semperis

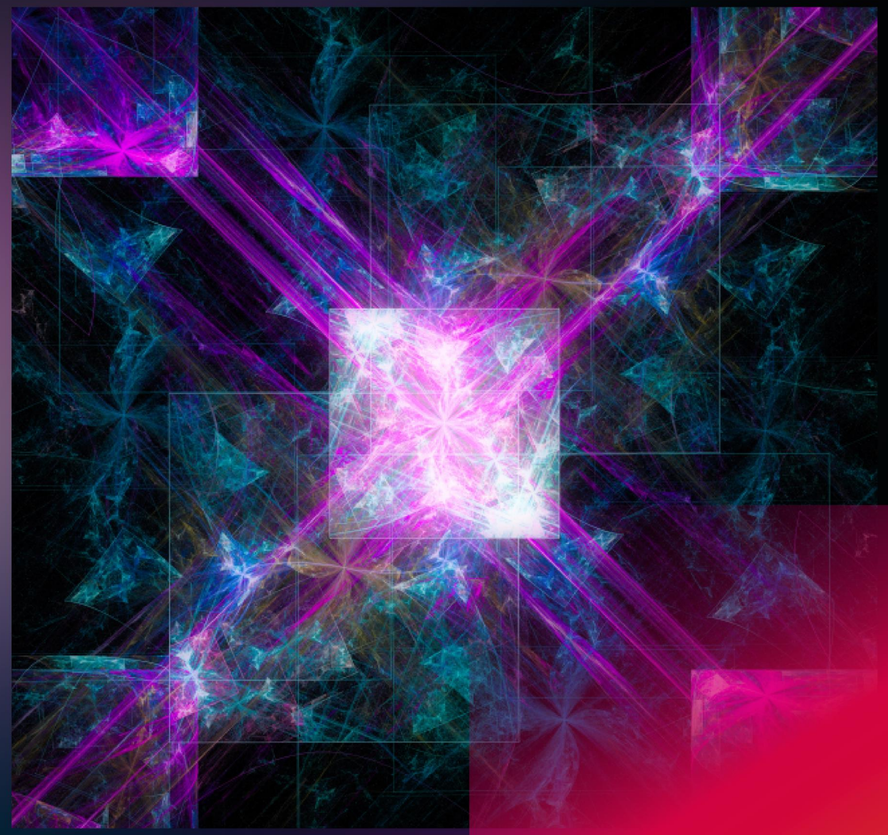
WELCOME

Semperis Overview

Calum Field

Channel Solution Architect

calumf@semperis.com



KKR

INSIGHT PARTNERS

Microsoft Partner

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

semperis

ABOUT SEMPERIS

Foundational identity security

Identity-driven cyber resilience and threat mitigation for hybrid and multi-cloud environments

Gartner peerinsights™

5.0 ★★★★★

The world's biggest brands trust Semperis

100+ million

Identities protected by Semperis (and counting)

- **#1** health system in the US, **top 5** in the world
- **2/3** top consulting firms in the world
- **2/3** top airlines in the world
- **#1** and **#5** big box retailer in the world
- **#1** bank in Europe. **#2** bank in the U.S.
- **Top 5** property insurer in the U.S. **#2** auto insurer

semperis

DOMAIN EXPERTISE

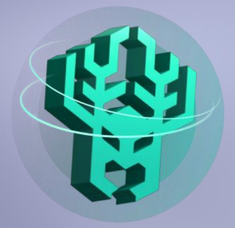
150+ years' Microsoft MVP experience

Microsoft Enterprise Cloud Alliance | Microsoft Accelerator Alumni
Azure Co-sell Partner | Microsoft Intelligent Security Association

No vendor or services provider can outmatch Semperis' collective Microsoft MVP experience in **Directory Services and Group Policy**

The team behind Purple Knight

Purple Knight is a free AD cybersecurity assessment tool built and managed by Semperis' threat research team



The team behind Forest Druid

Forest Druid is a first-of-its-kind Tier 0 attack path discovery tool for Active Directory environments

Hybrid Identity thought leaders

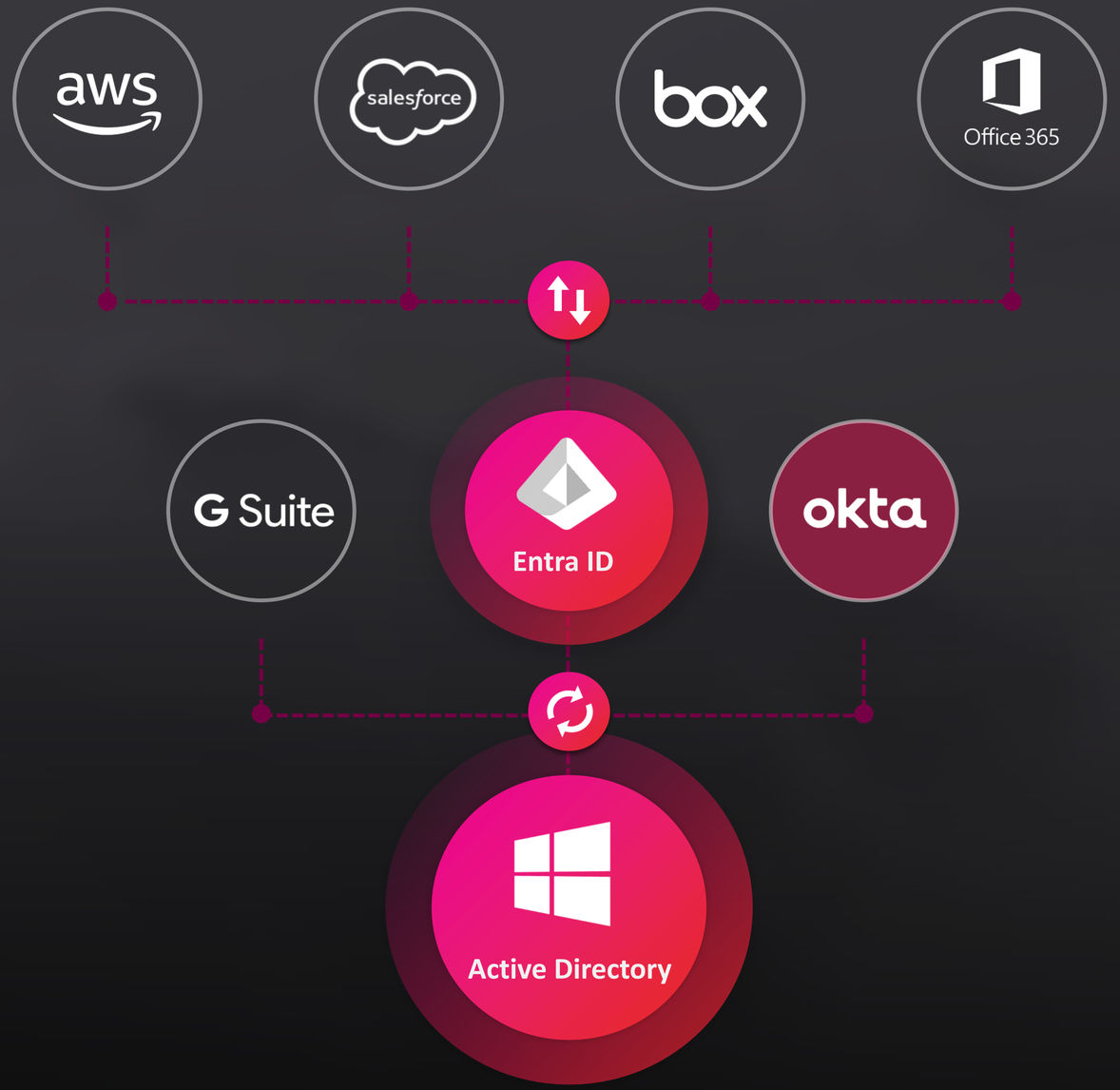
Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series

semperis

KEYS TO THE KINGDOM

If Active Directory isn't secure, nothing is

- 80% of all breaches involve credential abuse
- Systemic weakness make AD a soft target
- Cloud identity extends from AD
- Zero Trust model assumes hybrid AD integrity



For 90% of enterprises, identity starts with AD

semperis

FOUNDATIONAL IDENTITY SECURITY

So, what does it take to protect hybrid AD?

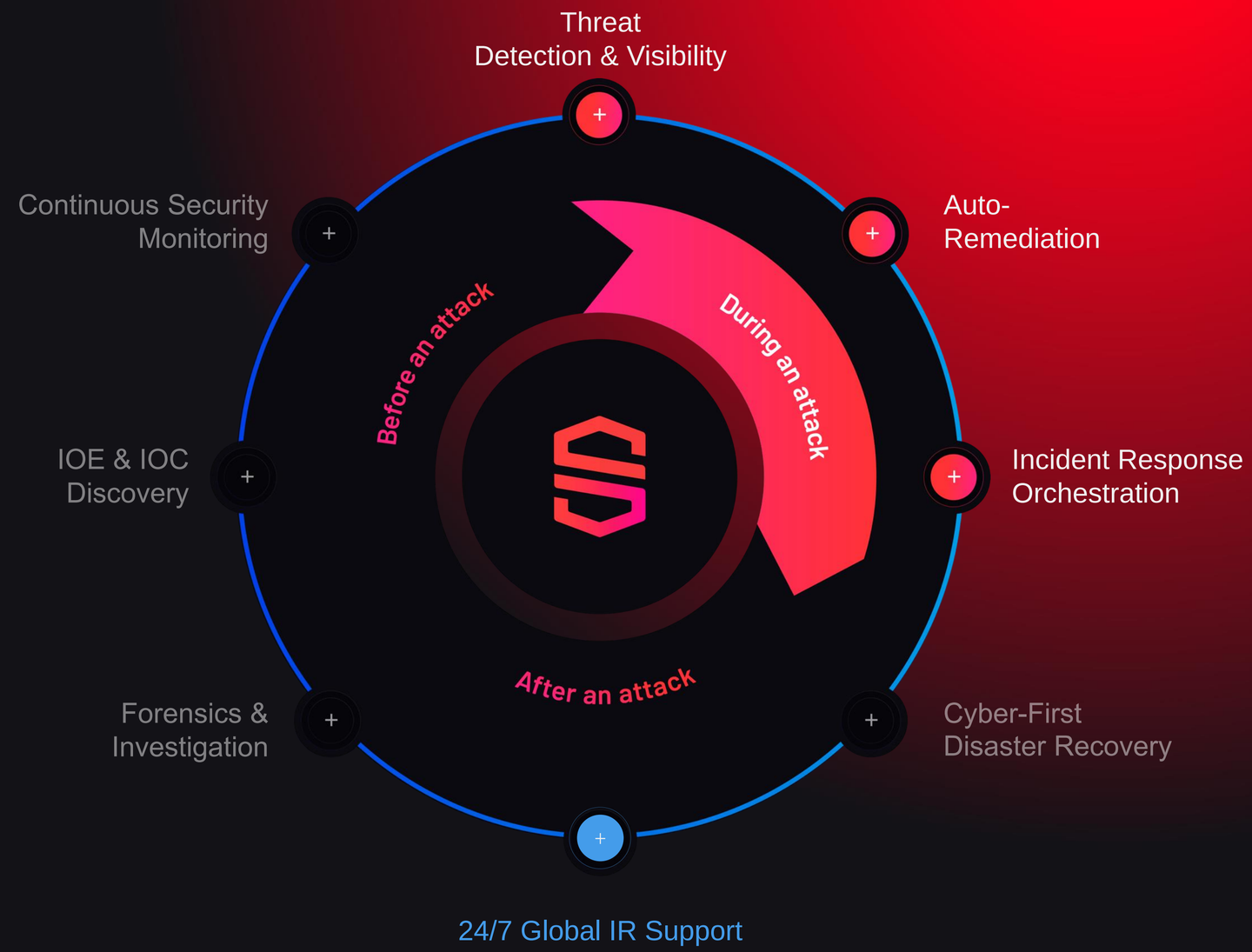
(AD and Entra ID)

semperis

PRE attack

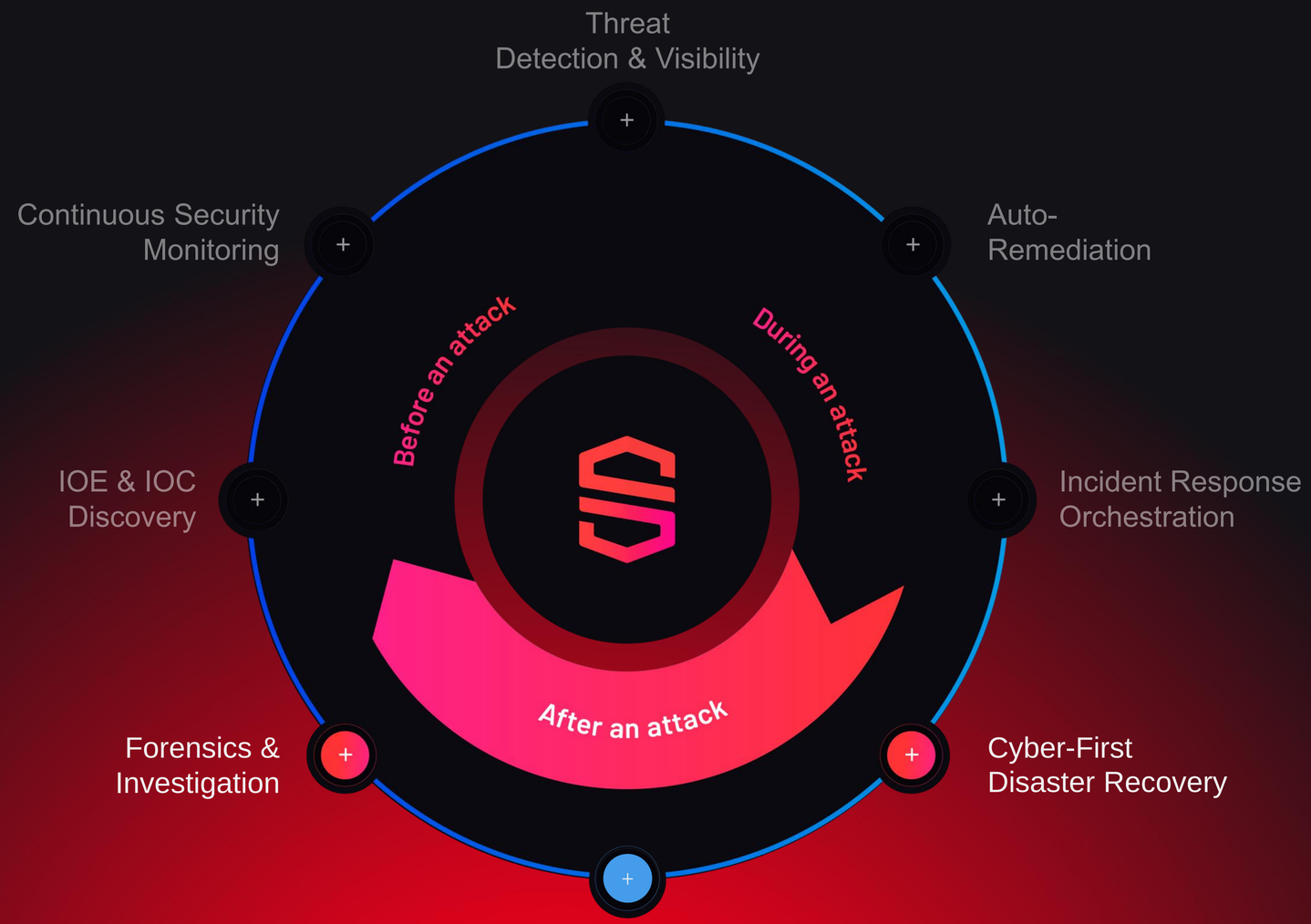
semperis

DURING attack



semperis

POST attack



Identity Resilience Platform

End to end resilience for your Microsoft Hybrid identity

Active Directory Forest Recovery
Cyber-first AD disaster recovery

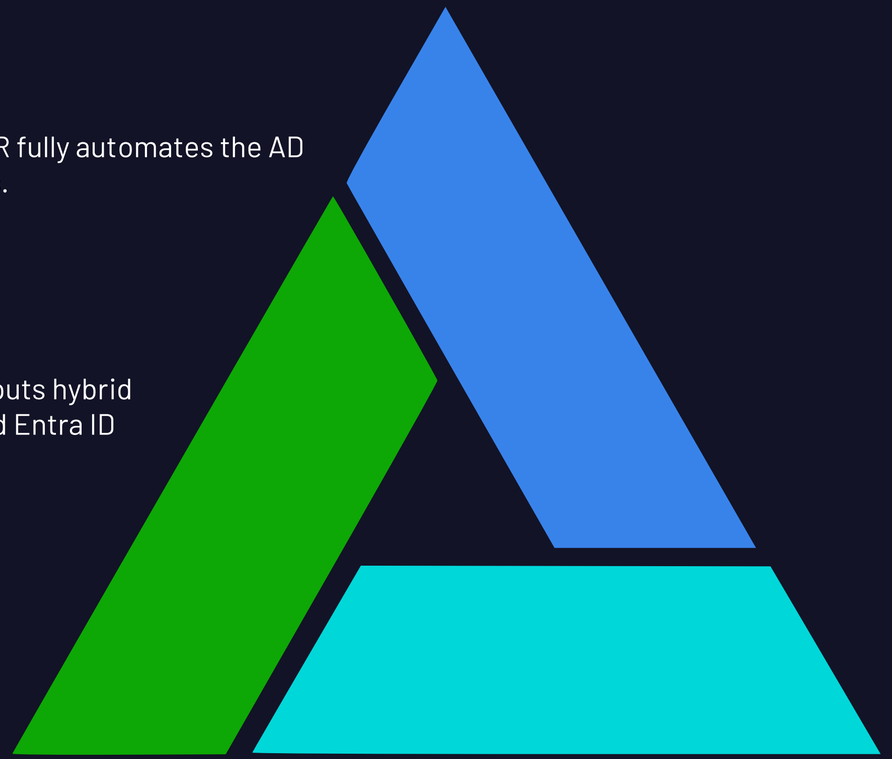
ADFR is the only backup and recovery solution purpose-built for recovering Active Directory from cyber disasters. ADFR fully automates the AD forest recovery process, reduces downtime, eliminates risk of malware reinfection, and enables post-breach forensics.

Directory Services Protector
Hybrid AD threat prevention, detection, and response

Directory Services Protector (DSP) is a Gartner-recognized identity threat detection and response (ITDR) solution that puts hybrid Active Directory security on autopilot with continuous monitoring and unparalleled visibility across on-premises AD and Entra ID environments, tamperproof tracking, and automatic rollback of malicious changes.

Disaster Recovery for Entra Tenants
Backup and recovery for Entra ID resources

Disaster Recovery for Entra Tenant (DRET) gives you secure, reliable backup services for critical Entra ID data, eliminating time-consuming storage management processes and ensuring fast post-attack recovery.



semperis

#1 NEW TARGET

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

“While organizations understand the criticality of AD, the security of AD is often overlooked. If AD is breached, an attacker gets virtually unrestrained access to the organization’s entire network and resources. **This makes AD a prominent high-value target for threat actors.”**

Gartner

Emerging Technologies and Trends Impact Radar: Security

semperis

UNPARALLELED SUPPORT

Breach preparedness & incident response

Semperis isn’t just another security vendor but instead a true partner through and through

Threat Research Team (IOE & IOC Discovery)

24/7 Incident Response Team

semperis

Gartner recommends adding an AD-specific disaster recovery tool

> Organizations without a useful backup system will be left with **few options but to pay the ransom.”**

Gartner

How to Protect Backup Systems from Ransomware

"Accelerate recovery from attacks by adding a dedicated tool for backup and recovery of Microsoft Active Directory.”

"Tools from vendors such as ...Semperis... offer a **more complete backup and recovery platform for Active Directory** than those found in the Active Directory backup modules included in most enterprise backup software.”

Gartner: How to Protect Backup Systems from Ransomware

"If Active Directory isn’t **cleaned and secured** before applications are brought back online, there is a high risk that attackers will quickly regain control of recovered applications.”

"Maintain regular backups of Active Directory in a secure location, such as data vault and practice the recovery process. If the budget allows, add Active Directory-specific backup tools to **simplify and speed up the process.”**

Gartner: Restore vs. Rebuild – Strategies for Recovering Applications After a Ransomware Attack

AD FOREST RECOVERY

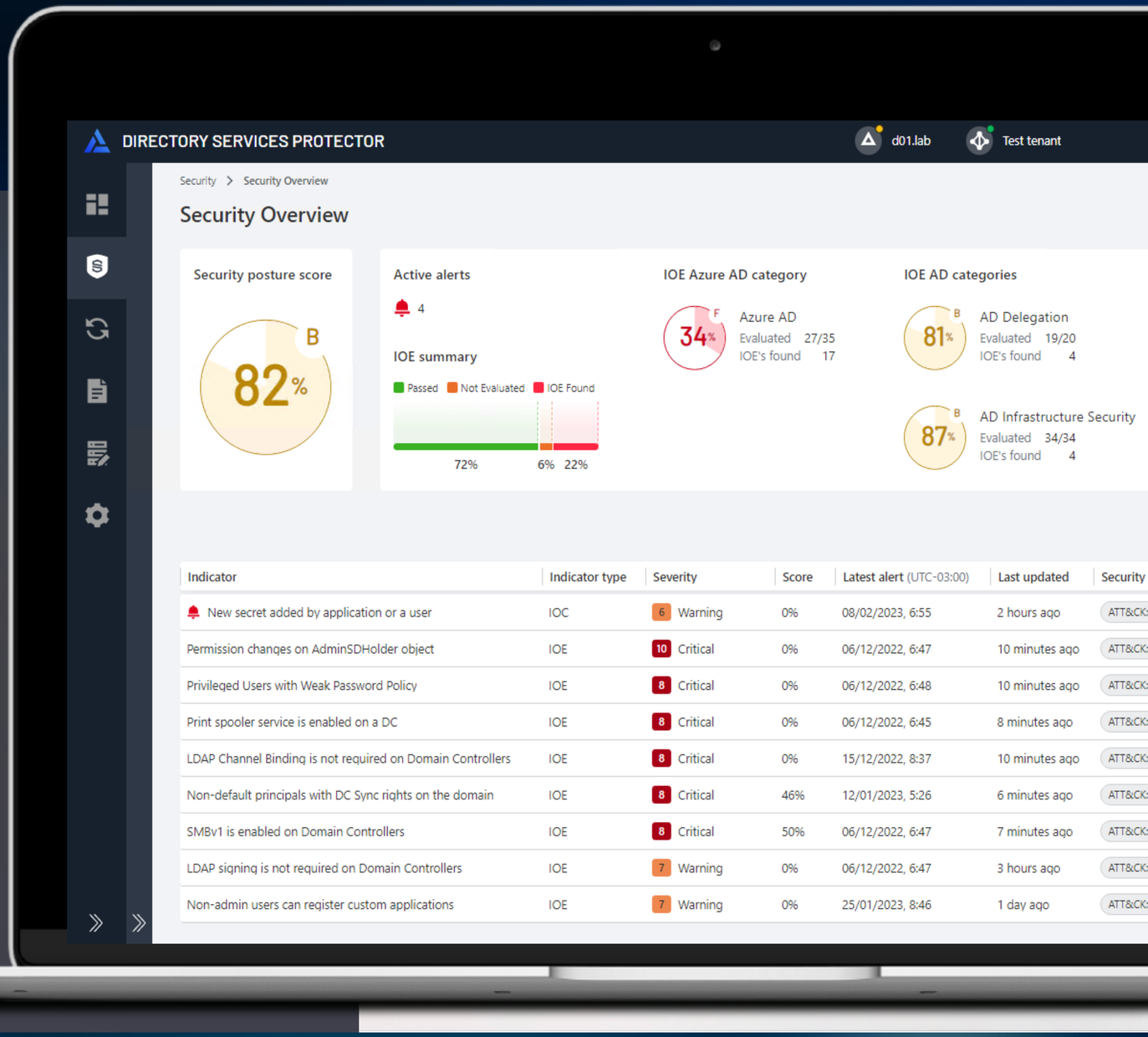
Shorten forest recovery by 90%

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

DIRECTORY SERVICES PROTECTOR

Prevent, detect, & respond

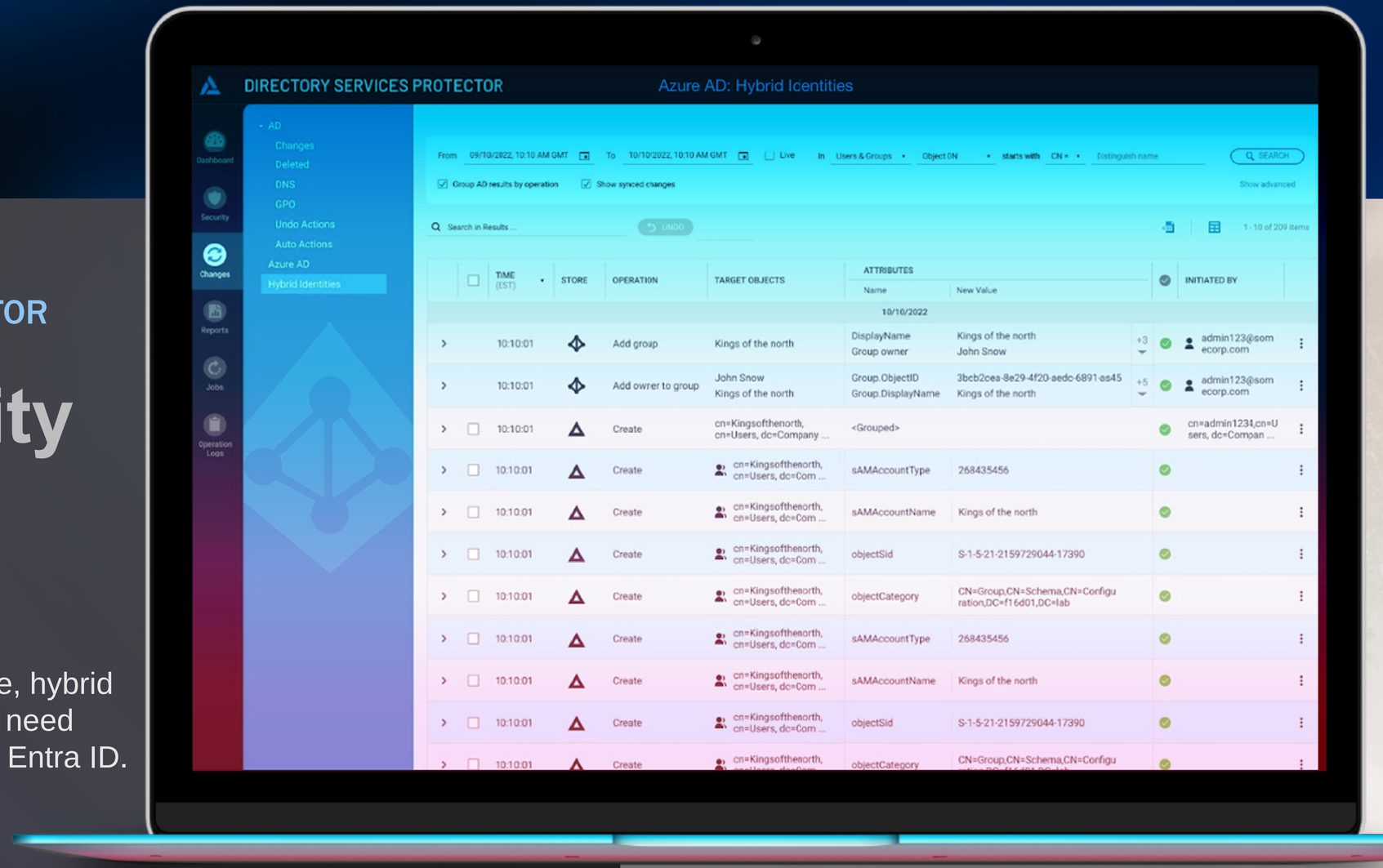
- Continuous vulnerability assessment
- Tamperproof tracking
- Real-time security alerts
- Auto-remediation (malicious change rollback)
- Compliance reporting



DIRECTORY SERVICES PROTECTOR

Extend identity protection to Entra ID

Without seeing the complete picture, hybrid AD attacks fly under the radar. You need visibility into threats across AD and Entra ID.



- Entra ID security indicators
- Entra ID change tracking and rollback
- Hybrid view of AD and Entra ID

Prevention, detection, and response all in one console.

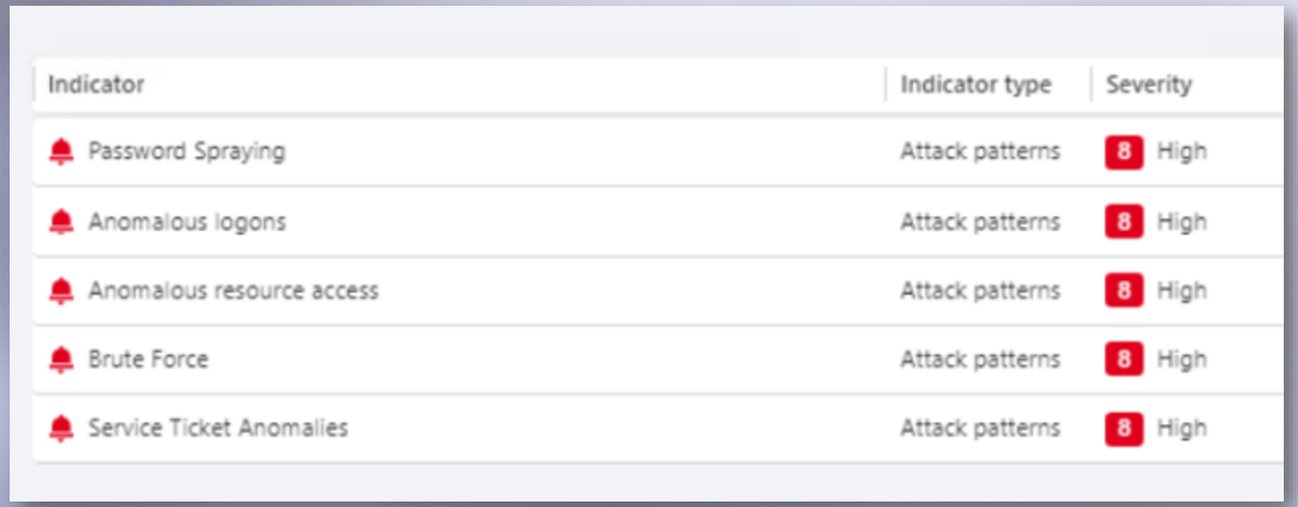
semperis

IDENTITY RUNTIME PROTECTION

Powered by Lightning

ML-powered, expert-built live attack pattern detection

Lightning IRP helps organizations **reduce cyberattack risk** and **save response time** by providing live detection of attack patterns that could signal an impending attack



Indicator	Indicator type	Severity
Password Spraying	Attack patterns	8 High
Anomalous logons	Attack patterns	8 High
Anomalous resource access	Attack patterns	8 High
Brute Force	Attack patterns	8 High
Service Ticket Anomalies	Attack patterns	8 High

- Reduce attack noise to focus on true threats
- Detect dangerous attack patterns such as password spray attacks, brute force attacks, and service ticket anomalies
- Accelerate response time and reduce cyberattack risk

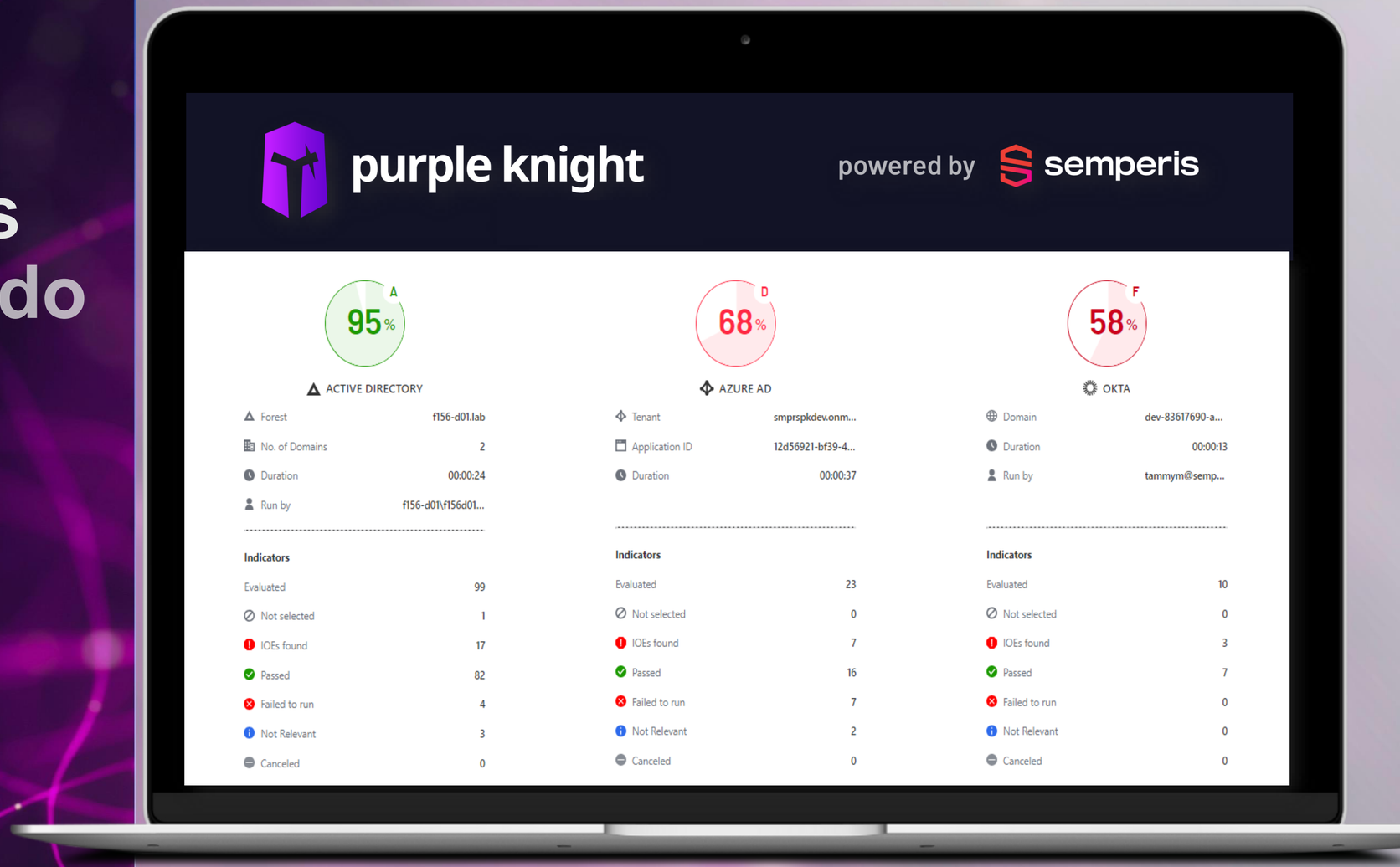
semperis

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

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

4 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