AN INTERVIEW WITH MICKEY BRESMAN
CEO, SEMPERIS

# COMPREHENSIVE IDENTITY PROTECTION AND RESILIENCY

Identity is the new security perimeter in a world of ever-evolving digital threats, and Semperis stands at the forefront of this change with its innovative Identity Resiliency Platform. Offering comprehensive protection across Active Directory (AD) and Azure AD, the platform ensures operational resilience and robust security in the face of modern threats. Beyond threat detection, Semperis provides automated remediation and quick, malware-free recovery. In a recent chat with Mickey Bresman, CEO of Semperis, we learned more about the nuances of their platform, their proactive approach to evolving cybersecurity risks, the importance of their dedicated incident response team, and their substantial role in aiding with AD modernization—an essential, yet often underestimated facet of cyber defense.

***TAG Cyber: Can you provide an overview of Semperis' Identity Resiliency Platform and its key features?***

**SEMPERIS:** Cyberattackers persistently exploit vulnerabilities and evade security measures, necessitating a layered defense strategy. While EDR, MFA, and similar tools are essential, relying on a single tool is insufficient to protect against evolving threats.

At the same time, organizations and analysts (such as Gartner) acknowledge that identity has become the security perimeter. For example, an Active Directory (AD) is an active target, and eight or nine out of every 10 cyberattacks include AD. Considering that most organizations have AD and Azure AD (now called Microsoft Entra ID) as their core identity platform, bad actors specifically focus on those services, trying to get the "keys to the kingdom," which makes identity threat detection and response (ITDR) vital to modern cyber defense.

The Semperis Identity Resiliency Platform equips organizations with a comprehensive suite of tools and services for robust defense against cyberattacks. It offers in-depth protection for Active Directory (AD) and Azure AD—the identity backbone for 90% of organizations—ensuring operational resilience and identity security.

Organizations rely on the Semperis platform to enhance AD security by closing gaps, monitoring configurations, and analyzing attack paths. Our ITDR tools detect threats that evade traditional monitoring with change auditing and auto-remediation designed to counter fast-moving attacks. Our backup and recovery

**Organizations rely on the Semperis platform to enhance AD security by closing gaps, monitoring configurations, and analyzing attack paths. Our ITDR tools detect threats that evade traditional monitoring while change auditing and auto-remediation counter fast-moving attacks.**

tools reduce AD recovery time, ensuring a malware-free recovery. Strengthening identity defense, we offer post-breach forensics, breach preparedness, and response services delivered by AD cybersecurity experts. Additionally, we provide AD modernization and consolidation tools and services, valuable in M&A scenarios during the AD migration stage.

***TAG Cyber: How does Semperis stay ahead of evolving cybersecurity risks targeting Active Directory?***

**SEMPERIS:** AD and identity security experts are a significant part of our research and development teams. These teams have deep knowledge of AD and Azure AD, how cyberattackers target them, and emerging threats.

Our teams have decades of combined experience responding to cyber incidents. For example, our incident response (IR) practice allows us to see cyber criminals' techniques. We combine insights from our IR teams and security researchers to constantly enhance our solutions to deal with the latest types of attacks.

Considering our customers' industry and AD infrastructure, we customize our expertise to meet their needs. Our approach encompasses the entire life cycle of an identity-based attack, from identifying entry points to understanding post-infiltration activities and the injection of pervasive malware. Our solutions continually update IOEs, IOCs, and IOAs to monitor and counter evolving threats.

***TAG Cyber: How does Semperis address the security challenges of securing AD environments?***

**SEMPERIS:** Semperis gives defenders the advantage at every stage of an identity-based cyberattack. Our platform provides deep, comprehensive ITDR for AD and Azure AD across each stage of the identity-based attack cycle: before, during, and after an attack.

We help organizations fend off cyber threats through hybrid identity assessments that spot IOEs, IOCs, and IOAs, combined with attack-path analysis that prioritize Tier 0 assets, such as AD-privileged accounts. We also offer AD migration and consolidation support to help organizations modernize their hybrid AD environments for optimal security.

When attackers evade other defense systems, Semperis solutions can detect and remediate suspicious activity in AD and Azure AD and respond to active attacks through auto-remediation, notification, and incident response services. And in the worst-case scenarios, we enable fast AD recovery that eliminates back doors that attackers have left behind.

***TAG Cyber: Can you elaborate on the role of your dedicated incident response team?***

**SEMPERIS:** No vendor or services provider can outmatch Semperis' collective security experience in Directory Services. Our Breach Preparedness and Incident Response team comprises Microsoft MVPs, former Microsoft Premier Field Engineers, and other leading security experts. Together, they provide unrivaled experience protecting the most sensitive environments and deep expertise in on-prem AD, Azure AD, Okta, and other enterprise identity systems.

Our goal is to make hybrid AD security as efficient, comprehensive, and easy as possible. We help with fast recovery and post-breach forensics in the event of a breach and offer multiple services to help optimize identity-based security.

The AD Security Assessment is a high-level review of the environment and the considerations that led to the current design. This review evaluates important AD security boundaries and functions. The Operational Procedures Review evaluates current operational procedures.

Our Security Configuration Review uses automated tools like Purple Knight AD security assessment and manual methods to identify IOEs and IOCs in the AD environment. The Standard Active Directory Security Assessment (ADSA) targets the tactical level of the organization's AD security posture. It gathers technical information from AD and auxiliary systems, offering tactical remediation guidance.

The Attack Surface Reduction service involves an annual ADSA and quarterly sessions with Semperis experts to analyze IOCs, IOEs, and IOAs. Our team makes recommendations for reducing the attack surface and eliminating security exposures in the AD environment. We can also perform an attack path analysis to identify abnormal delegated rights and dangerous or unintended attack paths to Tier 0 assets and other critical assets.

***TAG Cyber: How does Semperis help organizations modernize their AD systems?***

**SEMPERIS:** Nine out of 10 attacks exploit AD, and many AD vulnerabilities are the result of years of configuration drift. Attackers also exploit vulnerabilities exposed during AD migration and consolidation following a merger or acquisition. Multi-forest environments face exponential risk, as the breach of one forest often leads to another, ending in a complete organization compromise.

Where AD is involved, modernization is often an urgent security priority. AD modernization is the surest way to dramatically reduce the AD attack surface. However, a full-scale AD migration and consolidation initiative requires extensive effort and planning, so many organizations delay the project.

Semperis offers a comprehensive AD modernization solution backed by industry-leading identity security tools and expert support, with a high focus on AD security throughout the migration and modernization process. We also help design the desired environment to meet modern security standards. Careful planning enables organizations to avoid security pitfalls, mitigate potential problems, and fix existing AD exposures.

As part of our approach to AD migrations, we mitigate risks during the migration process by spinning up an exact copy of the production AD to test the migration, set DSP to monitor for new vulnerabilities, and roll back unintended changes. Post-migration, Semperis monitors the destination AD to prevent configuration drift and continuously assesses the new environment for IOEs and IOCs to maintain an optimal level of AD security.