



# The industry's most comprehensive hybrid Active Directory threat detection and response platform.

One platform for peace of mind. Semperis Directory Services Protector (DSP) is a comprehensive platform that continuously monitors Active Directory and Azure Active Directory for indicators of exposure, detects advanced attacks, and enables rapid response.

[Request demo →](#)

- Stop attackers from gaining access to on-premises AD and Azure AD
- Automate threat protection and response
- Continuously validate your AD security posture

## If your hybrid AD isn't secure, nothing is.

Business applications on-premises and in the cloud rely on Active Directory and Azure Active Directory, making it a critical piece of your IT infrastructure. But securing Active Directory is difficult given its constant flux, sheer number of settings, and increasingly sophisticated threat landscape. Securing a hybrid system brings additional challenges as many attacks start on-premises and move to the cloud. Semperis Directory Services Protector (DSP) continuously monitors Active Directory and Azure Active Directory for indicators of exposure and provides a single view of activities on-prem and in the cloud.

### CATCH AD AND AZURE AD VULNERABILITIES BEFORE ATTACKERS DO

### ELIMINATE BLIND SPOTS IN HYBRID ACTIVE DIRECTORY SECURITY

### ENABLE RAPID RECOVERY

## Proactively protect AD and Azure AD from cyberattacks.

Attackers are getting better by the minute at targeting soft spots in your hybrid AD system, exploiting weaknesses in on-premises AD to enter the environment, then moving online to Azure AD.

- DSP continuously monitors for indicators of exposure and compromise—uncovered by the Semperis threat research team—that threaten AD and Azure AD.

Attackers use powerful hacking and discovery tools to create backdoors and establish persistent access inside of hybrid Active Directory—avoiding detection by traditional SIEM solutions.

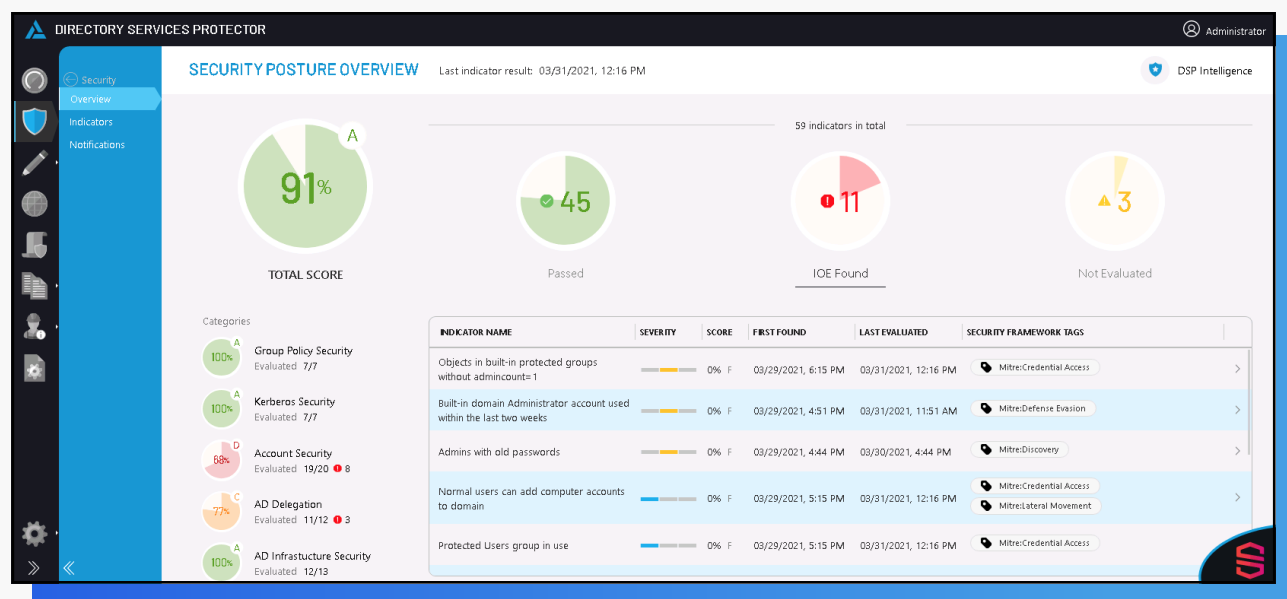
- DSP uses multiple data sources—including the AD replication stream—to capture changes that evade agent-based or log-based detection.

Intruders and rogue administrators can rapidly wreak havoc across your systems on a scale that is difficult to monitor and remediate effectively with human intervention.

- Semperis DSP provides a unified dashboard that shows malicious changes in your on-prem Active Directory and Azure Active Directory so you can close security gaps before attackers strike.

# Semperis DSP

Figure 1.0 - DSP Dashboard: Security Posture Overview



## Continuously track your hybrid AD security score

In a single view, track overall security posture as well as status of:

- Kerberos security
- AD delegation
- Group policy
- Account security
- AD infrastructure security

## Put hybrid AD security on autopilot.

Most organizations can't keep eyes on monitors 24/7. But threat actors are working round-the-clock—through weekends and holidays—to break into your information systems. DSP provides continuous threat monitoring, real-time alerts, and autonomous remediation capabilities.

### INDUSTRY ANALYST

“Active Directory is the Achilles’ heel for enterprise security programs. Semperis is offering a timely solution considering that AD has been at the center of many widespread and business-crippling attacks in recent years.”



- Christina Richmond, Vice President of IDC

**VULNERABILITY ASSESSMENT**

Continuously monitor for “indicators of exposure” that could result in security compromises to your hybrid AD environment. Leverage built-in threat intelligence from a community of security researchers.

**AUTOMATED REMEDIATION**

Create audit notifications on changes to sensitive AD and Azure AD objects and attributes with the option to automatically undo select changes.

**TAMPERPROOF TRACKING**

Capture changes even if security logging is turned off, logs are deleted, agents are disabled or stop working, or changes are injected directly into AD or Azure AD.

**INSTANT FIND AND FIX**

Use Semperis DSP’s online database to find and fix unwanted hybrid AD object and attribute changes in two minutes or less.

**GRANULAR ROLLBACK**

Revert changes to individual attributes, group members, objects, and containers – and to any point in time, not just to a previous backup.

**FORENSIC ANALYSIS**

Identify suspicious changes, isolate changes made by compromised accounts, and more. Use DSP data to support Digital Forensics and Incident Response (DFIR) operations to track down the sources and details of incidents.

**SIEM ENRICHMENT**

Eliminate blind spots in your security incident and event management (SIEM) system with out-of-the-box integration.

**DELEGATION**

Leverage robust Role-Based Access Control (RBAC) and a rich web user interface to give administrators view and restore capabilities for their specific scope of control.

**POWERFUL REPORTING**

Gain insight into the operational, best practice, compliance, and security aspects of your hybrid AD environment using built-in reports created by AD experts. Create custom reports based on sophisticated LDAP and DSP database queries.

**REAL-TIME NOTIFICATIONS**

Be alerted through email notifications as operational and security related changes happen in your hybrid AD environment.

**POWERSHELL SUPPORT**

Use the DSP PowerShell module to automate processes and integrate DSP operations and management into existing toolsets.

**SUPPORT REGULATORY COMPLIANCE**

Semperis DSP provides preconfigured compliance modules for major regulations and frameworks to automate reporting.

- PCI
- HIPAA
- SOX
- GDPR

**CONTINUOUS SECURITY VALIDATION**

Automated monitoring to combat security posture regression caused by configuration drift—compromised configuration settings that accrue over time, leaving you vulnerable to attacks.

**TRACK AZURE AD CHANGES**

Use near real-time change tracking in the DSP for Azure AD module to monitor changes to role assignments, group memberships, and user attributes.

**VISUALIZE HYBRID AD SECURITY**

With the DSP for Azure AD module, easily view changes that originated in Azure AD and use the hybrid view to correlate changes between on-prem AD and Azure AD.

# Is your hybrid AD environment secure?

Security scores from users of the Semperis Purple Knight security assessment tool revealed that organizations are failing to close security gaps in the hybrid AD systems, reporting an average score of 61%—a barely passing grade—leaving them vulnerable to the increasing number of attacks that start on-premises and move to Azure AD.

Better by design and **built for the enterprise**, Semperis Directory Services Protector provides the capabilities that organizations need to defend hybrid Active Directory systems from today's most sophisticated cyberattacks, as well as to recover quickly from everyday mistakes.

Defenders must anticipate their adversaries' advances and be able to thwart attacks at every stage of the cyber kill chain.

**Meet Semperis DSP.**

**Semperis**

IT Resilience Orchestration




Source: Gartner Peer Insights

info@semperis.com  
www.sempersis.com

**Semperis Headquarters**  
221 River Street  
9th Floor  
Hoboken, NJ 07030  
+1-703-918-4884

**Request demo** →

 **Microsoft Partner**  
Enterprise Cloud Alliance  
Microsoft Accelerator Alumni  
Microsoft Co-sell

# Hybrid Active Directory environments are under attack.

With a hybrid scenario, the potential attack surface expands for adversaries.

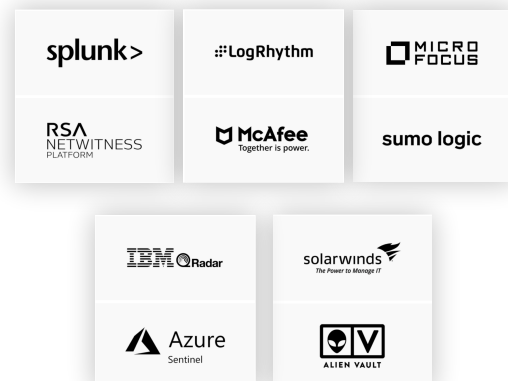
DSP for Azure Active Directory simplifies protecting your hybrid AD environment by tracking changes to on-prem AD and Azure AD in a single view, so you can stop attackers in their tracks.

[Learn More](#) →

## Restore sight to your SIEM

Semperis Directory Services Protector provides visibility into what's happening, who's doing what, as well as insight into the security posture of your hybrid Active Directory environment. And DSP catches advanced attacks that bypass traditional security logging—leaving most SIEM solutions blind. By continuously monitoring for vulnerabilities and allowing you to automatically remediate malicious or unwanted changes to AD and Azure AD, you can stop attackers in their tracks.

### OUT-OF-THE-BOX SIEM INTEGRATIONS



**VULNERABILITY ASSESSMENT, CHANGING TRACKING, AND REMEDIATION IN ONE SOLUTION FOR BOTH ON-PREMISES ACTIVE DIRECTORY AND AZURE ACTIVE DIRECTORY**

**A GROWING NUMBER OF ATTACKS CIRCUMVENT SECURITY AUDITING**

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures 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 New Jersey and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winning Hybrid Identity Protection conference ([www.hipconf.com](http://www.hipconf.com)). The company has received the highest level of industry accolades, most recently ranked #157 in the Inc. 5000 and the fourth fastest-growing company in the tri-state area and 35th overall in Deloitte's 2020 Technology Fast 500™. Semperis is accredited by Microsoft and recognized by Gartner.