semperis

Hybrid identity systems are under attack.

Many organizations are embracing a hybrid cloud journey—deploying the optimal mix of on-premises assets and cloud services for their needs. But with that flexibility comes complexity—especially in managing hybrid identity security in a Microsoft environment.

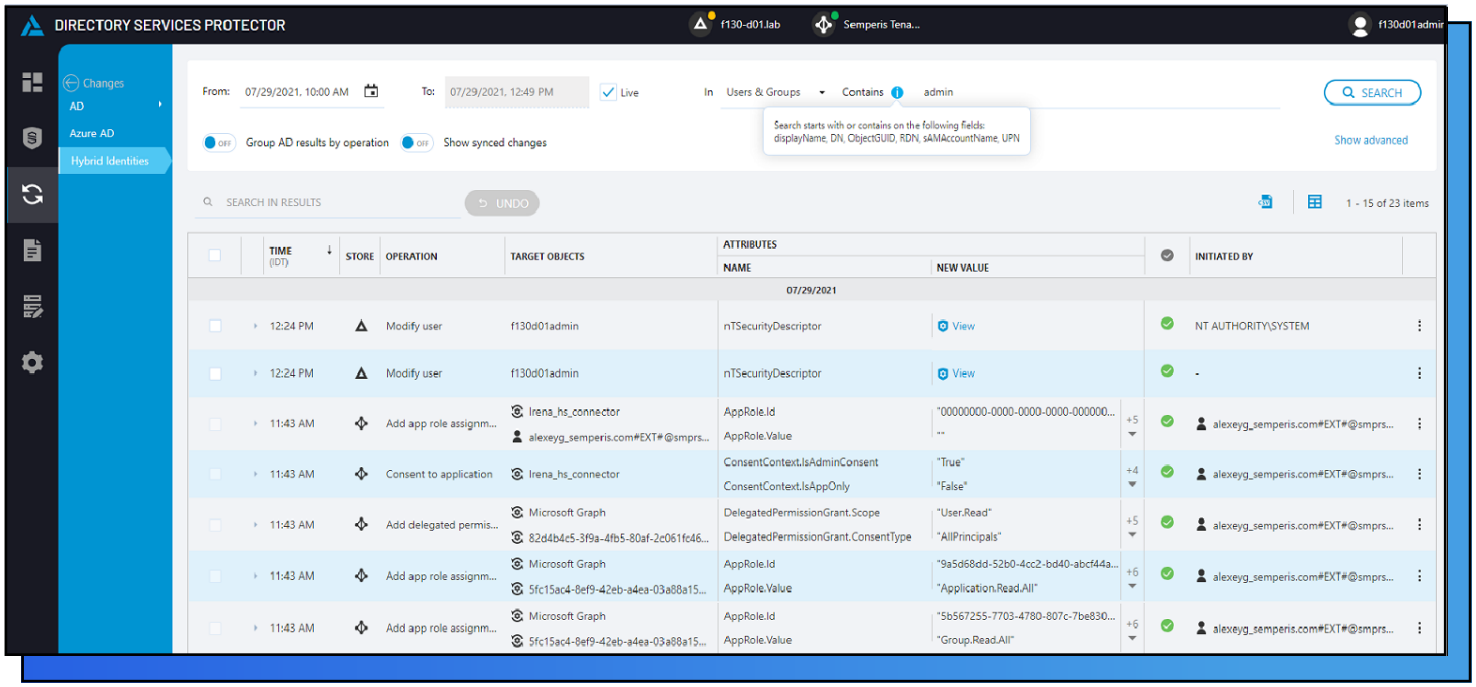
Securing Active Directory requires a different approach from securing Azure Active Directory: The tools, processes, and threats are distinct.

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.

Manage hybrid identity security in one view with Directory Services Protector for Azure Active Directory

- Shows clear view of activities on-premises and in the cloud
- Illustrates actions that begin on-premises but then move to Azure AD—and might indicate underlying security concerns
- Provides powerful search function for time-sensitive forensics



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.

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

info@semperis.com
www.semperis.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

DSP for Azure Active Directory gives a clear view of hybrid identity system security posture.

Hybrid organizations need a complete picture of the risk exposure for their entire environment—Active Directory and Azure Active Directory. DSP for Azure Active Directory provides visibility across the hybrid identity system:

- Displays a single view of indicators of exposure (IOEs) and indicators of compromise (IOCs) in both Active Directory and Azure Active Directory
- Generates a risk profile mapped to appropriate frameworks and regulations for the entire hybrid environment
- Simplifies configuring security settings and remediating malicious changes
- Fully automates and optimizes Active Directory and Azure Active Directory recovery
- Proactively and continually assesses the hybrid AD security stance to combat subsequent attacks
- Complements and enhances existing enterprise security and governance programs

Simplify managing hybrid identity security with Directory Services Protector for Azure Active Directory

"While managing identity in a hybrid environment might seem as simple as joining a Windows device to AAD, failing to account for changes to the risk landscape opens the door to issues that can cause headaches in the future."

- Doug Davis, Senior Product Manager at Semperis