



## SOLUTION BRIEF

# SPHEREboard SecureAD

Enhance visibility, simplify reporting, and mitigate risks across Active Directory.

## The challenge with Active Directory governance

Even the most capable administrators with the highest level of vigilance will admit that consistently updating and organizing Active Directory (AD) is no easy feat. Keeping pace with the dynamic nature of a rapidly evolving organization, including role-changes, lateral and departmental moves, and onboarding/offboarding processes, proves to be a formidable challenge. Mergers, Acquisitions, and Divestitures as well as legacy systems exacerbate this issue.

When Active Directory is subject to a lack of oversight and governance, the dynamic nature of AD creates a sprawl of risk, and companies are unable to effectively identify the issues. Even when issues are found, resolving them is a challenge without clear ownership due to the fear of breaking critical systems in the process. These historical issues become systematic, making Active Directory hard to secure, creating more risk. With AD now the main target for bad actors, addressing these risks is absolutely critical.

## The risks of a mismanaged Active Directory

Active Directory serves as the backbone of IT infrastructures and the foundation of security in many organizations, orchestrating human and computer identity management across networked systems. However, its central role also makes it a prime target for cyber threats.

**\$4.5M**

Average cost of a breach in 2023

**25.6B**

AD & Azure AD attacks every day

**23 Days**

Average downtime from ransomware attack



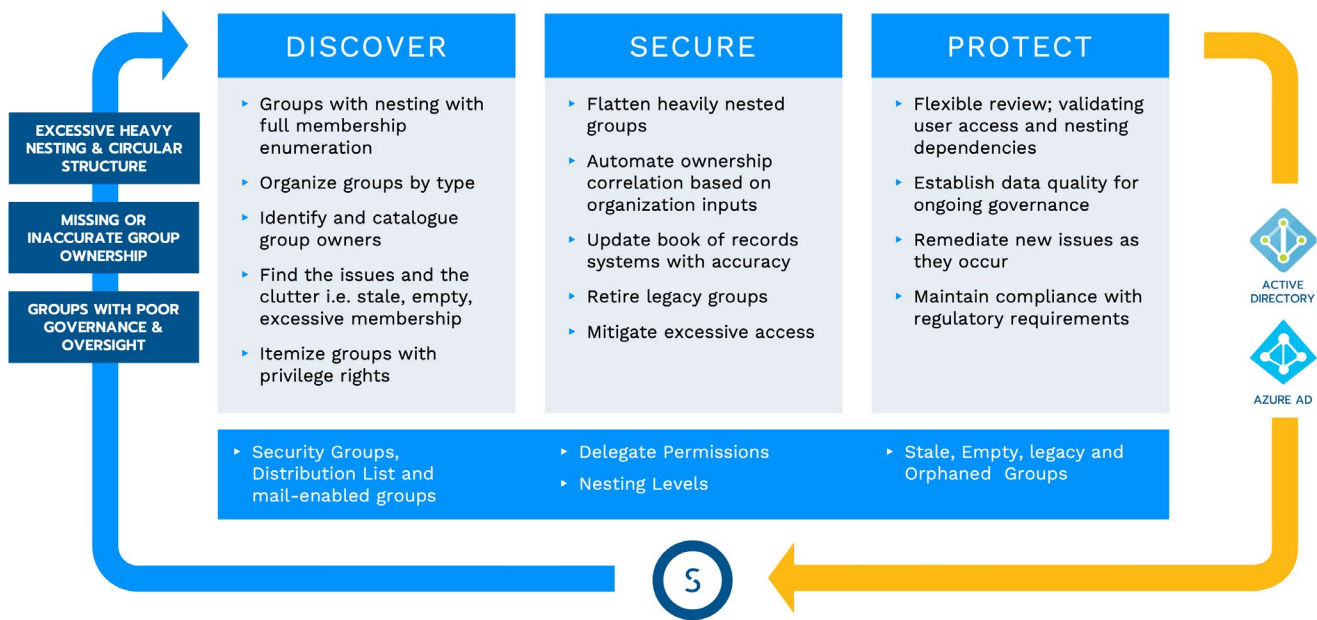
## What kind of problems occur with poor hygiene across Active Directory?

- **Stale & Empty Groups** – A large number of stale or empty groups increase the chances of an attacker finding a path to exploit.
- **Nested and Circular Groups Structure** – Complex nesting obfuscates true membership, creating gaps in visibility of access routes, resulting in mismanaged access controls.
- **Missing Group Ownership** – Missing, incomplete or inaccurate ownership prevents organizations from performing reviews, approving or rejecting changes and remediating risk.
- **Unknown Delegate Permissions** – Without visibility to delegate access, an excessive number of accounts can assign elevated rights to non-administrative users or groups.
- **Hidden and Buried Privileged Access** – Highly privileged accounts inadvertently added to heavily nested groups are underreported and can be used to exploit a company’s most critical assets.

## Introducing SPHEREboard SecureAD

SPHEREboard SecureAD is a turnkey solution that enhances discovery, analysis, and automation of risk reduction across your Active Directory. Its agentless architecture quickly and comprehensively enumerates your full AD environment, across all domains, both on prem and in Azure.

Additionally, SPHEREboard’s Asset Review Module (ARM) enables flexible workflows to identify, interact with and confirm designated owners and lines of business, a critical step to remediate the issues without causing business disruption. Finally, SPHEREboard’s Virtual Worker (VW) capabilities automate the execution of the remediation workflow and many of steps needed to reduce the attack surface.



## Continuous Hygiene with SPHEREboard SecureAD

## How does SPHEREboard SecureAD address Active Directory issues?



### Step 1: Intelligent Discovery

SPHEREboard SecureAD leverages intelligent connectors to quickly and completely extract data from various sources. Regardless of the scale or complexity of your environment, it meticulously aggregates the data, delivering a comprehensive inventory of all Active Directory objects, fully enumerating group membership.



### Step 2: Analysis and Reporting

Knowing and being able to identify the risk and path to remediation is often more valuable than the end state. SPHEREboard SecureAD quickly provides a comprehensive overview of the risks and their potential impact on an organization. Additional reports outlining the most egregious issues, as well as low-impact, high-value remediation options, provide immediate time-to-value.



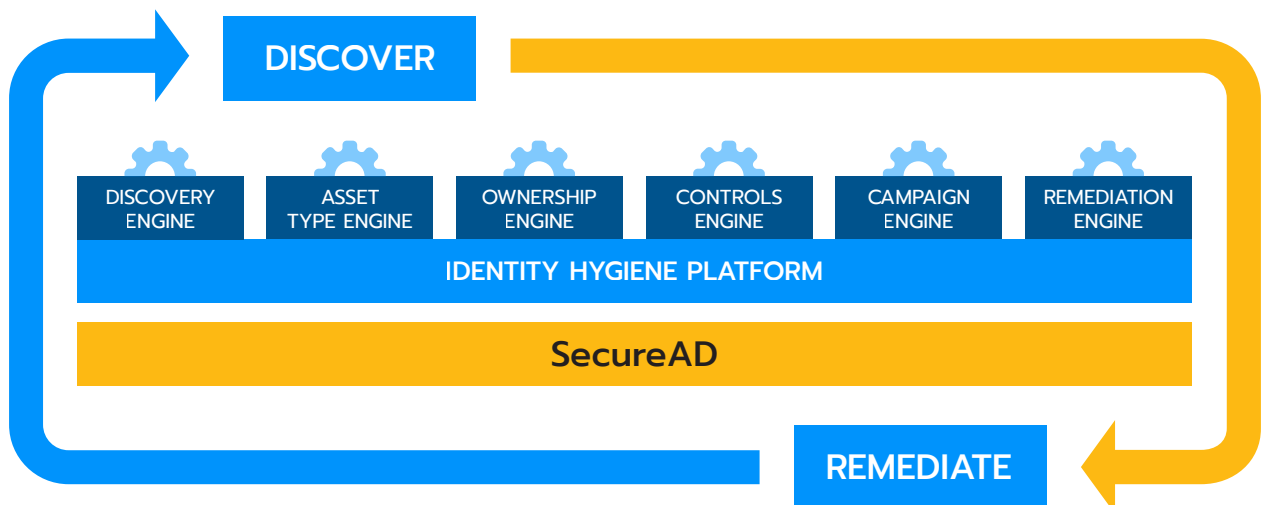
### Step 3: Risk Reduction and Remediation

SPHEREboard SecureAD identifies and validates ownership, allowing for corrective measures to address problematic groups, minimize access, and promote standardized access controls. Its intuitive ability to communicate with owners and automate the remediation process, requirements such as flattening group structures or updating key group properties, can be achieved with uninterrupted access to required systems.



### Step 4: Sustain Results with Ongoing Hygiene

SPHEREboard SecureAD is designed to protect you from these recurring issues in addition to the discovery and remediation of existing risk. SPHEREboard Hygiene Hub provides consistent reporting of metrics with a continuous view of risk and its potential impact. This allows companies to report on status with confidence, knowing that Active Directory is secure. SPHEREboard continuously identifies, prioritizes, and remediates violations to critical Controls, creating a perpetual state of order, with strong hygiene.



## Continuous Hygiene Platform

## Benefits of adding SPHEREboard SecureAD to your Active Directory Strategy



### Comprehensive and continuous risk insights

Change starts with knowledge. SPHEREboard SecureAD provides a clear picture of your Active Directory environment, account-group relationships, and all associated risks. With this knowledge at your fingertips, you can manage your environment more efficiently and reduce risk.



### Time and cost savings

Effectively discovering, managing, and remediating Active Directory risk usually demands a team of skilled professionals and involves hundreds, if not thousands, of hours of continuous manual effort. SPHEREboard SecureAD automates these tasks, handling everything from confirming ownership and usage through automated campaigns to implementing membership changes. This not only alleviates administrative workload but also saves your organization valuable time and resources.



### Actionable intelligence

SPHEREboard's algorithms and machine learning provide intelligence-driven insights into the security posture of your users and groups. By enabling you to identify specific risks in your environment, SPHEREboard SecureAD empowers you to quickly remediate without ever interrupting the access users need to continue working efficiently.



### Sustainable risk reduction

Once your Active Directory environment is optimized, SPHEREboard's sustainability processes ensure that controls and policies are met on an ongoing basis. Conduct security assessments on-demand, monitor over time, identify emerging security risks, and address them proactively before internal or external auditors become involved.

## LEARN MORE

Protect your privileged accounts and reduce Active Directory risk by making SPHEREboard SecureAD part of your risk-reduction strategy. To learn more about SPHEREboard or other SPHERE solutions, please visit [www.sphereco.com](http://www.sphereco.com)

## SPHEREboard Case Study

› Financial Services

› 40K Employees

› 360K AD Groups

### Security Risks

- › Unclassified Active Directory Groups
- › AD privileged groups are not reviewed periodically for access appropriateness
- › Changes to privileged AD groups and associated permissions not monitored
- › Empty and Stale groups are not governed accordingly with organization security standards

### TIME-TO-VALUE OUTCOMES

Intelligent Discovery deployed and identified full extent of exposures and scope of effort to correct in less than 30 days.

Risk reduction activities were initiated within 2 weeks, focused on mitigating internal audit findings.

Sustainability achieved; ensuring Least Privileged Access and adoption of a mature Target Operating Model

LINE OF BUSINESS	TOTAL	ORPHANED OWNERSHIP 21%	EMPTY 31%	STALE (3+YEARS) 19%	HEAVILY NESTED 7%	EXCESSIVE MEMBERSHIP 3%	CIRCULAR MEMBERSHIP 1%	DELEGATE GROUPS 1%
Back Office	234,320	28,550	63,630	32,330	5,490	8,390	2,610	25
Equities	39,610	4,560	11,210	3,460	270	310	1,550	150
Marketing	4,100	3,470	1,750	310	10	0	10	5
Trading	150	80	20	0	0	0	1,050	0
Compliance	990	450	480	10	0	10	50	350
Finance	1,070	340	450	0	0	0	20	540
DevOps	80,620	38,640	35,090	33,160	19,500	3,020	790	2,430
<b>Grand Total</b>	<b>360,860</b>	<b>76,090</b>	<b>112,630</b>	<b>69,830</b>	<b>25,270</b>	<b>11,720</b>	<b>5,135</b>	<b>3,500</b>

Powered by SPHEREboard



## Bringing Identity Hygiene to Active Directory

Active Directory is the core identity system for almost every organization, making it a prime target for threat actors in most of DoS and ransomware attacks. Time, organizational changes, and complexity only make it harder to find more of the exposure points threat actors exploit. To address these challenges, SPHERE developed SPHEREboard SecureAD. A purpose-built solution designed to provide organizations with discovery, reporting, and automated remediation work flows to reduce risks across both Active Directory and Azure AD.

### About SPHERE

SPHERE is the global leader in Identity Hygiene. We are dedicated to reshaping modern identity programs by embedding this foundational fabric, enabling organizations to quickly reduce risks. Our expertise lies in leveraging automation to deliver immediate time-to-value. We work through an identity lens that protects an organization's accounts, data, and infrastructure.

Driven by our core values of passion, empathy, and authenticity, our vision drives us to continually innovate. We're ready to help you address your Identity Hygiene and security challenges.

We're ready to help you address your identity hygiene and security challenges. To find out more about SPHERE and our solutions, please visit [www.sphereco.com](http://www.sphereco.com).

