semperis

COMPLETE SOLUTION FINDER
Empowering Data Protection

DIRECTORYSERVICES PROTECTOR

The industry's most comprehensive 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 for indicators of exposure, detects advanced attacks, and enables rapid response.

Request demo →

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

If AD isn't secure, nothing is.

More than ever, Active Directory is in the attackers' crosshairs. If Active Directory goes down, your entire business goes down. AD is the primary gateway to your critical information systems—and an easy target for cyber-attackers looking for a way to steal sensitive information, deploy ransomware, or even bring down your business operations completely. Why is AD so easy to exploit? Because of its constant flux sheer number of settings and increasingly sophisticated threat landscape. Even the most rigorous security implementation can degrade over time because of configuration drift—the gradual erosion of security-optimized settings and practices that comes with rapidly evolving businesses.

Proactively protect AD from cyberattacks.

CATCH AD VULNERABILITIES BEFORE ATTACKERS DO

Attackers are getting better by the minute at finding and exploiting your AD weak spots—such as accounts with unconstrained delegation, unprivileged users with DC rights, and many more.

→ DSP continuously monitors for indicators of exposure and compromise that threaten AD, empowering you to gain and keep control of AD security.

ELIMINATE BLIND SPOTS IN ACTIVE DIRECTORY SECURITY

Attackers use powerful hacking and discovery tools to create backdoors and establish persistent access inside of 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-baseddetection.

ENABLE RAPID RECOVERY

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.

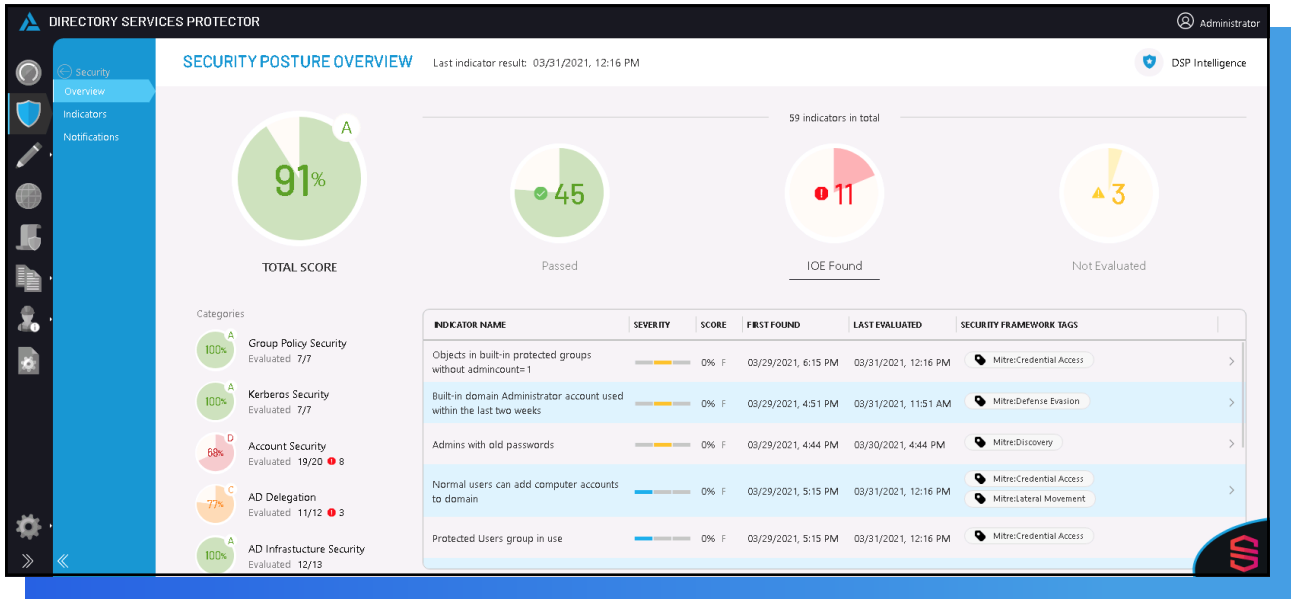
→ With DSP, you can see who made changes and automatically reverse malicious or unwanted changes—without mounting backups or taking DCs offline.

semperis

So how do you accomplish this? **That's easy:**

Semperis DSP

Figure 1.0 –DSP Dashboard: Security Posture Overview



Continuously track your 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 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

semperis

VULNERABILITY ASSESSMENT

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

AUTOMATED REMEDIATION

Create audit notifications on changes to sensitive 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.

INSTANT FIND AND FIX

Use Semperis DSP's online database to find and fix unwanted 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.

SIEMENRICHMENT

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 AD 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 AD.

POWERSHELL SUPPORT

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

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 cause by configuration drift—compromised configuration settings that accrue over time, leaving you vulnerable to AD attacks.

Request demo →

Would Your Organization Fail the Active Directory Security Assessment?

Initial scores from Purple Knight, an Active Directory security assessment tool from Semperis, revealed that organizations are failing at an alarming rate—**61% score on average**—extending the risk of systemic cyberattacks. Large organizations with legacy AD deployments at highest risk of falling victim to widespread attacks—like SolarWinds—that target inherent Windows vulnerabilities.

Better by design and **built for the enterprise**, Semperis Directory Services Protector provides the capabilities that organizations need to defend AD 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.

Take back the keys to your kingdom.

VULNERABILITY ASSESSMENT, CHANGING TRACKING, AND REMEDIATION—IN ONE SOLUTION.

Active Directory is under attack from a barrage of cybercriminal groups. It's been the entry point for dozens of recent cyberattacks, including the massive SolarWinds breach. And since AD extends to the cloud, any tampering of it will cause a ripple effect across the entire identity infrastructure.

But you can successfully defend AD against attacks with a proactive, comprehensive approach to threat protection.

Restore sight to your SIEM

A GROWING NUMBER OF ATTACKS CIRCUMVENT SECURITY AUDITING

Semperis Directory Services Protector provides visibility into what's happening, who's doing what, as well as insight into the security posture of your AD. 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, you can essentially stop attackers in their tracks.

OUT-OF-THE-BOXSIEMINTEGRATIONS

splunk> · LogRhythm · MICRO FOCUS · RSA NETWITNESS PLATFORM · McAfee Together is power. · sumo logic · IBM QRadar · solarwinds · Azure Sentinel · ALIEN VAULT

Semperis
IT Resilience Orchestration
5 ★★★★★
Source: Gartner Peer Insights

Semperis is the pioneer of identity-driven cyber resilience for cross-cloud and hybrid environments. The company provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services—the keys to the kingdom. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors. Semperis is headquartered in New York City and operates internationally, with its research and development team distributed between San Francisco and Tel Aviv.

Semperis hosts the award-winningHybrid Identity Protection conference. The company has received the highest level of industry accolades; most recently being ranked the fourth fastest-growing company in the tri-state area and 35th overall in Deloitte's 2020Technology Fast 500™.Semperis is accredited by Microsoft and recognized by Gartner.

info@semperis.com
www.semperis.com

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

Request demo →

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