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 Azure AD environments, tamperproof tracking, and automatic rollback of malicious changes.

- 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 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 Azure Active Directory for indicators of exposure and provides a single view of activities on-prem and in the cloud.

Proactively protect AD and Azure AD from cyberattacks.

CATCH AD AND AZURE AD 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 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

ELIMINATE BLIND SPOTS IN HYBRID ACTIVE DIRECTORY SECURITY

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.

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, offers manual rollback of Azure AD changes, and provides a unified dashboard so you can correlate changes across the hybrid AD environment.

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 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 in on-prem AD and Azure AD—
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.

POWERSHELL SUPPORT

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

ALIGN WITH SECURITY FRAMEWORKS

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

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?

Only 27% of enterprise organizations are "very confident" they could prevent an Azure AD attack. Lack of visibility into attacks that start with on-prem AD and move to Azure AD drives concern about preventing attacks.

Hybrid identity systems are under attack.

Hybrid identity systems—embracing both Active Directory and Azure Active Directory—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.

Securing Active Directory requires a different approach from securing Azure Active Directory: The tools, processes, and threats are distinct.

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

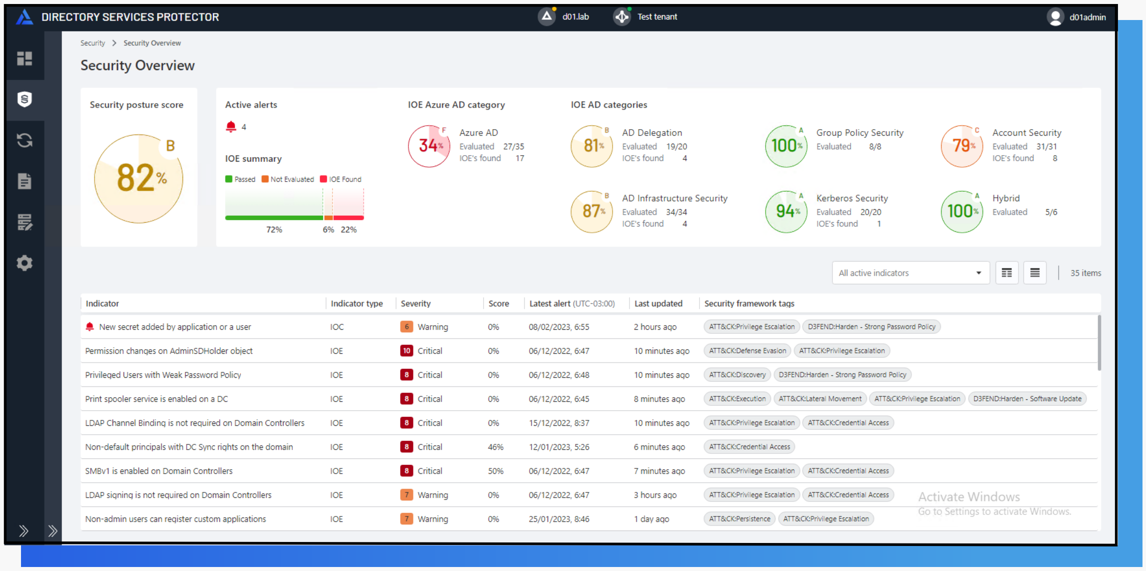
It's now common for attacks to start on-premises and move to the cloud—as in the SolarWinds attack—or move from cloud to on-premises. Managing hybrid identity system security is complicated. And since Azure AD is a critical piece of the security puzzle, organizations embracing a hybrid identity model must guard against an endless number of potential entry points. Directory Services Protector protects hybrid AD environments from cyberattacks with Azure AD change tracking, manual rollback of malicious changes in Azure AD, and a hybrid view of the environment that helps correlate changes across on-prem AD and Azure AD.

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

Clearly communicate overall hybrid AD security posture and manage AD and Azure AD 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, Azure AD, and hybrid security
- Drill down to specific indicators of exposure (IOEs) and compromise (IOCs)
- Use prioritized remediation guidance to immediately reduce the AD attack surface
- Track and manually roll back malicious changes in Azure AD
- Visualize and correlate changes across Azure AD 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 AZURE ACTIVE DIRECTORY



Indicator	Indicator type	Severity	Score	Latest alert (UTC-03:00)	Last updated	Security framework tags
New secret added by application or a user	IOC	6 Warning	0%	08/02/2023, 6:55	2 hours ago	ATT&CK:Privilege Escalation D3FEND:Harden - Strong Password Policy
Permission changes on AdminSDHolder object	IOE	10 Critical	0%	06/12/2022, 6:47	10 minutes ago	ATT&CK:Defense Evasion ATT&CK:Privilege Escalation
Privileged Users with Weak Password Policy	IOE	8 Critical	0%	06/12/2022, 6:48	10 minutes ago	ATT&CK:Discovery D3FEND:Harden - Strong Password Policy
Print spooler service is enabled on a DC	IOE	8 Critical	0%	06/12/2022, 6:45	8 minutes ago	ATT&CK:Execution ATT&CK:Lateral Movement ATT&CK:Privilege Escalation D3FEND:Harden - Software Update
LDAP Channel Binding is not required on Domain Controllers	IOE	8 Critical	0%	15/12/2022, 8:37	10 minutes ago	ATT&CK:Privilege Escalation ATT&CK:Credential Access
Non-default principals with DC Sync rights on the domain	IOE	8 Critical	46%	12/01/2023, 5:26	6 minutes ago	ATT&CK:Credential Access
SMBv1 is enabled on Domain Controllers	IOE	8 Critical	50%	06/12/2022, 6:47	7 minutes ago	ATT&CK:Privilege Escalation ATT&CK:Credential Access
LDAP signing is not required on Domain Controllers	IOE	7 Warning	0%	06/12/2022, 6:47	3 hours ago	ATT&CK:Privilege Escalation ATT&CK:Credential Access
Non-admin users can register custom applications	IOE	7 Warning	0%	25/01/2023, 8:46	1 day ago	ATT&CK:Persistence ATT&CK:Privilege Escalation

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

> 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**

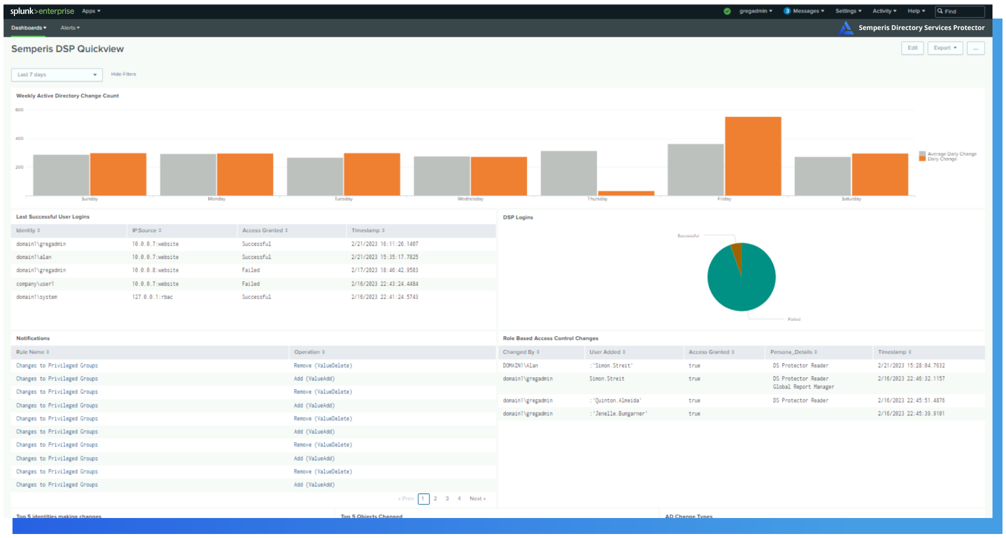
Restore sight to your SIEM

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.



Last Successful User Logins

Identity	IP:Source	Access Granted	Timestamp
domain1\gregadmin	10.0.0.7:website	Successful	2/21/2023 16:11:26.1407
domain1\alan	10.0.0.7:website	Successful	2/21/2023 15:35:17.7825
domain1\gregadmin	10.0.0.8:website	Failed	2/17/2023 18:46:42.9583
company\user1	10.0.0.7:website	Failed	2/16/2023 22:43:24.4484
domain1\system	127.0.0.1:rbac	Successful	2/16/2023 22:41:24.5743

Notifications

Rule Name	Operation
Changes to Privileged Groups	Remove (ValueDelete)
Changes to Privileged Groups	Add (ValueAdd)
Changes to Privileged Groups	Remove (ValueDelete)
Changes to Privileged Groups	Add (ValueAdd)
Changes to Privileged Groups	Remove (ValueDelete)
Changes to Privileged Groups	Add (ValueAdd)
Changes to Privileged Groups	Remove (ValueDelete)
Changes to Privileged Groups	Add (ValueAdd)
Changes to Privileged Groups	Remove (ValueDelete)
Changes to Privileged Groups	Add (ValueAdd)

Role Based Access Control Changes

Changed By	User Added	Access Granted	Persona_Details	Timestamp
DOMAIN1\Alan	:'Simon.Streit'	true	DS Protector Reader	2/21/2023 15:28:04.7632
domain1\gregadmin	Simon.Streit	true	DS Protector Reader Global Report Manager	2/16/2023 22:46:32.1157
domain1\gregadmin	:'Quinton.Almeida'	true	DS Protector Reader	2/16/2023 22:45:51.4876
domain1\gregadmin	:'Jenelle.Bumgarner'	true		2/16/2023 22:45:39.9101

DSP brings Active Directory security data into familiar Splunk views

splunk>

Microsoft Sentinel

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)