semperis

DIRECTORY SERVICES PROTECTOR

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

Semperis Directory Services Protector (DSP) 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.

- Stop attackers from gaining access to on-premises AD and Entra ID
- Automate remediation of unwanted changes in on-prem AD and Entra ID
- 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 Entra ID, making it a critical piece of your IT infrastructure. But securing Active Directory is difficult given its constant flux, sheer number of settings, and the 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 Entra ID for indicators of exposure, provides a single view of activities on-prem and in the cloud, and automatically remediates unwanted changes in AD and Entra ID.

Proactively protect AD and Entra ID from cyberattacks.

CATCH AD AND ENTRA ID VULNERABILITIES BEFORE ATTACKERS DO

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 to Entra ID.

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

ELIMINATE BLIND SPOTS IN HYBRID ACTIVE DIRECTORY SECURITY

Threat actors use powerful attack 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.

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.

→ Semperis DSP automatically rolls back malicious changes in on-prem AD and Entra ID, offers manual rollback of Entra ID changes, and provides a unified dashboard so you can correlate changes across the hybrid AD environment.

semperis

VULNERABILITY ASSESSMENT

Continuously monitor for indicators of exposure (IOEs) 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 Entra ID 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 Entra AD.

POWERSHELL SUPPORT

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

GRANULAR ROLLBACK

Revert changes to individual attributes, group members, objects, and containers in on-prem AD and Entra ID—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 with Splunk and Microsoft Sentinel.

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—including a graphical overall security posture report. 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.

ENTRA ID ALERT & RESPONSE RULES

Use customizable alert and response rules to auto-undo or alert on specific changes to Entra ID.

ALIGN WITH SECURITY FRAMEWORKS

Map security indicators to standard security industry frameworks, including MITRE ATT&CK and MITRE D3FEND.

CONTINUOUS SECURITY VALIDATION

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

TRACK ENTRA ID CHANGES

Use near real-time change tracking to monitor changes to role assignments, group memberships, and user attributes.

VISUALIZE HYBRID AD SECURITY

Easily view changes that originated in Entra ID and use the hybrid view to correlate changes between on-prem AD and Entra ID.

Is your hybrid AD environment secure?

According to the Microsoft Digital Defense Report 2023, incident response teams found insecure AD configuration in **43% of engagements**.

semperis

Hybrid identity systems are under attack.

Hybrid identity systems—embracing both Active Directory and Entra ID—are increasingly common as organizations are deploying the optimal mix of on-premises assets and cloud services. But with that flexibility comes complexity—especially in managing hybrid identity security in a Microsoft environment. According to the Microsoft Digital Defense Report 2023, prevalent security gaps uncovered by the incident response team included "a broken security barrier between on-premises and cloud administration," which enables initial access, lateral movement, and persistence.

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

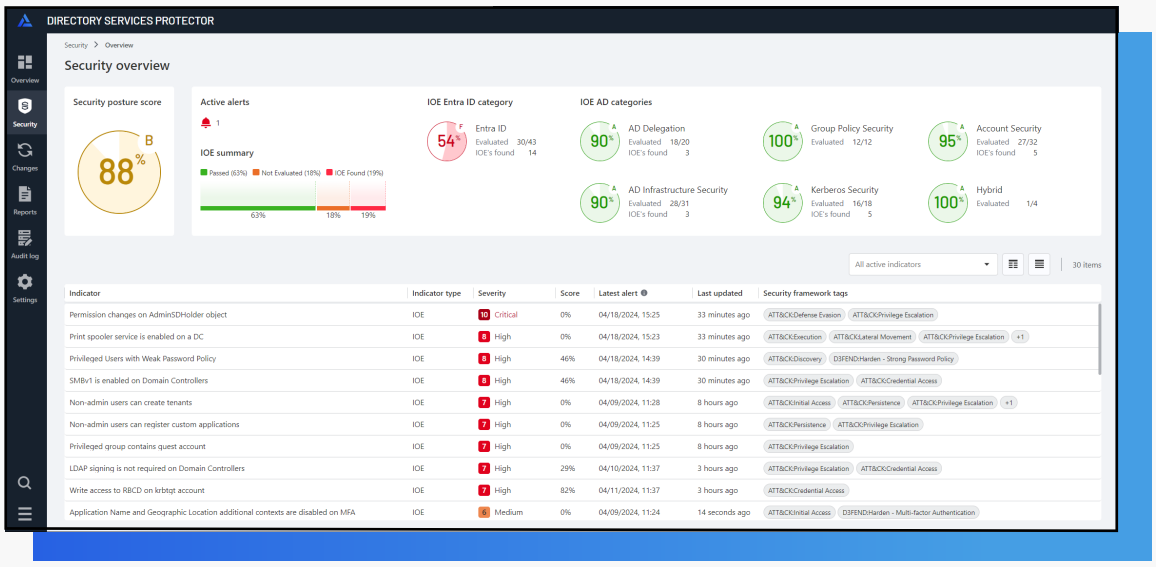
Managing hybrid identity system security is complicated. And since Entra ID is a critical piece of the security puzzle, organizations embracing a hybrid identity model must guard against an endless number of potential entry points. Directory Services Protector protects hybrid AD environments from cyberattacks with Entra ID change tracking, automated remediation of unwanted changes and customizable alert and response rules for Entra ID, and a hybrid view of the environment that helps correlate changes across on-prem AD and Entra ID.

Easily track security posture across AD and Entra ID with Directory Services Protector.

Clearly communicate overall hybrid AD security posture and manage AD and Entra ID threat detection and response:

- View overall score and scores in individual security categories, including AD account security, Group Policy security, Kerberos security, AD delegation, AD infrastructure, Entra ID, and hybrid security
- Drill down to specific indicators of exposure (IOEs) and compromise (IOCs)
- Use prioritized remediation guidance to immediately reduce the hybrid AD attack surface
- Automate rollback of unwanted changes in AD and Entra ID
- Visualize and correlate changes across Entra ID and on-prem AD in a single hybrid view
- Detect advanced AD attacks that bypass traditional log- and event-based monitoring such as SIEMs

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



Semperis

IT Resilience Orchestration

5 ★★★★★

Source: Gartner Peer Insights

DSP is the ultimate enterprise tool that offers a complete set of features required for a secure Active Directory. With change control, rollback, automation, alerts, comparison, secure implementation, ease of use, full support, and an excellent implementation team, DSP provides everything an enterprise needs to protect their Active Directory.

JULIO CESAR Z.
Technical Team Leader
(See more DSP reviews on G2)

info@semperis.com
www.semperis.com

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)

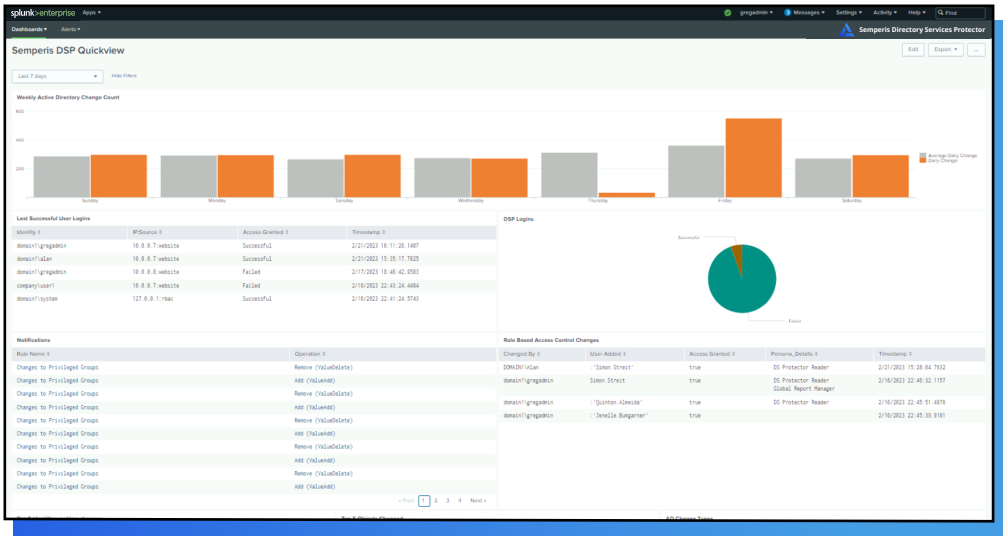
Restore sight to your SIEM

A GROWING NUMBER OF ATTACKS CIRCUMVENT SECURITY AUDITING

Unlike tracking tools that rely solely on security logs and agents on every domain controller, Semperis DSP monitors multiple data sources, including the Active Directory replication stream. The AD replication stream is the only reliable method of catching every change, no matter how attackers attempt to cover their tracks. Semperis DSP forwards suspicious AD changes to your SIEM system with meaningful context, drastically reducing the burden on security analysts. You can use pre-defined alerts for Microsoft Sentinel, Splunk, and other SIEM and SOAR tools, and build custom alerts for SecOps tools and ticketing systems such as ServiceNow.

OUT-OF-THE-BOX SIEM INTEGRATIONS

DSP simplifies threat detection and response with out-of-the-box integration, bringing previously hidden AD security data to the forefront in usable, familiar views for Sentinel and Splunk users.



DSP brings hybrid Active Directory security data into familiar Splunk views

splunk> Microsoft Sentinel