identity



semperis

If Active Directory isn't secure, nothing is

semperis

Why is AD-specific security a must?

semperis

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

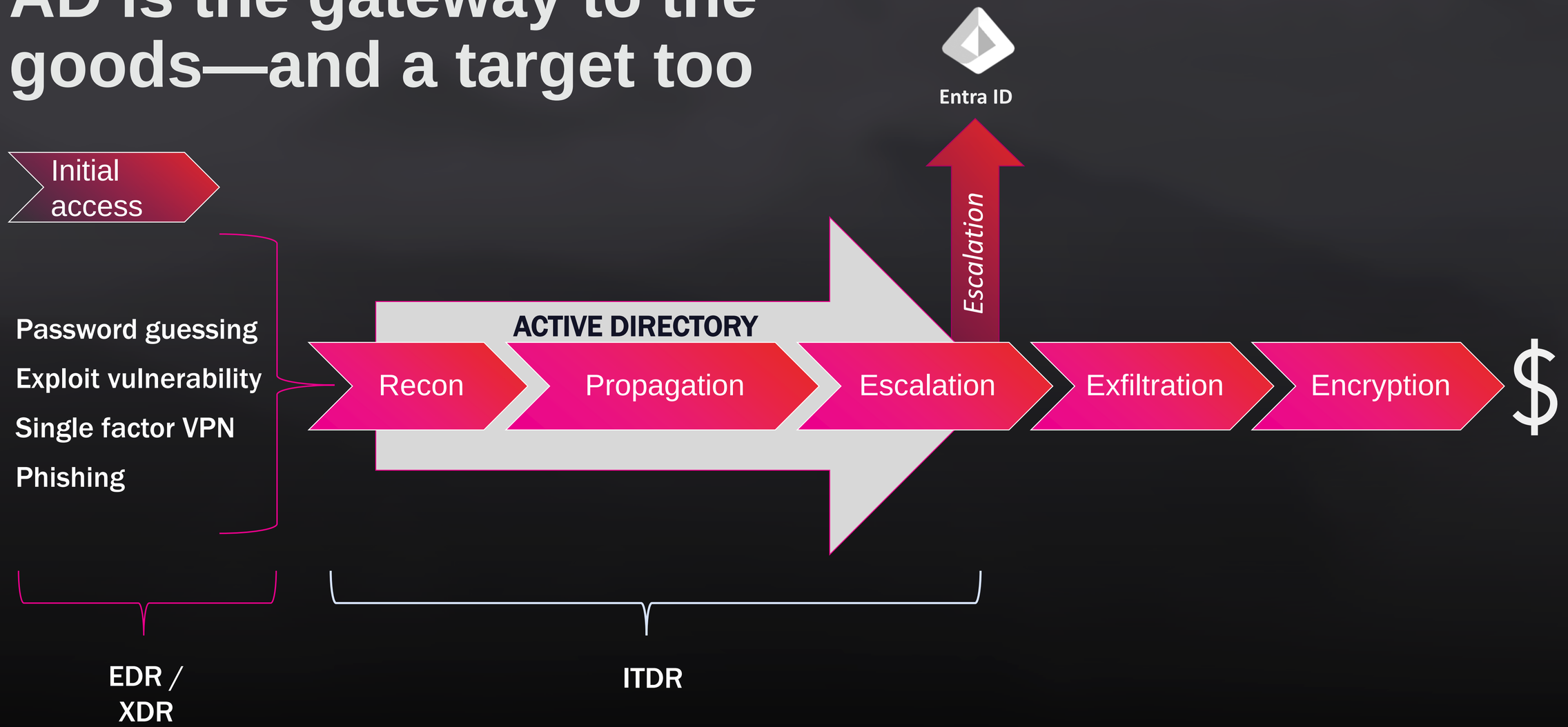
Gartner

semperis

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

semperis

AD is the gateway to the goods—and a target too



semperis

Results of an attack on AD

The AD servers can’t be trusted

- 2022 malware dwell time
  - 20-52 days (Sophos)
- Useful AD backups ~< 14 days
  - ➢ Conventionally restored domain controllers (DCs) = persistent malware

The AD service can’t be trusted

- Backdoor accounts
- Installed malware requires DC admin rights
  - ➢ Admin rights on 1 DC = access to entire forest

semperis

Hybrid identity threats and risks

semperis

Improving Active Directory Security

1

Implement strong identity processes

semperis

Improving Active Directory Security

2

Implement Active Directory Forest Trust Security

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

semperis

Improving Active Directory Security

3

Secure Kerberos

- Create a process to rotate the KRBTGT account password
- Remove SPNs assigned to administrators
- Eliminate unconstrained delegation

semperis

Improving Active Directory Security

4

Deter Lateral Movement

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

semperis

Improving Active Directory Security

5

Secure privileged users and groups

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

semperis

Improving Active Directory Security

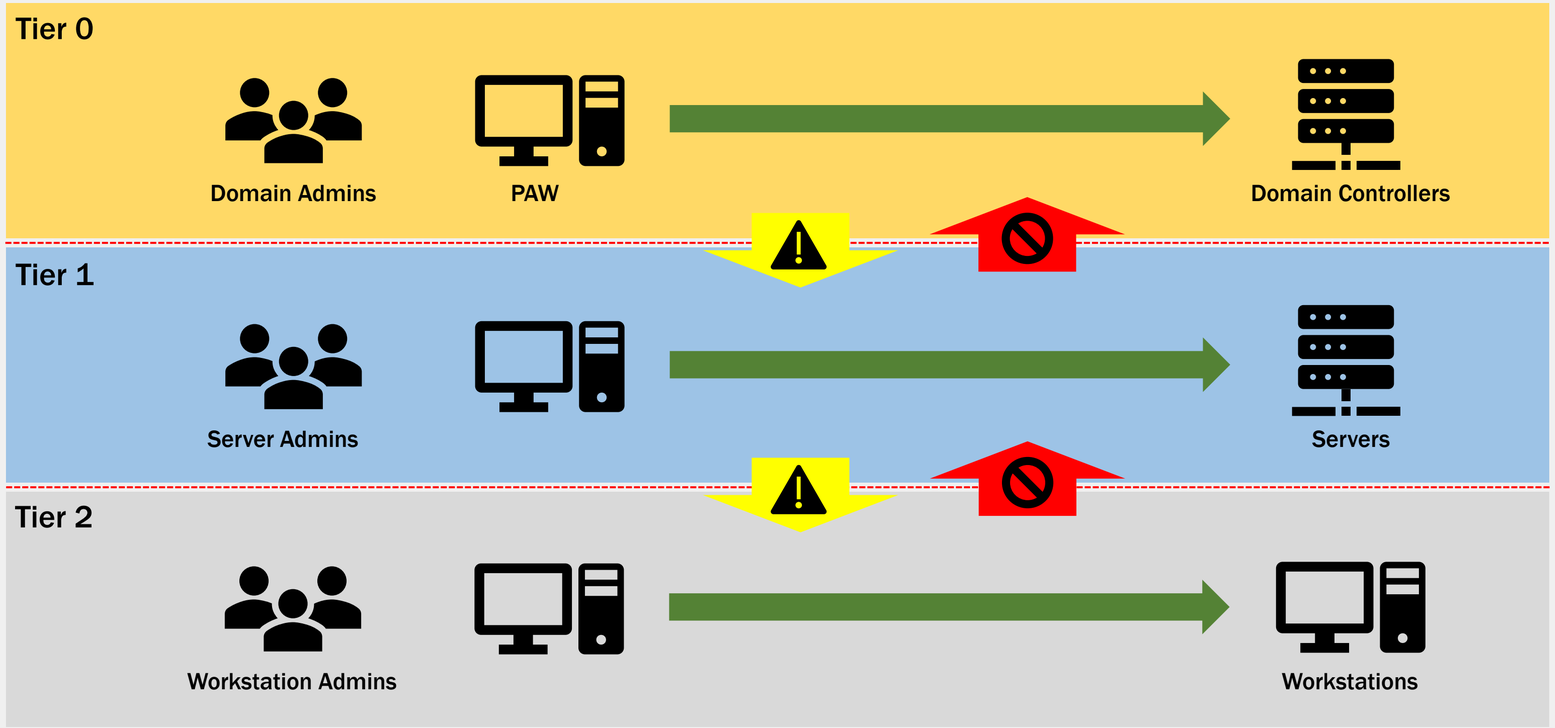
6

Harden privileged access

semperis

Improving Active Directory Security

6



semperis

Improving Active Directory Security

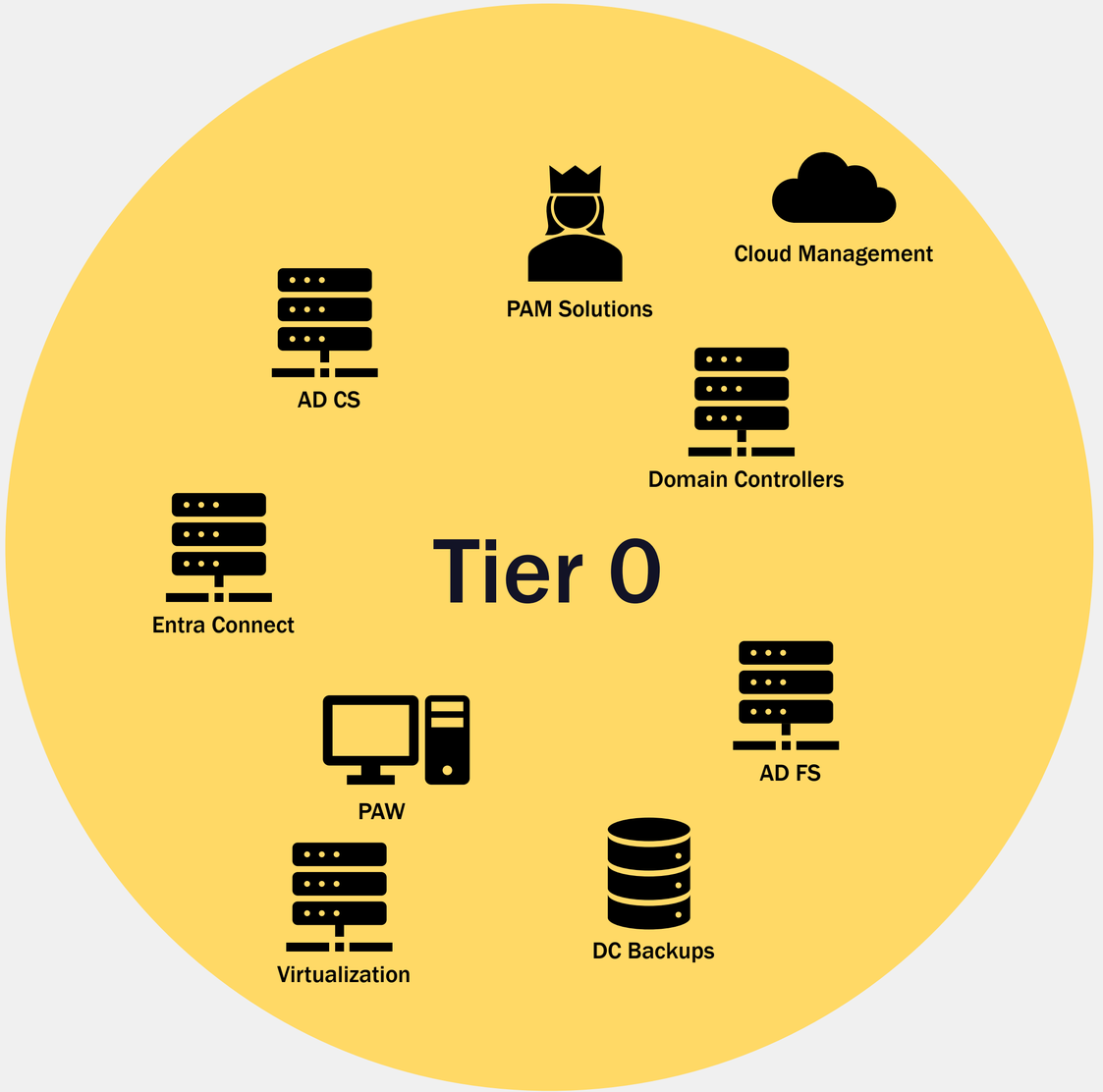
7

Secure Tier 0 dependencies

semperis

Improving Active Directory Security

7



semperis

Improving Active Directory Security

8

Harden domain controllers

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

semperis

Improving Active Directory Security

9

Monitor for unusual activity

semperis

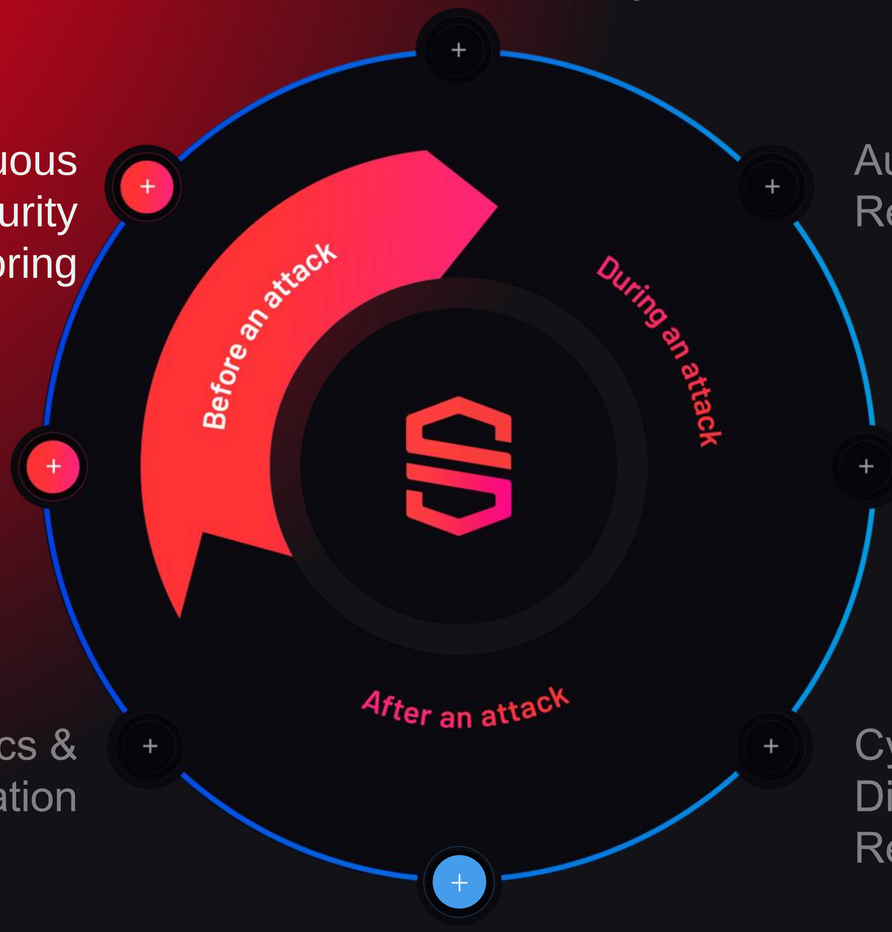
Improving Active Directory Security

10

Backup Active Directory... and ensure you can recover

semperis

PRE attack



Threat Detection & Visibility

Auto-Remediation

Incident Response Orchestration

Cyber-First Discovery Recovery

24/7 Global IR Support

Forensics & Investigation

IOE & IOC Discovery

Continuous Security Monitoring

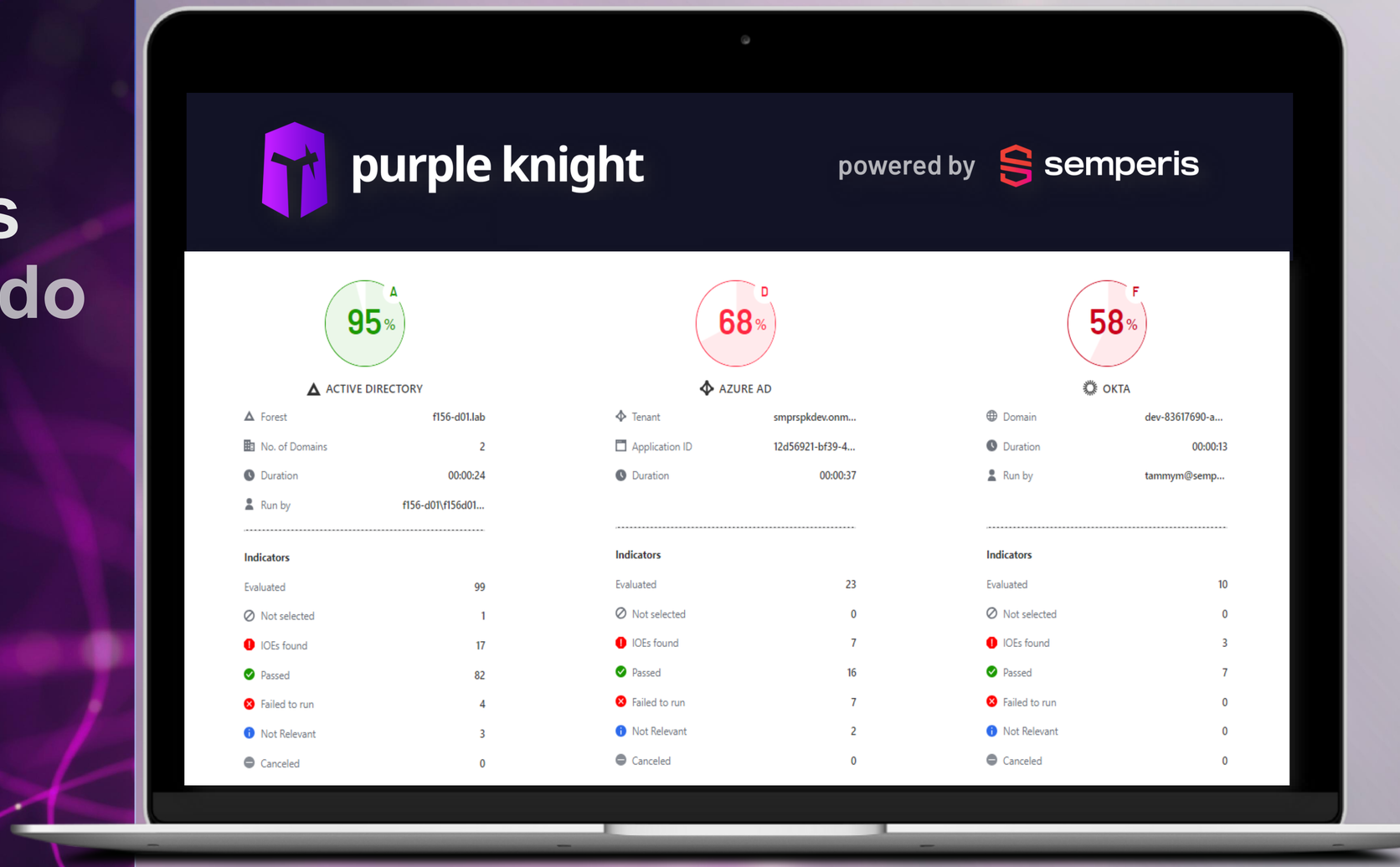
semperis

MEET PURPLE KNIGHT

Spot weaknesses before attackers do

Get the #1 community hybrid AD security assessment tool

- **20,000+** downloads
- **150+** security indicators
- **45%** attack surface reduction

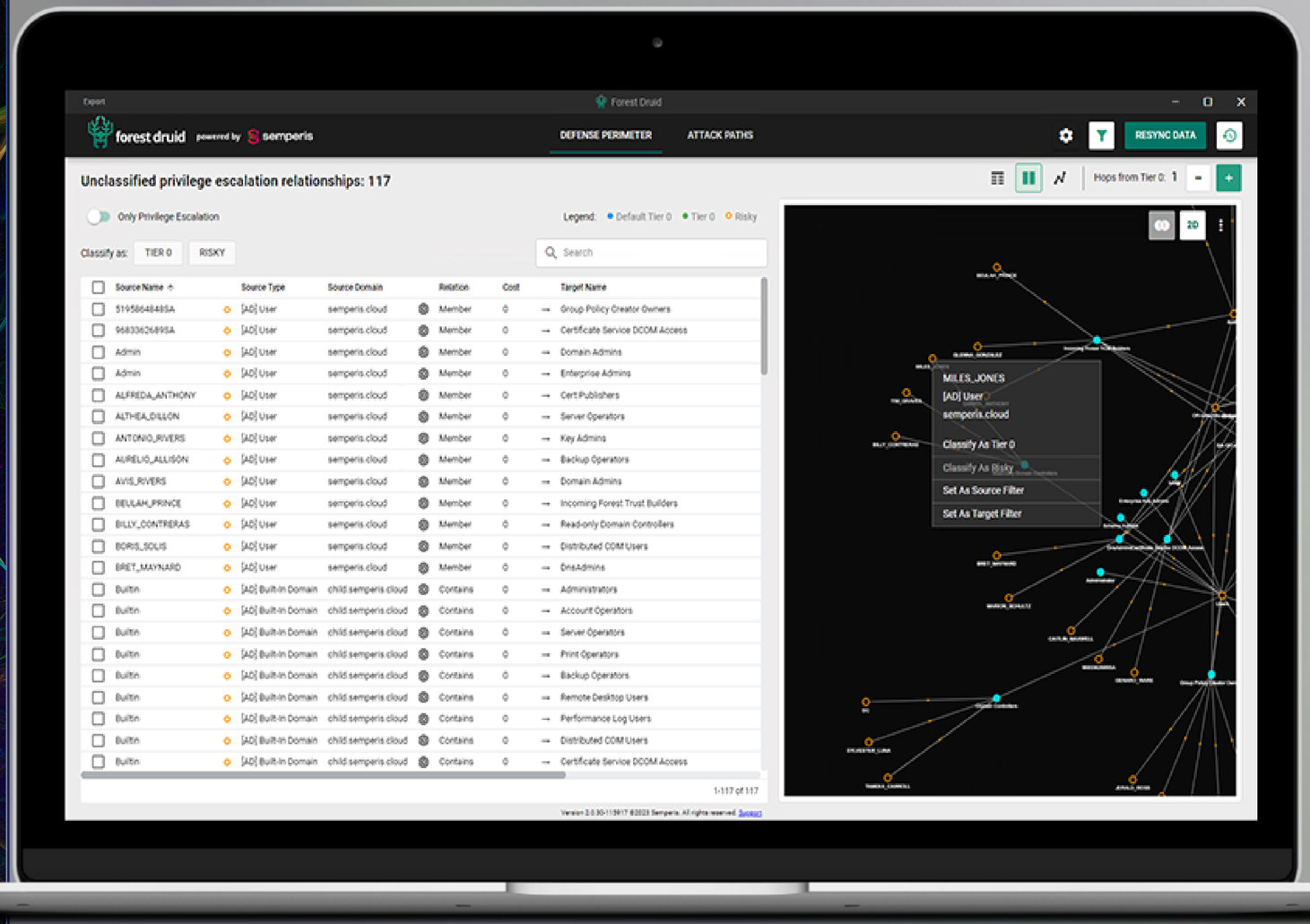


semperis

MEET FOREST DRUID

Close the paths attackers use to target Tier 0 assets

- Uncover vulnerable Tier 0 assets before it's too late
- Lock down excessive privileges, which create 99% of attack paths into Tier 0 assets
- Discover the most dangerous attack paths—not just the most common ones

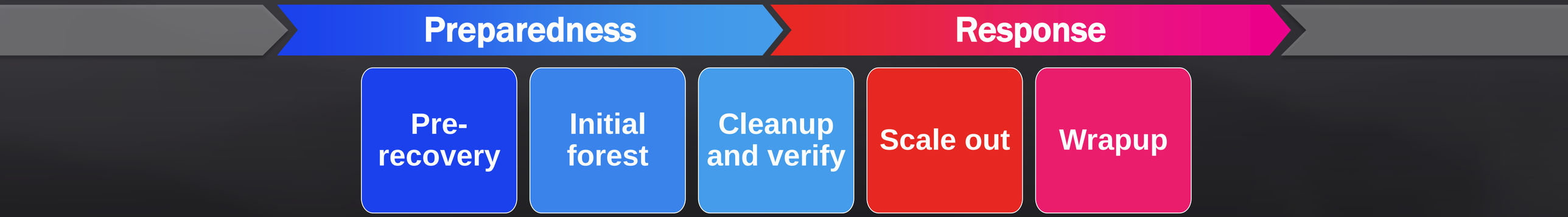


semperis

Implementing an AD ITDR solution

semperis

DEVELOP A STEP-BY-STEP RECOVERY PLAN



DO

semperis

POST attack

semperis

Active Directory DR Backup and Recovery

1

Backup every domain, including the root

semperis

Active Directory DR Backup and Recovery

2

Backup two or more DCs per domain

semperis

Active Directory DR Backup and Recovery

3

Test your backups regularly

semperis

Active Directory DR Backup and Recovery

4

Use supported backup methods

semperis

Active Directory DR Backup and Recovery

5

Ensure backups are malware free

semperis

Active Directory DR Backup and Recovery

6

Keep offline or air gapped copies

semperis

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

https://aka.ms/ADRecovery

semperis

Cyberattack recovery timeline

Dwell time

?? days

Encryption event

To identify

5 hours

Invoke incident response plan

12 hours

Cyber insurer engagement

24+ hours

Forensic analysis

2-3 days

Rebuild of primary IT functionality

5-14 days

Data recovery

7+ days

Reestablish production environment

Weeks-months

21-day average

AD FOREST RECOVERY

Shorten forest recovery by 90%

- Clean restore (malware free)
- Rapid recovery
- Advanced automation
- Anywhere recovery
- Post-attack forensics (AD anti-virus)

semperis

Key takeaways

1. AD is the foundation of Zero Trust.

2. An attacked AD can lead to an attacked Azure AD and vice versa.

3. Attackers are become adept at evading endpoint security and security logs.

4. Continuously scanning both AD and Azure AD for vulnerabilities—and fixing them, where possible—is a key requirement to reduce the attack surface.

5. Be prepared for the worst: Ensure that you can recover your AD forest safely and quickly. Your disaster recovery plan depends on it!

   ➢Check out Semperis **Purple Knight** and **Forest Druid** to get started.

semperis

THANK YOU

Questions?

KKR

INSIGHT PARTNERS

Microsoft Partner

Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-Sell
Microsoft Intelligence Security Association (MISA)

TOP 5 FASTEST-GROWING CYBERSECURITY COMPANIES

3 YEARS IN A ROW OF DOUBLE-DIGIT GROWTH

NAMED TO FORTUNE'S CYBER 60 2024 LIST

2 CONSECUTIVE YEARS ON THE LIST

#14 ON DUN'S 100 2022 RANKING OF BEST STARTUPS

150+ COMBINED YEARS OF MICROSOFT MVP EXPERIENCE

EY HONORS SEMPERIS CEO MICKEY BRESMAN

TOP 10 OF US 100 FASTEST-GROWING VETERAN-OWNED BUSINESSES