semperis

Get the industry's most comprehensive hybrid Active Directory protection.

Identity Threat Detection and Response (ITDR) is among Gartner's top cybersecurity trends.

Active Directory is exploited in 9 out of 10 attacks.

The exploitation of Active Directory, the identity system used in 90% of organizations worldwide, is a common thread in the surge of recent ransomware attacks. Attackers take advantage of weak AD configurations to identify attack paths, access privileged credentials, and deploy ransomware into target networks. Semperis is the only Identity Threat Detection and Response (ITDR) provider that protects AD and Azure AD across the entire identity-attack lifecycle—before, during, and after an attack—all supported by a global incident response team.

- **50M+ identities protected globally**
- **130+ AD-specific threat indicators updated daily**
- **Continuous IOC discovery & monitoring**
- **Fully automated malicious change tracking & rollback**
- **90% reduction in AD full forest recovery time**
- **24/7 digital forensics & incident response (DFIR)**

Are you considering an ITDR solution for hybrid AD protection?

Semperis checks all the boxes.

Gartner's specific ITDR guidance for organizations include:

- ✓ Evaluate AD TDR tools for use with your enterprise AD and cloud AD implementations
- ✓ Prioritize tools that implement security posture assessment and real-time monitoring functionality
- ✓ Prioritize tools that support both preventive and detective controls
- ✓ Give preference to tools that incorporate guidance from de facto industry standards such as: MITRE ATT&CK, MITRE D3FEND, and ANSSI
- ✓ Prepare for the unexpected: Uncover new zero-day exploits against AD. Include Active Directory in your organization's vulnerability and threat management and incident response planning.

FROST & SULLIVAN

Semperis won Frost & Sullivan's Competitive Strategy Leadership Award for global AD security and recovery industry excellence

"Semperis has **unmatched experience in breach preparedness and incident response** to Active Directory and other identity-based cyberattacks. Semperis' solution-based approach focuses not only on their premier technology to meet customer challenges but also best practices and guidance for people and processes, setting them apart from their competitors."

SARAH PAVLAK | FROST & SULLIVAN

Learn why Semperis is among the top fastest-growing cybersecurity companies in America.

100+ YEARS'

Microsoft MVP experience

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

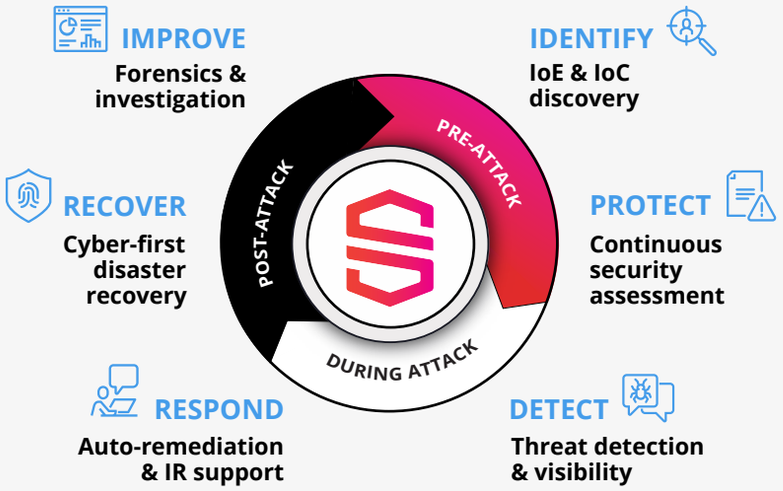
ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 50 million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, NJ, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series (www.hipconf.com) and built the free Active Directory security assessment tool, Purple Knight (www.purple-knight.com). The company has received the highest level of industry accolades, named to Inc. Magazine's list of best workplaces and ranked the fastest-growing cybersecurity company in America by the Financial Times.

Integrity and availability. Always.

Purpose-built for securing hybrid AD environments, Semperis delivers first-of-its-kind solutions to address the entire lifecycle of an identity-based attack—including finding and fixing security vulnerabilities, intercepting privilege escalation and persistence, and quickly responding to ransomware and other data integrity emergencies.



Products and Services

Directory Services Protector (DSP) puts AD security on autopilot with continuous threat monitoring, real-time alerts, and autonomous remediation capabilities.

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

Active Directory Forest Recovery (ADFR) orchestrates a fully automated forest recovery process—avoiding human errors, reducing downtime by 90%, and eliminating the risk of malware reinfection.

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

Purple Knight is a community-driven Active Directory security assessment tool used by thousands of organizations to quickly identify vulnerabilities in hybrid AD environments and receive prioritized remediation guidance. Request free access at purple-knight.com.

- 10,000+ downloads to date
- 130+ security indicators
- 45% AD attack surface reduction

Forest Druid is a Tier 0 attack path management tool—natively compatible with Active Directory—that helps defensive teams identify the true Tier 0 perimeter and quick prioritize high-risk misconfigurations that could lead to an attack.

- Identity the true Tier 0 perimeter
- Cut down excessive privileges
- Save time in closing attack paths

BREACH PREPAREDNESS & RESPONSE SERVICES

Semperis provides extensive support with access to AD security and incident response experts who can conduct in-depth assessments and help with pre- and post-attack investigations and disaster recovery.

Threat Research Team (IOE & IOC Discovery)

24/7 Incident Response Team

Semperis Headquarters
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)