semperis

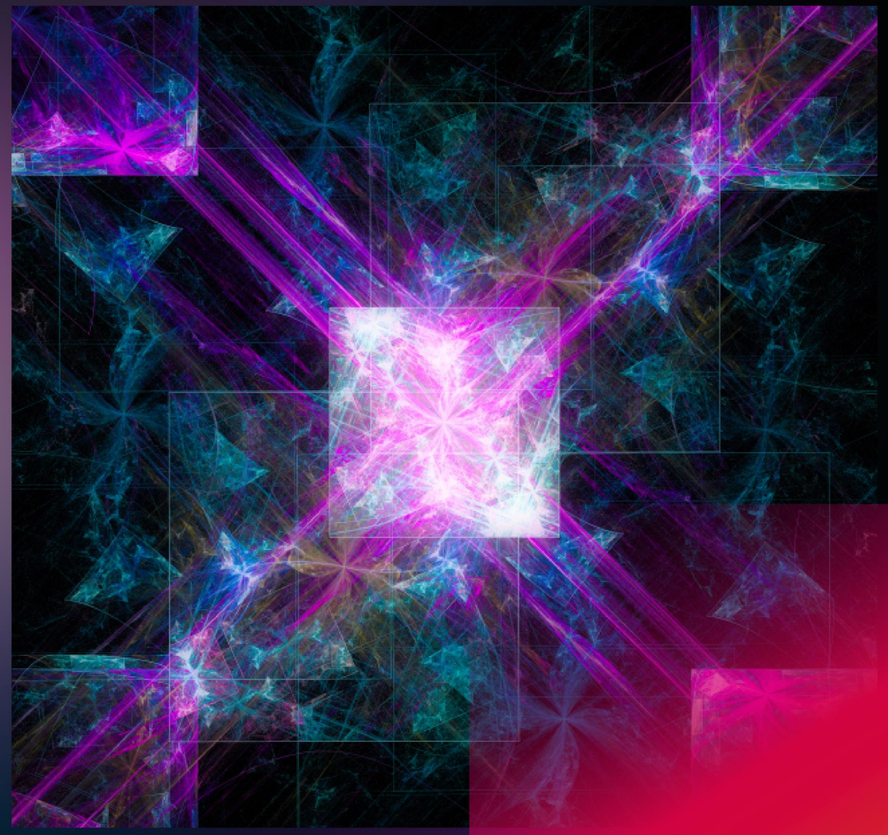
Mitigating Risk to the #1 Target for Attackers:

Your Enterprise Identity System

Guido Grillenmeier

PRINCIPAL TECHNOLOGIST, SEMPERIS

GUIDOG@SEMPERIS.COM



semperis

Identity is Fundamental to Modern Security

semperis

IDENTITY IS FUNDAMENTAL TO ZERO TRUST

Enhanced identity governance (EIG) is seen as the foundational component of zero trust architecture.

- “Implementing a Zero Trust Architecture”

NIST

Identity is central to providing appropriate, accurate and secure access to data, services and systems.

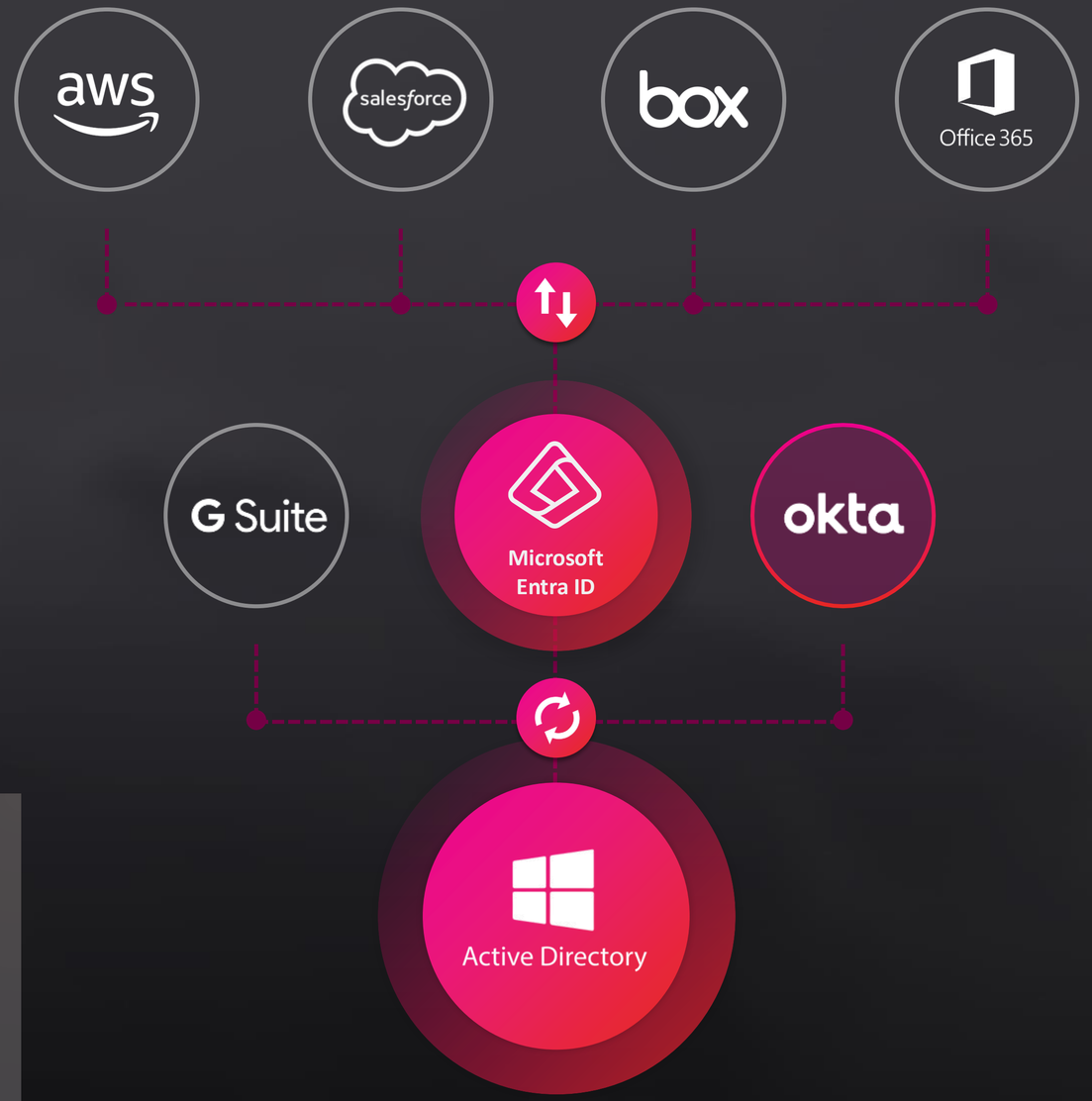
Gartner®

semperis

KEYS TO THE KINGDOM

If Active Directory isn't secure, nothing is

- AD is the **de facto identity system** in almost all medium and large organizations
- **Hybrid Identity**: AD integrated with cloud identity services
- **Zero trust model** assumes hybrid AD integrity



For 90% of enterprises, security starts with AD

semperis

2024 New Zealand Cyber Security Guidance: Protect Active Directory

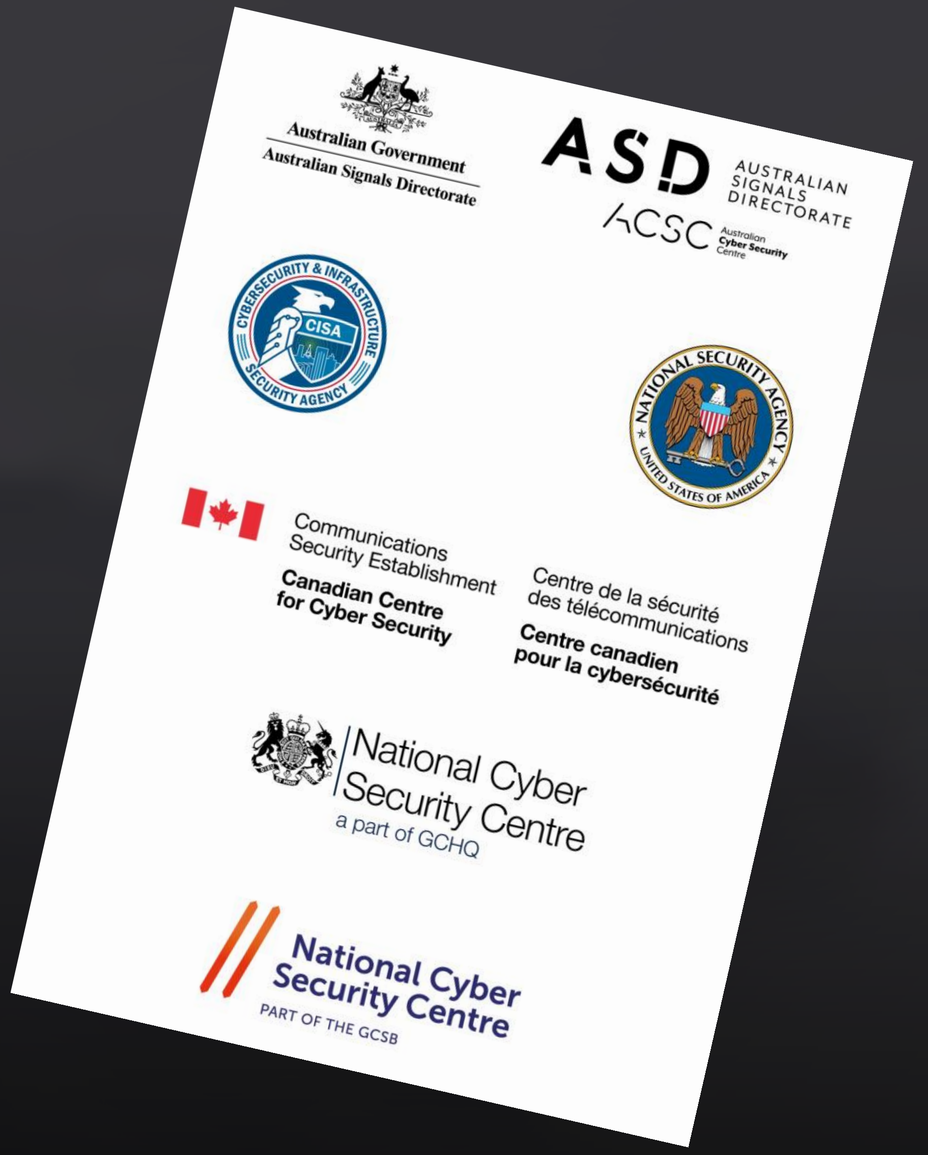
Source: Sept. 2024 Guidance “Detecting and Mitigating Active Directory Compromises”

“**Joint Guidance: Detecting and mitigating Active Directory compromises**

… organisations are encouraged to implement the recommendations within this guidance to better protect Active Directory from malicious actors and prevent them from compromising it.”

New Zealand National Cyber Security Centre (NCSC-NZ)

semperis



https://www.cyber.gov.au/sites/default/files/2024-09/PROTECT-Detecting-and-Mitigating-Active-Directory-Compromises.pdf

semperis

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Understanding Active Directory

For many organisations, Active Directory consists of thousands of objects interacting with each other via a complex set of permissions, configurations and relationships. Understanding object permissions and the relationships between those objects is critical to securing an Active Directory environment.

To gain a better understanding of an organisation's environment, malicious actors commonly enumerate Active Directory for information after gaining initial access to an environment with Active Directory. Using the information gained, they seek to understand the structure, objects, configurations and relationships that are unique to each organisation. By doing this, malicious actors sometimes gain a better understanding of the organisation's Active Directory environment than the organisation itself. This enables them to target Active Directory with increased likelihood of success. Malicious actors use their knowledge of the environment to exploit weakness and misconfigurations to escalate their privileges, move laterally, and gain full control of the Active Directory domain.

To improve Active Directory, organisations must comprehensively understand their own unique configuration of Active Directory. There are numerous commercial and open source tools available to support an organisation's understanding of Active Directory, including the following:

- BloodHound: A tool that provides a graphical user interface to help with understanding Active Directory, as well identifying any misconfigurations and weaknesses that malicious actors may seek to exploit.
- Netwrix PingCastle: A tool that provides an Active Directory security report.
- Purple Knight: An application that provides information on the security of an Active Directory environment.

https://www.cyber.gov.au/sites/default/files/2024-09/PROTECT-Detecting-and-Mitigating-Active-Directory-Compromises.pdf

semperis

Most Cyberattacks Involve Active Directory Compromise

semperis

#1 TARGET

*When Microsoft Incident Response is engaged during an incident…**in most engagements, threat actors have taken full control of Active Directory** –i.e., total domain compromise.*

Microsoft

***90% of attacks investigated involve AD in some form**, whether it is the initial attack vector or targeted to achieve persistence or privileges.*

MANDIANT

semperis

2024 New Zealand Cyber Security Guidance: Protect Active Directory

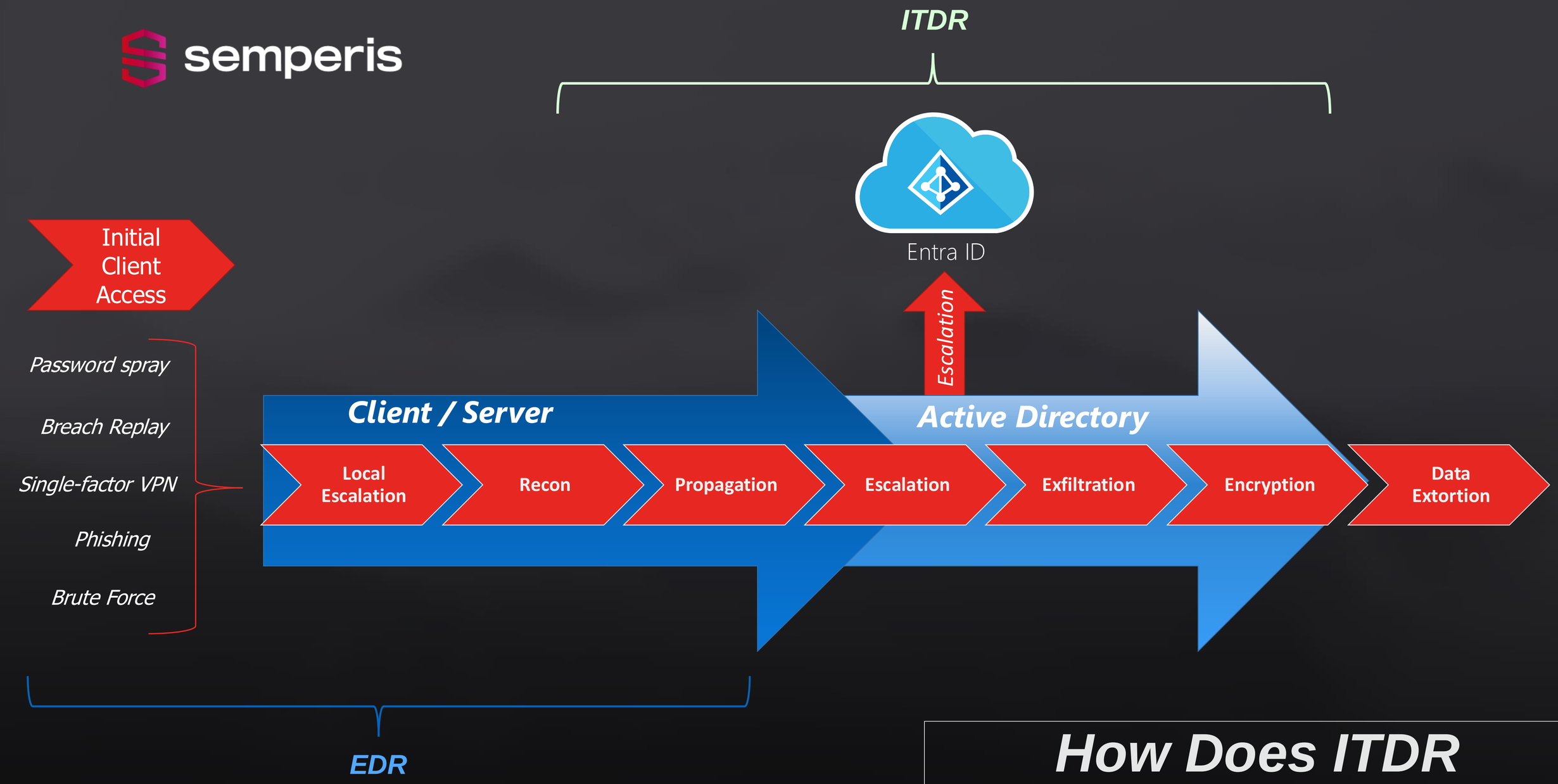
Source: Sept. 2024 Guidance “Detecting and Mitigating Active Directory Compromises”

“Specifically, Active Directory’s susceptibility to compromise is, in part, because every user in Active Directory has sufficient permission to enable them to both identify and exploit weaknesses.

These permissions make Active Directory’s attack surface exceptionally large and difficult to defend against.”

New Zealand National Cyber Security Centre (NCSC-NZ)

semperis



How Does ITDR Compare to EDR?

- May 2021
- **Initial access: phishing email ”someone opened an email attachment they shouldn't have”**
- *“…crippled the Waikato DHB’s IT systems, including hospital computer systems and phone lines. This disruption affected patient care, with some surgeries postponed and critical services impacted.”*
- The attack prompted a nationwide review of cybersecurity measures across New Zealand’s health sector

- June 2023
- **Warning about increased Criminal Activity**
- The National Cyber Security Centre (NCSC) noted a sharp increase in criminal cyber activity, with financially motivated attacks becoming more prevalent.
- *“Domestically, and internationally, we see heightened determination from cyber criminal actors attempting to extort payment from organisations.”*
- This included ransomware and other forms of extortion

semperis

MITIGATING IDENTITY RISK

Defending Hybrid Identity with Identity Threat Detection & Response

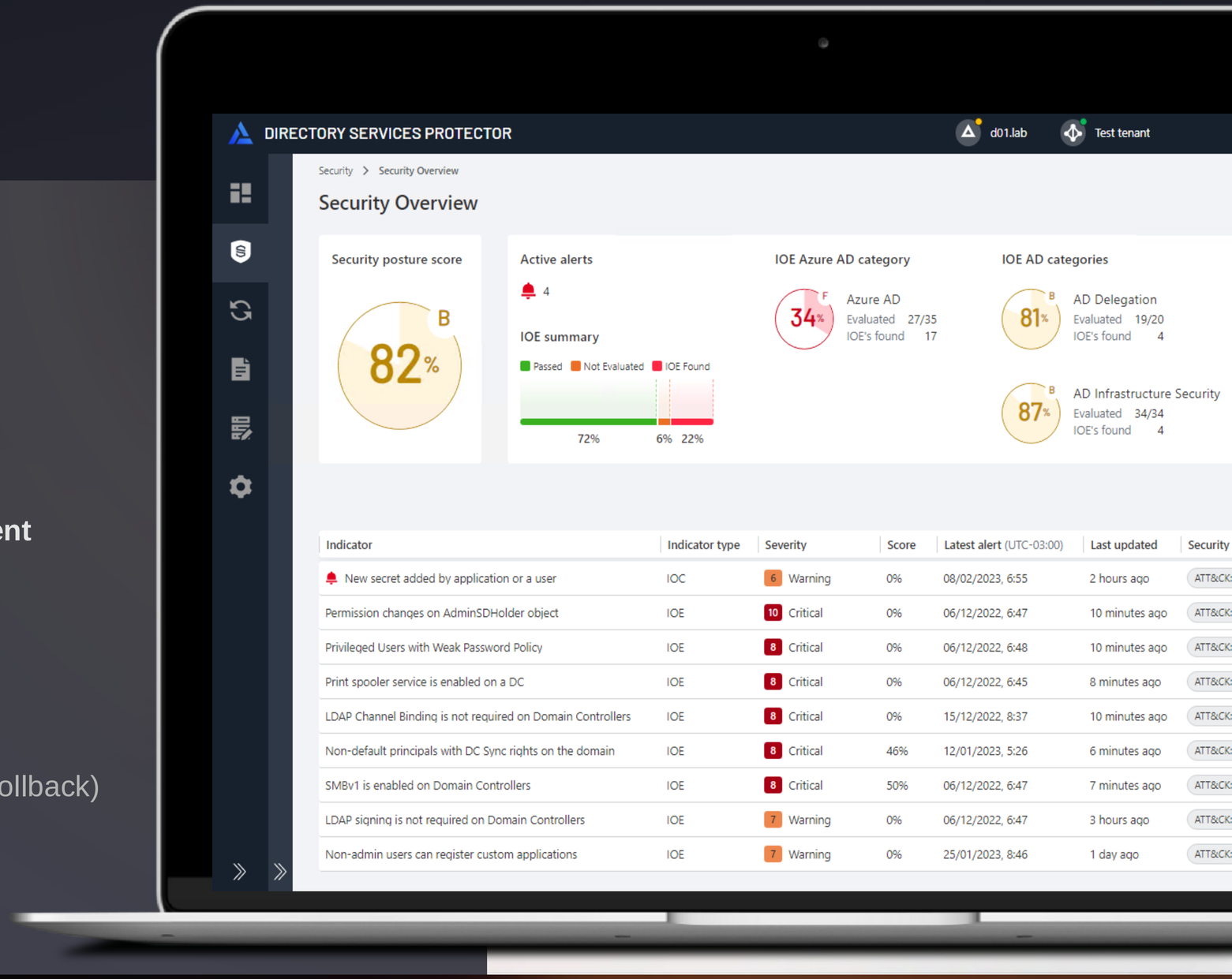
semperis

PRE attack

DIRECTORY SERVICES PROTECTOR

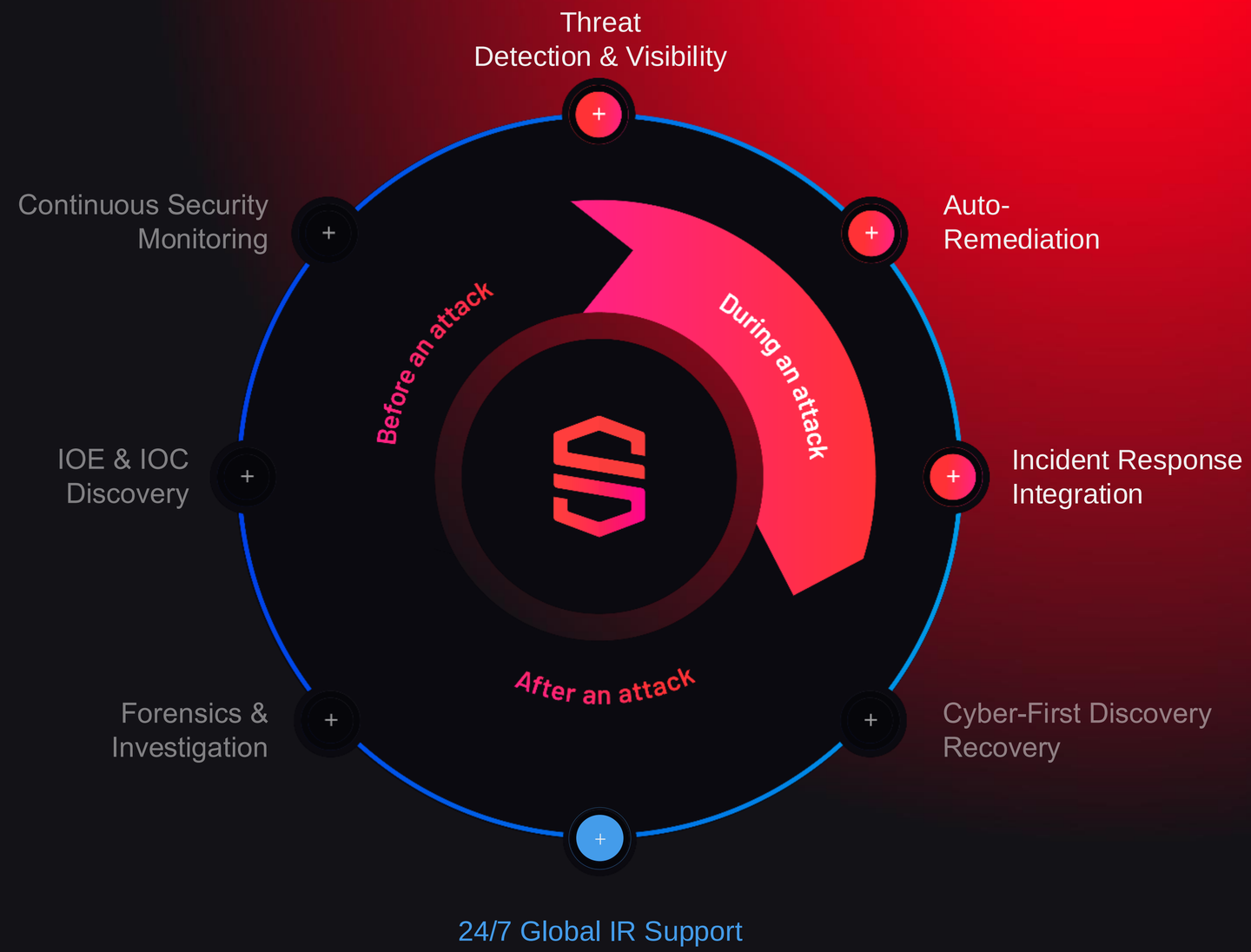
Prevent, detect, & respond

- **Continuous vulnerability assessment**
- Tamperproof tracking
- Real-time security alerts
- Auto-remediation (malicious change rollback)
- Compliance reporting



semperis

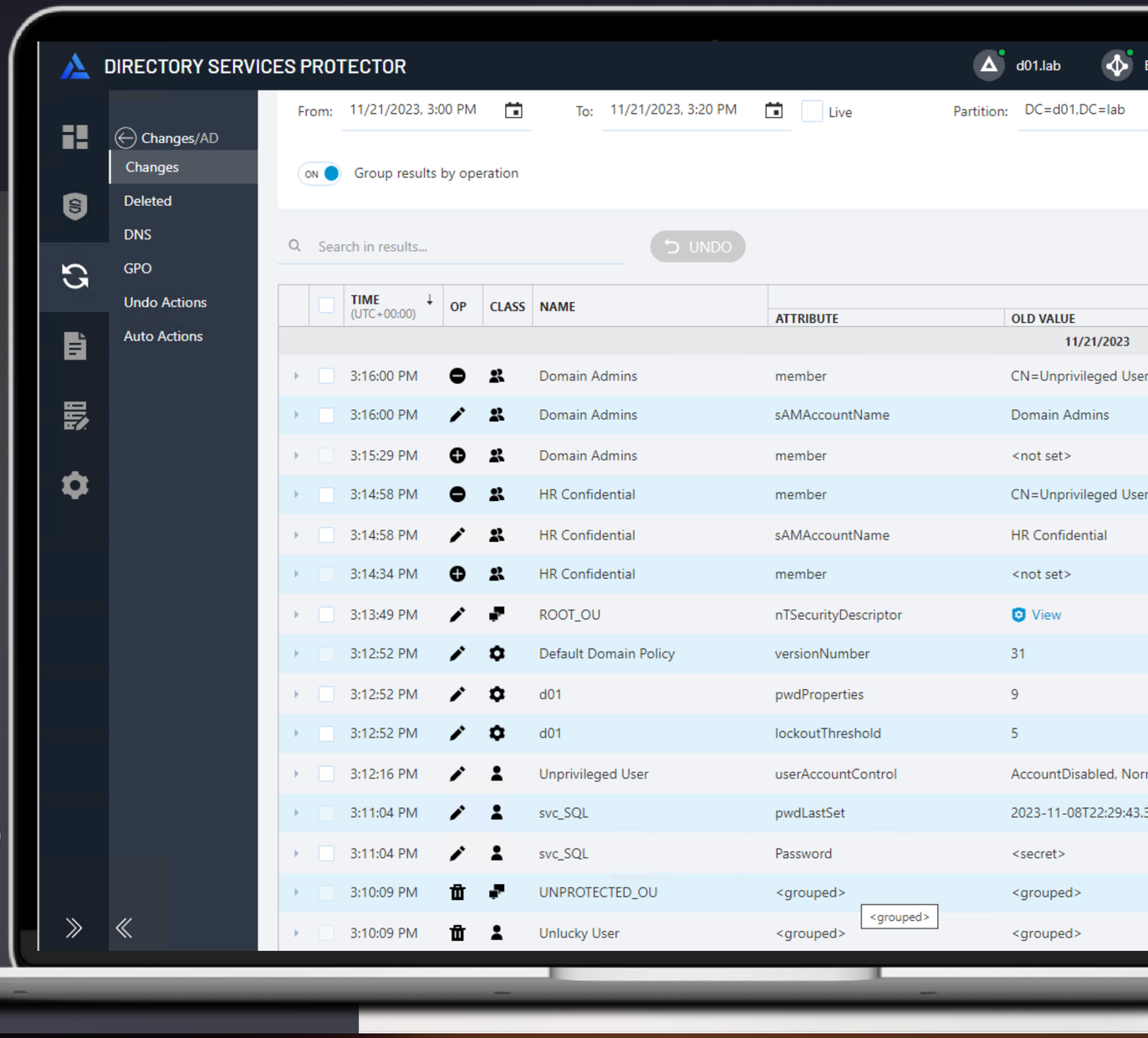
DURING attack



DIRECTORY SERVICES PROTECTOR

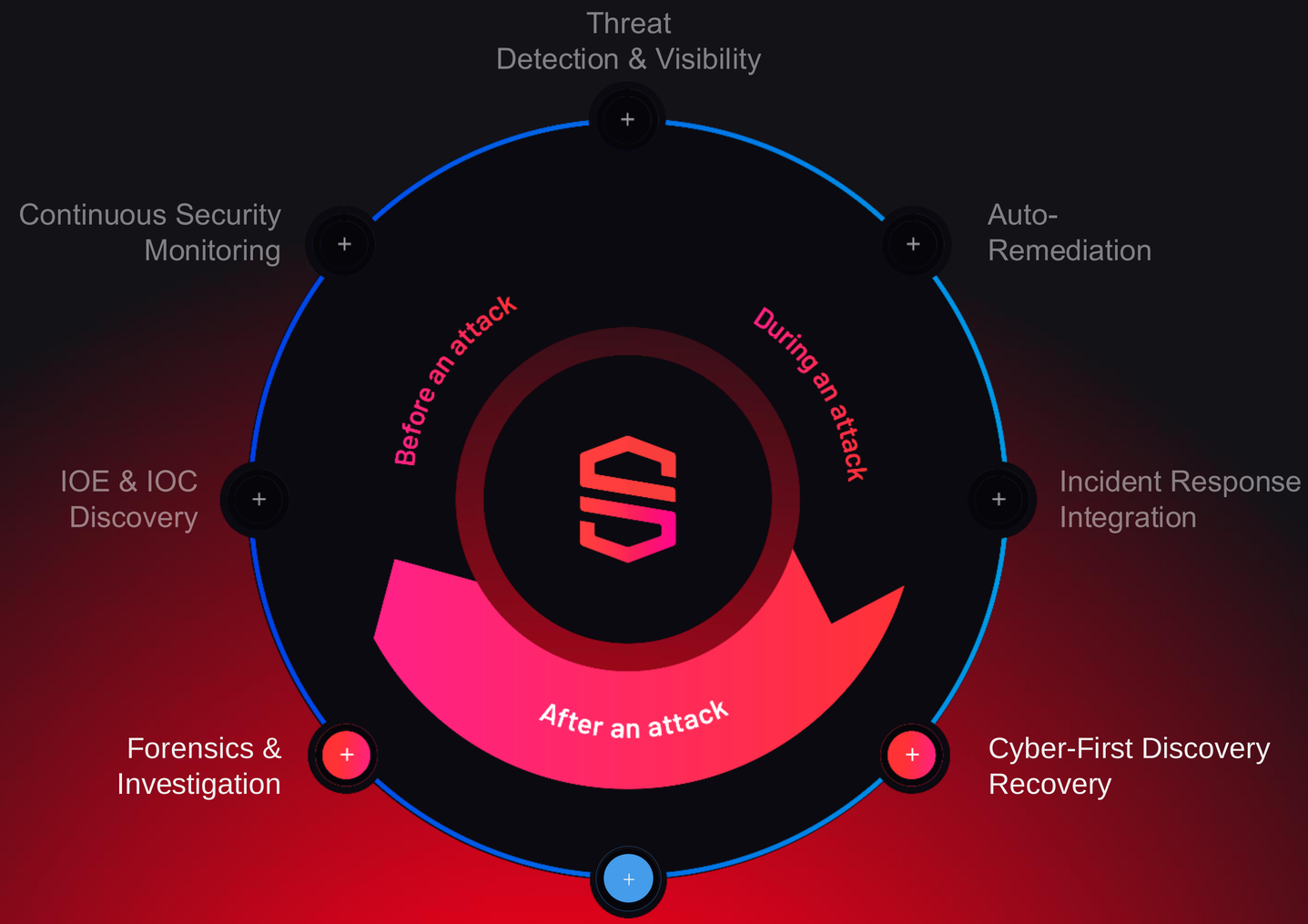
Prevent, detect, & respond

- Continuous vulnerability assessment
- **Tamperproof tracking**
- **Real-time security alerts**
- **Auto-remediation (malicious change rollback)**
- **Compliance reporting**



semperis

POST attack



semperis

1. Pull the network cables from all DCs or otherwise disable network

2. Connect DCs to be restored to a private network (*Oh yes - establish a global private VLAN*)

For each domain:
3. Nonauthoritative restore of first writeable DC
4. Auth restore of SYSVOL on that DC
5. Remediate malware
6. Reset all admin account passwords
7. Seize FSMOs
8. Metadata cleanup of all writeable DCs except for targeted seed forest DCs
9. Configure DNS on the forest root DC
10. Remove the global catalog from each DC.
(Wait for global catalog to be removed)

11. Delete DNS NS records of DCs that no longer exist

12. Delete DNS SRV records of DCs that no longer exist

13. Raise the value of available RID pools by 100K

14. Invalidate the current RID pool for every DC

15. Reset the computer account of the root DC twice

16. Reset krbtgt account twice
(You have a seed forest at this point)

17. Configure Windows Time

18. Verify replication between seed DCs health

19. Add GC to a DC for each OS version in each domain
(Wait for GCs to be created)

20. Take a backup of all DCs in the seed forest

21. Create an IFM package for each OS version, in each domain your DCs are running

22. Build out seed forest with additional DCs to support Tier 0 / Tier 1 operations

For each DC to be repromoted into the seed forest:
23. Clean up the (former) DC using /FORCEREMOVAL or rebuild OS
24. Send IFM package to server (wait…)
25. Take the DC off the public network and put it on the seed forest network.
26. Run a DCPROMO IFM
(Days pass while you clean and rebuild DCs)
(Now you have a large enough forest to support basic operations)

27. Verify health of the full forest

28. Move restored forest to the corporate network

29. Reboot all servers and clients to force communications with the new forest

Important considerations

Manual recovery is error-prone and often requires additional cycles to correct missteps, extending the timeline even further.

Required staff for manual AD forest recovery:
Core AD team, operators at every datacenter, plus other external support (Estimated 10-15 IT support staffers in average enterprise)

General purpose backup only automates step 3, leaving the rest of the recovery process a mostly manual effort.

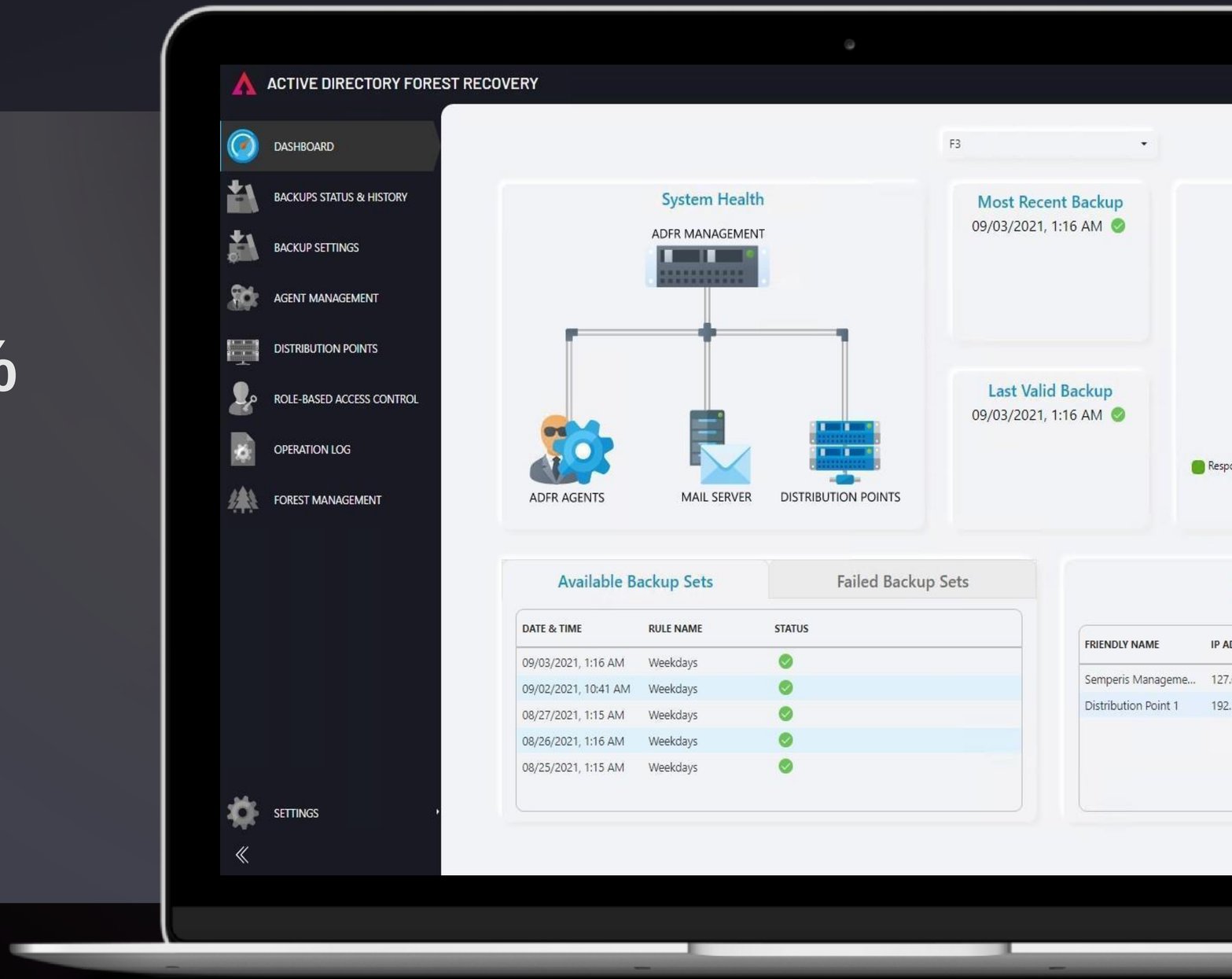
How long does it take to manually perform an Active Directory forest recovery?

Days to weeks...

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

PROTECTING IDENTITY

Next Steps

- **Review your ability to protect and remediate Active Directory**
  - Can you protect the AD *service* itself (not just the AD domain controller *servers*)?
  - Can you warn of IoEs and IoCs?
  - Can you roll back unauthorized changes to AD?
  - Can you quickly regain trust in your foundational identity system?
- **Evaluate your worst-case Active Directory cyber disaster preparedness**
  - Can you “sandbox restore” AD while in crises to threat hunt?
  - Do you have a cyber DR plan for AD that will work - quickly and reliably – when you most need it?

semperis

Thank You

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

EY HONORS SEMPERIS CEO MICKEY BRESMAN

2 CONSECUTIVE YEARS ON THE LIST

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

150+ COMBINED YEARS OF MICROSOFT MVP EXPERIENCE