semperis COHESITY

SEMPERIS-COHESITY ATTACK PATH MANAGEMENT

# Discover and close risky attack paths leading to business-critical data

*Semperis-Cohesity attack path management helps you prevent data breaches by uncovering risky access paths leading to critical data stores, closing security gaps to increase overall security posture, and accelerating incident response time*

Data breaches are on the rise, leading to business outages, revenue loss, customer trust, and other damages. Business-critical data is a lucrative target for threat actors who steal sensitive business data as leverage for ransom. The most common path to valuable data stores is through the identity system: 74% of data breaches start with privileged credential abuse. Threat actors exploit vulnerabilities to move laterally through the identity system, escalating privileges until they're capable of encrypting business-critical data assets—making recovery slow and painful, if not impossible.

In a typical organization's identity system, there are countless attack paths an adversary can take to achieve domain dominance and compromise data stores. The problem is clear—excessive privileges. However, sifting through every group and user relationship is an impossible task for defenders, wasting time in remediation and in responding to emerging threats.

## COUNTLESS ATTACK PATHS TO DATA

- Excessive privileges in legacy AD environments create thousands or millions of potential attack paths leading to sensitive business assets
- Undefined Tier 0 perimeter leaves organizations oblivious to potential security gaps

## DIFFICULTY IDENTIFYING HIGH-RISK PATHS

- Attack paths to vulnerable business-critical data often go undiscovered until after the attack occurs
- Common attack paths are often not the most dangerous ones

## LIMITED RESOURCES AND APPROACHES

- Security teams waste valuable time investigating countless attack paths rather than focusing on what matters—the Tier 0 perimeter
- Prioritizing attack paths by commonality rather than severity increases the risk of data breaches

"During a ransomware attack, if the threat actor encrypts the backup and recovery system, the victim organization is much more likely to pay the ransom, as the company finds itself in a position of very limited options. By helping our joint Semperis-Cohesity customers identify and close off attack paths leading to the organizational backup and recovery system, we can prevent data exfiltration and preserve the recovery option, removing one of the primary negotiating tactics threat actors have."

MICKEY BRESMAN
**Semperis CEO**

semperis COHESITY

## Save time in preventing data breaches

Protect your critical business data by locking down excessive privileges, prioritizing high-risk paths to sensitive data, and scanning the identity environment to uncover and close new attack paths.

**74%**

Of data breaches start with privileged credential abuse

**SOURCE**: IBM Data Breach Report

The Semperis-Cohesity attack path management solution:

- Saves time in identifying and closing risky paths leading to sensitive data by helping IT and security teams remove excessive privileges that open doors to adversaries
- Reduces risk of threat actors gaining access to Cohesity storage clusters
- Improves overall security posture by defining secure zones for privileged groups with access to the Cohesity platform
- Accelerates incident response time with on-demand scanning of the AD environment to quickly identify and close attack paths
- Prevents data breaches with manual, periodic scanning to uncover and remediate new attack paths leading to Cohesity storage clusters

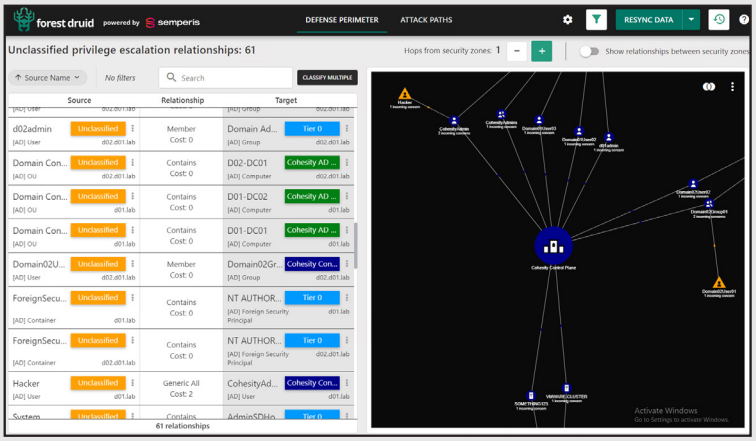
## How it works

Semperis-Cohesity attack path management saves time for cyber defenders by focusing on the attack paths leading to the organization's most sensitive assets—flipping the script on traditional approaches.

1. Scan the environment to create a visual map of accounts with privileged access leading to Cohesity storage clusters
2. Define security zones for designated privileged accounts
3. Remove excessive privileges from accounts
4. Periodically rescan the AD environment to uncover new attack paths that could lead to a data breach

## Ready to close attack paths to your business-critical data?

**LEARN MORE**




**SEMPERIS-COHESITY ATTACK PATH MANAGEMENT** *provides a visual map of risky attack paths leading to Cohesity storage cluster, helping organizations identify and remove risky access*

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

Gartner Peer Insights. Customer First

**Semperis**
IT Resilience Orchestration
**5.0**
Source: Gartner Peer Insights

Leader SPRING 2024

**Semperis**
Directory Services Protector
**4.7**
Source: G2.com

**Semperis Headquarters**
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030