semperis

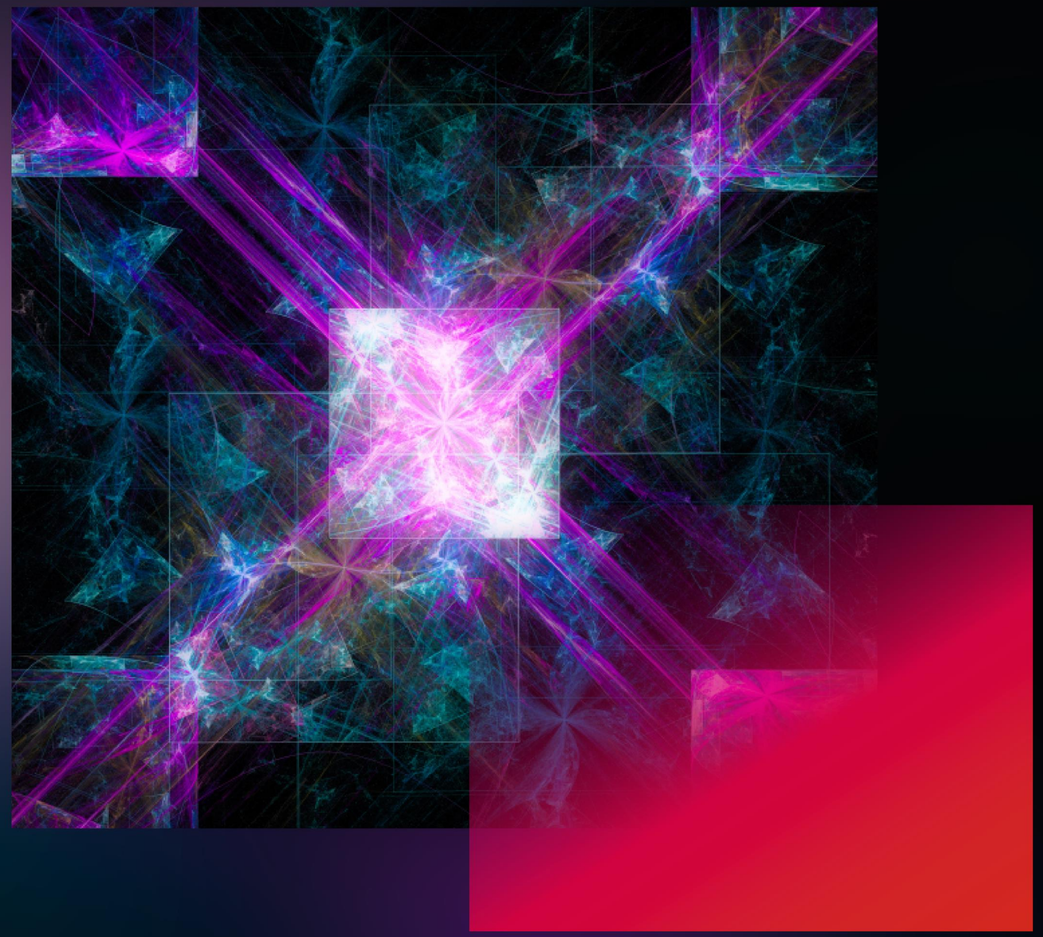
Mitigating Risk to the #1 Target for Attackers:

Your Enterprise Identity System

Sean Deuby

PRINCIPAL TECHNOLOGIST, SEMPERIS

SEAND@SEMPERIS.COM



Protect Identity.

1. Identity is **fundamental** to modern security

2. Most cyberattacks use **identity compromise**

3. Identity depends upon **Active Directory**
   …and it's *always* a target

4. Mitigating identity risk **requires specific identity threat detection & response (ITDR) solutions**

semperis

Identity is Fundamental to Modern Security

semperis

2023-2030 Australia Cyber Security Strategy: Zero Trust

“Develop a whole-of-government zero trust culture

to protect government data and digital estate. Government will implement defined controls across our networks that draw from internationally-recognised approaches to zero trust.”

Action 15,
“Uplift Cyber Security of the Commonwealth Government”

Source: 2023-2030 Australian Cyber Security Strategy Action Plan

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.

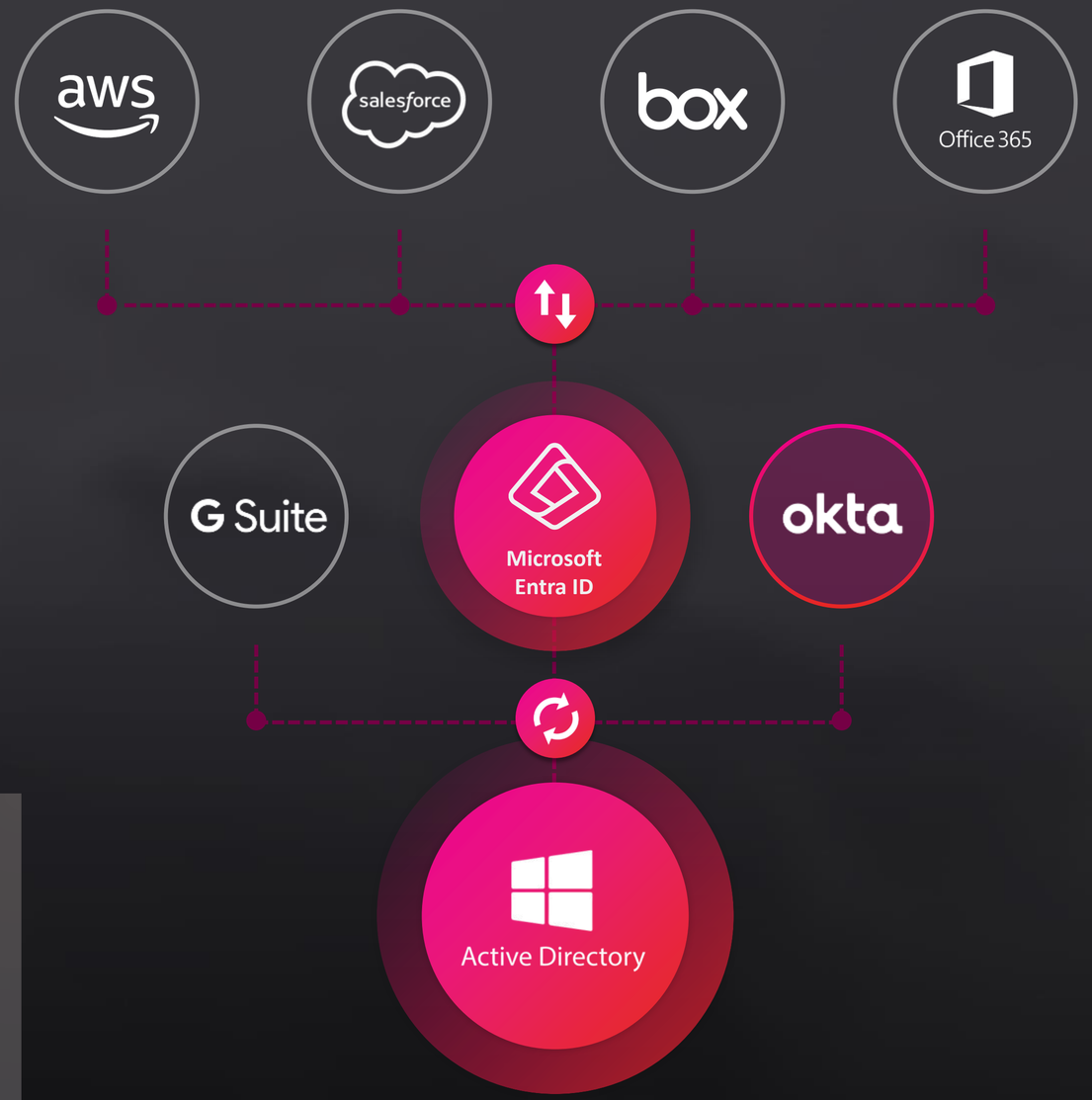
Gartner®

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

Most Cyberattacks Involve Active Directory Compromise

semperis

2023-2030 Australia Cyber Security Strategy: Critical Gaps

Source: 2023-2030 Australian Cyber Security Strategy Action Plan

"In Horizon 1, we will strengthen our foundations. **We will address critical gaps in our cyber shields**, build better protections for our most vulnerable citizens and businesses, and support initial cyber maturity uplift across our region."

Horizon 1 phase, "Strengthening Australia's Foundations", 2023-2025

semperis

#1 TARGET

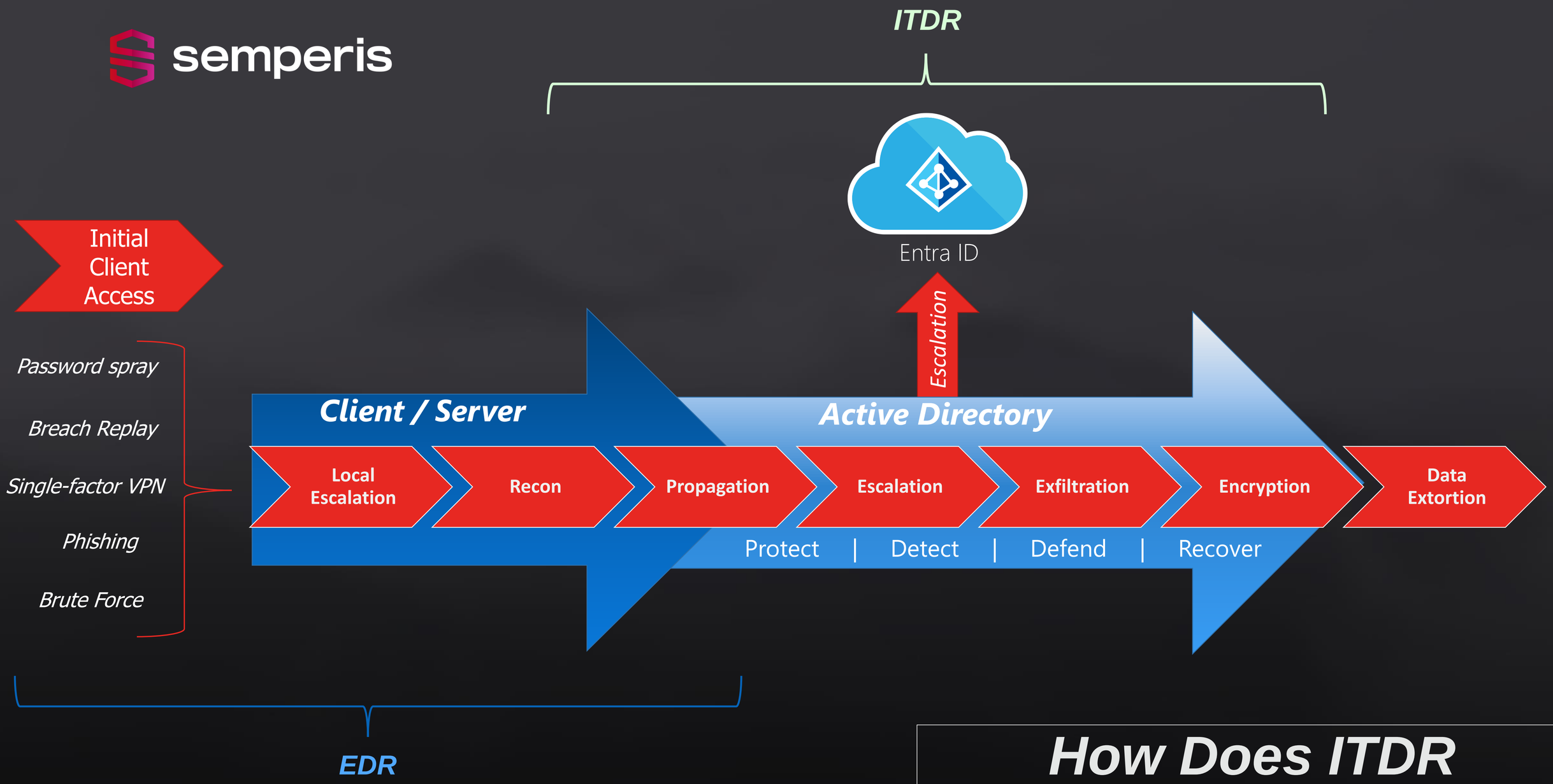
*When Microsoft Incident Response is engaged during an incident…**in most engagements, threat actors have taken full control of Active Directory** –i.e., total domain compromise.*

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

Microsoft

MANDIANT

semperis



How Does ITDR Compare to EDR?

St. Vincent Health
Where caring and community meet

- December 2023
- **Initial access: credential theft “of an individual with privileged access to internal systems”**
- Data theft and network disruptions
- “Critical infrastructure entities with the Risk Management Program requirements are required to have a Risk Management Program in place already, including covering cyber risks”

medibank

- October 2022
- **Initial access: credential theft**
- Accessed customer data & medical records - from athletes and media figures to the Prime Minister
- “The single most devastating cyber-attack we have experienced as a nation” - *Home Affairs Minister*
- Australia regulator tells Medibank to set aside $167 million after data breach (June 2023)

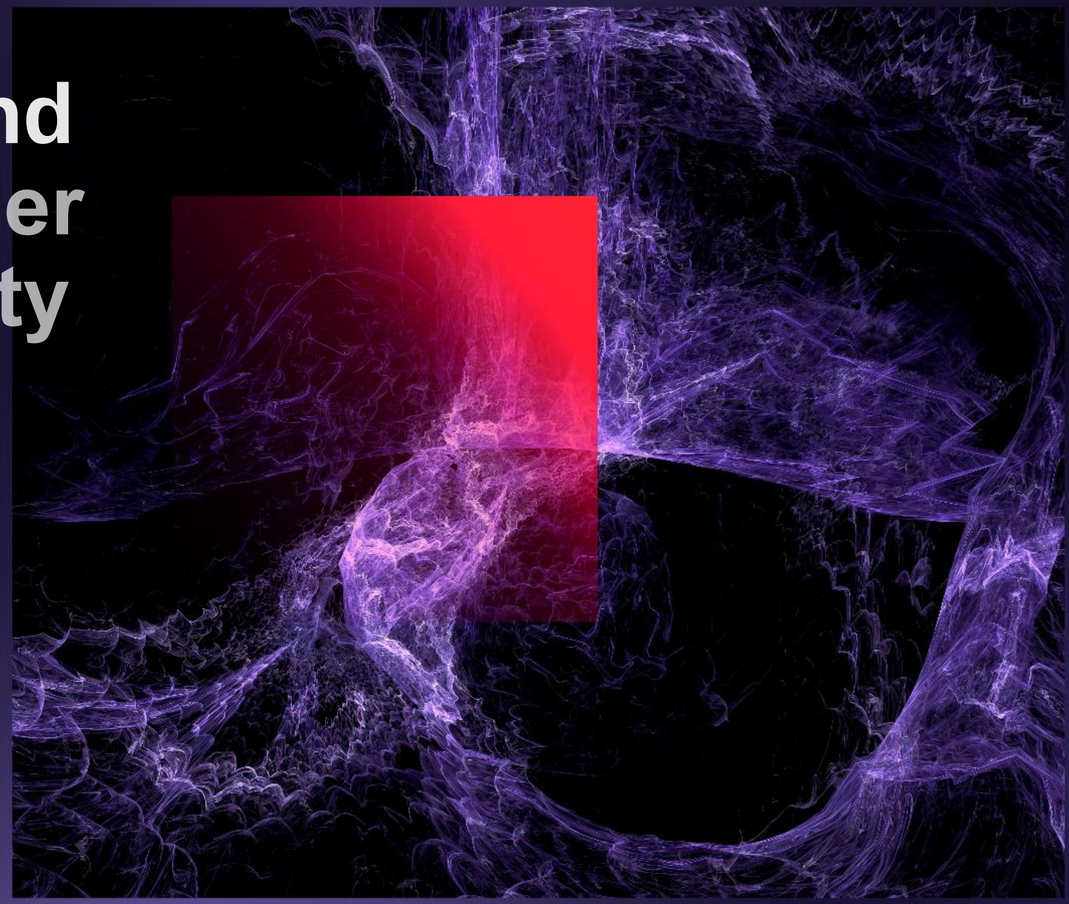
semperis

MITIGATING IDENTITY RISK

Defending Hybrid Identity with Identity Threat Detection & Response

semperis

Identity Threat Detection and Response (ITDR) is a Gartner “top trend” for cybersecurity



“ITDR is about correct and **secure operation of the identity infrastructure** rather than protection of individual users and resources managed by this infrastructure.”

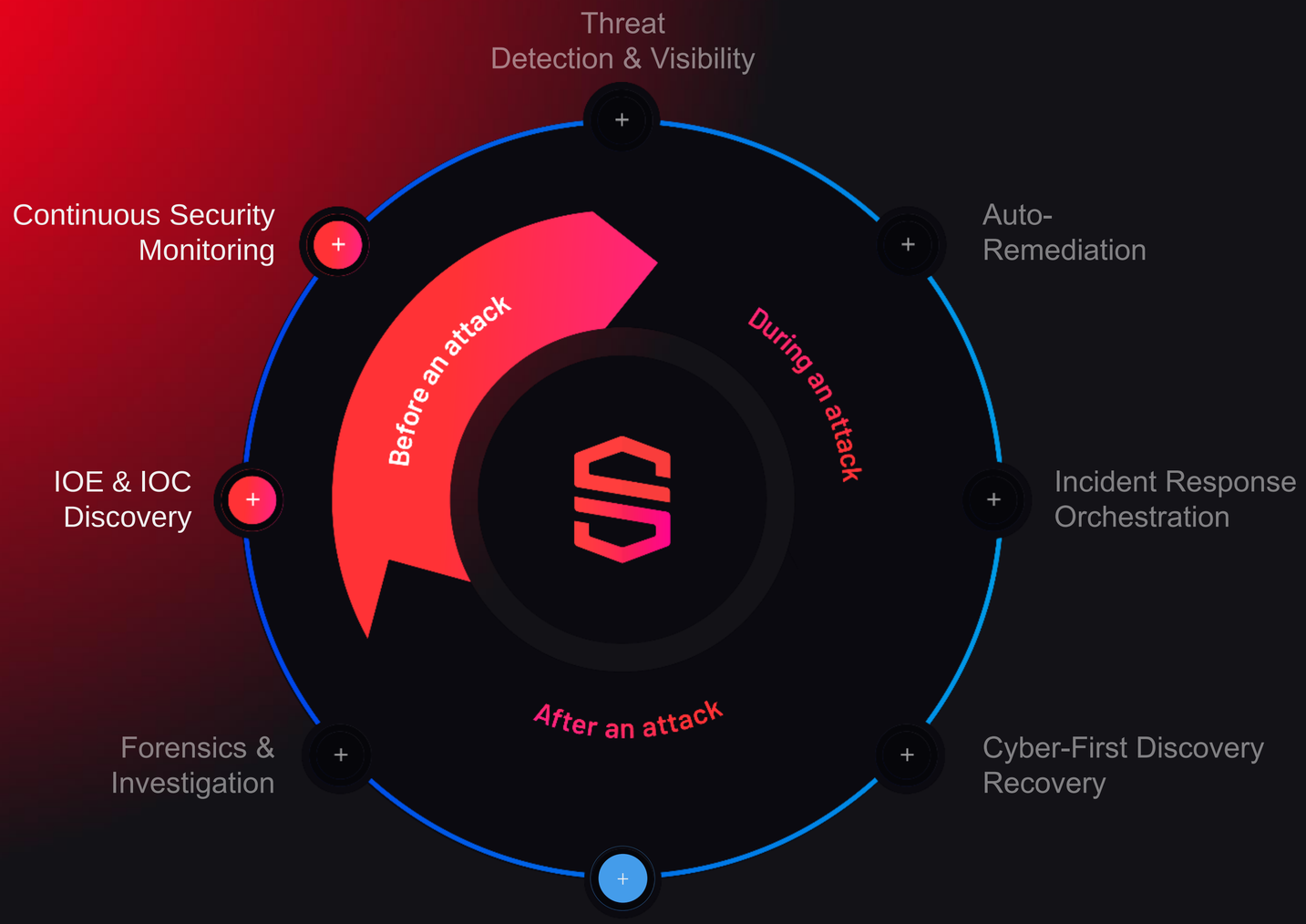
“AD TDR tools fulfill this mission by…**discovering indicators of exposure and indicators of compromise** in Active Directory. “

Gartner

Emerging Technologies and Trends Impact Radar: Security

semperis

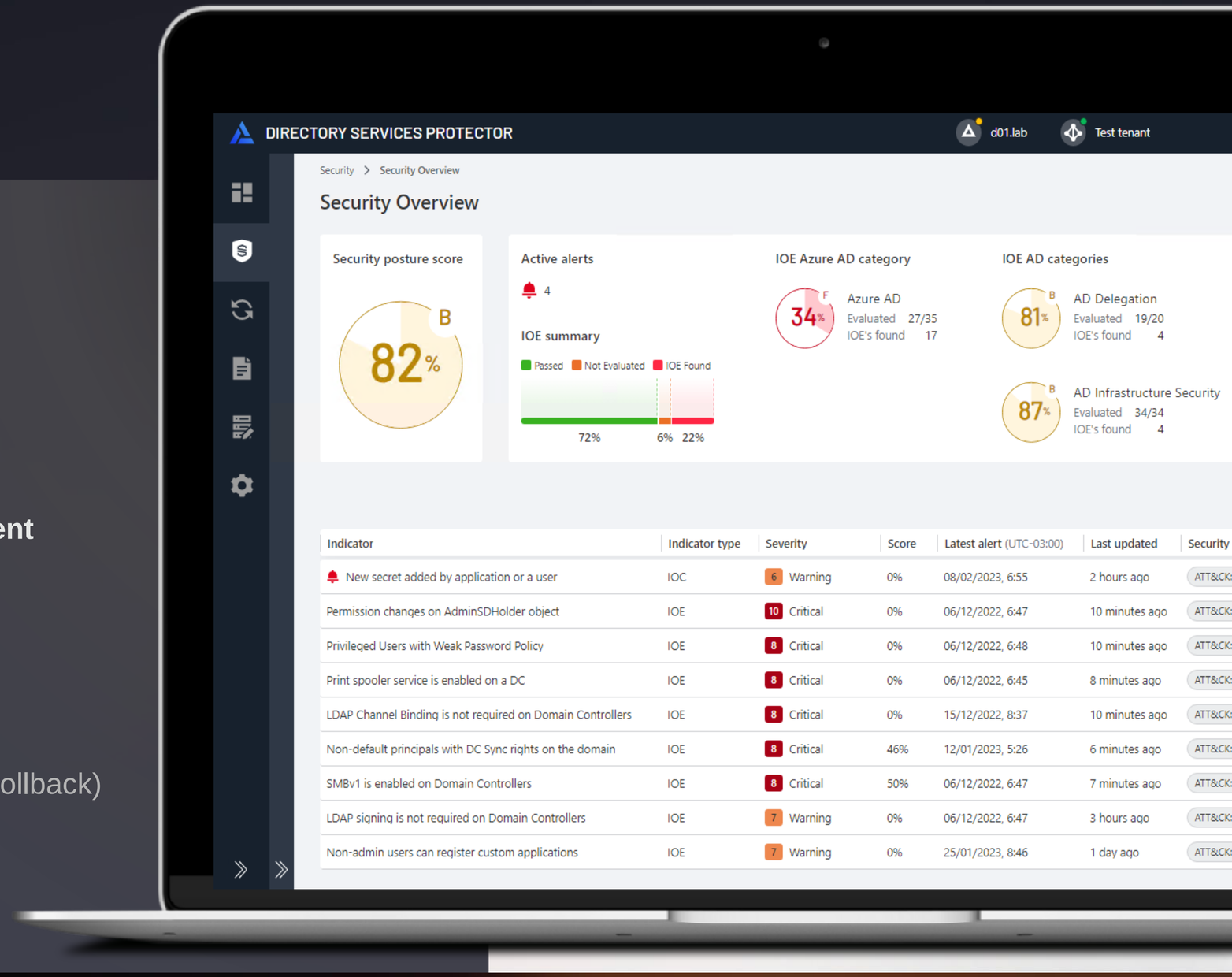
PRE attack



DIRECTORY SERVICES PROTECTOR

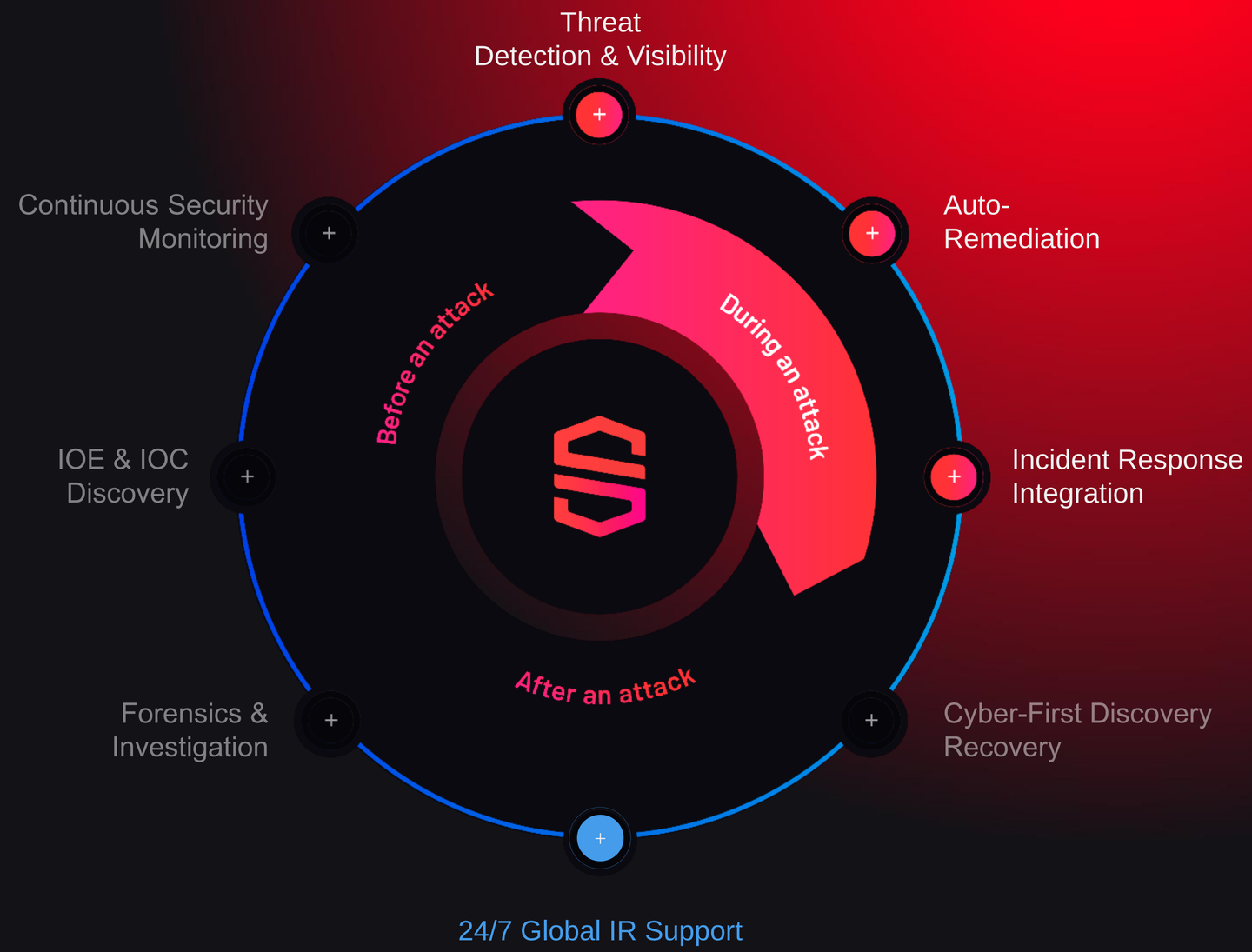
Prevent, detect, & respond

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



semperis

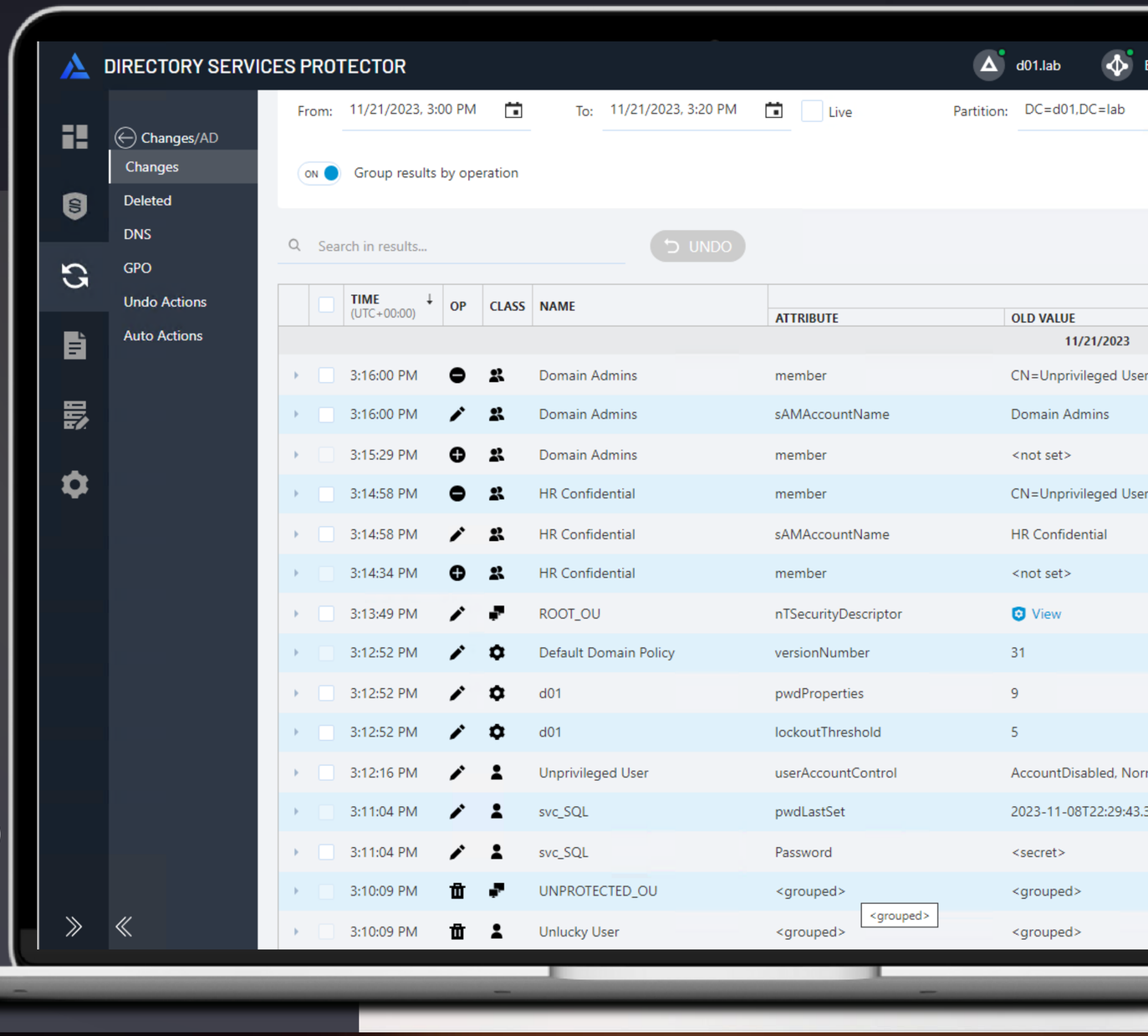
DURING attack



DIRECTORY SERVICES PROTECTOR

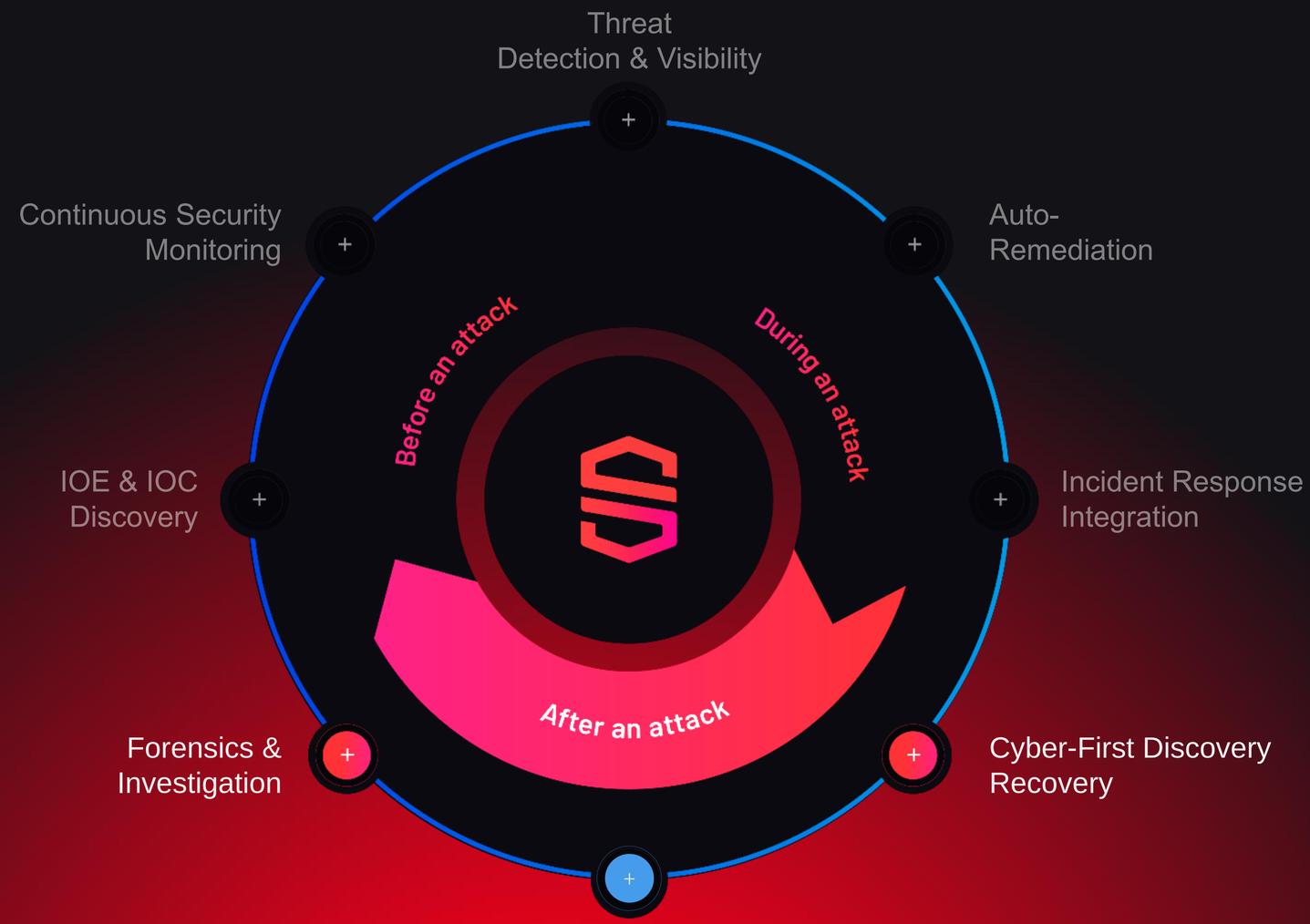
Prevent, detect, & respond

- 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.

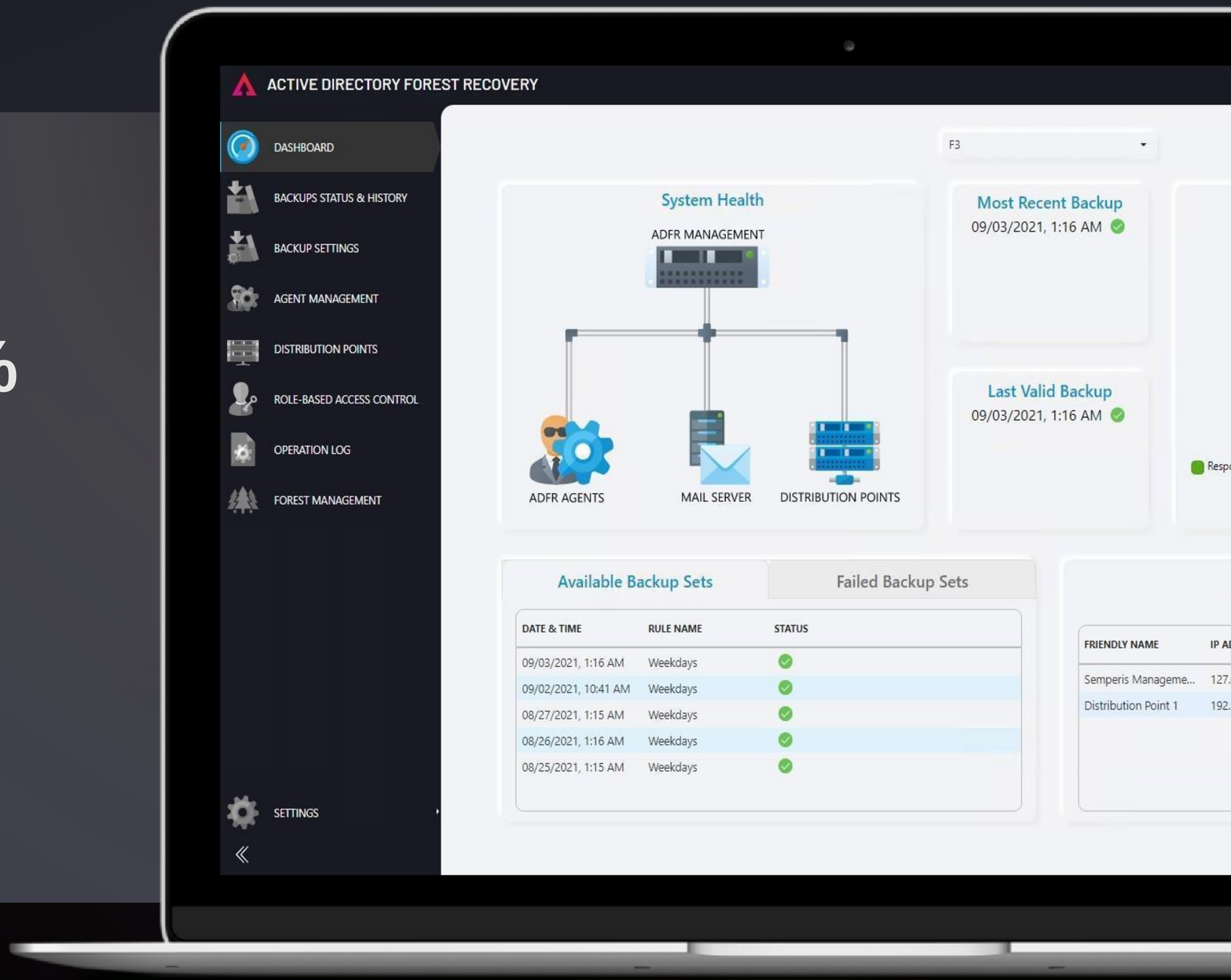
How long does it take to manually perform an Active Directory forest recovery?

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