SPHERE

SOLUTION BRIEF

# Addressing New M365 Cloud and Directory Challenges

Much of the business world runs on the Microsoft 365 (M365) suite. Apps like SharePoint, OneDrive and Teams revolutionized the way we work and became commonplace in our modern business environments. Then came the Covid-accelerated “digital transformation”, when most organizations were forced to quickly pivot from on-premises operations to the cloud in a matter of days, further increasing the global use of M365, and cloud platforms in general.

As M365 continues its successful rise, news like the release of Microsoft Copilot promise to further extend productivity capabilities through artificial intelligence and machine learning. Each fresh announcement and new capability present uncharted challenges for security teams wishing to manage their identity perimeters and secure their cloud environments.

At SPHERE, we help organizations get their identity and access issues under control. We call this Identity Hygiene, a holistic approach to securing identity and access. Our SPHEREboard platform integrates with M365 to help you identify and mitigate security gaps proactively, no matter how your teams are distributed.

## The Challenges

### Cloud Collaboration: A Double-Edged Sword for Security Professionals

The strength of the M365 suite lies in how it drives productivity, consolidating and sharing massive amounts of organizational data across apps. However, this strength also creates security challenges. All that shared data is a prime target for bad actors using credential theft to gain access to potentially sensitive data. It is no secret that account compromise and related data breaches have become a growing issue, with M365 being one of the most exploited systems worldwide.

From an identity standpoint, M365 presents some issues security practitioners should consider:

- Microsoft made it very easy to share individual documents across M365, which essentially creates document-specific entitlements. This produces exponential entitlement sprawl, making reviewing and managing access across an entire organization challenging with historical governance solution

  **When data can be shared to nearly any internal or external party, whether by design or by accident, the potential of data breach naturally increases.**

- Privileged access across M365 environments is important to monitor, with privileged escalation top-of-mind for vulnerability management teams. Often, identities have excessive privileges, or admin access is given to those who simply do not need it.

  **If an attacker gains access to these credentials, they can often access and exfiltrate sensitive data, or worse yet, cause harm to the systems themselves taking advantage of these compromised credentials.**

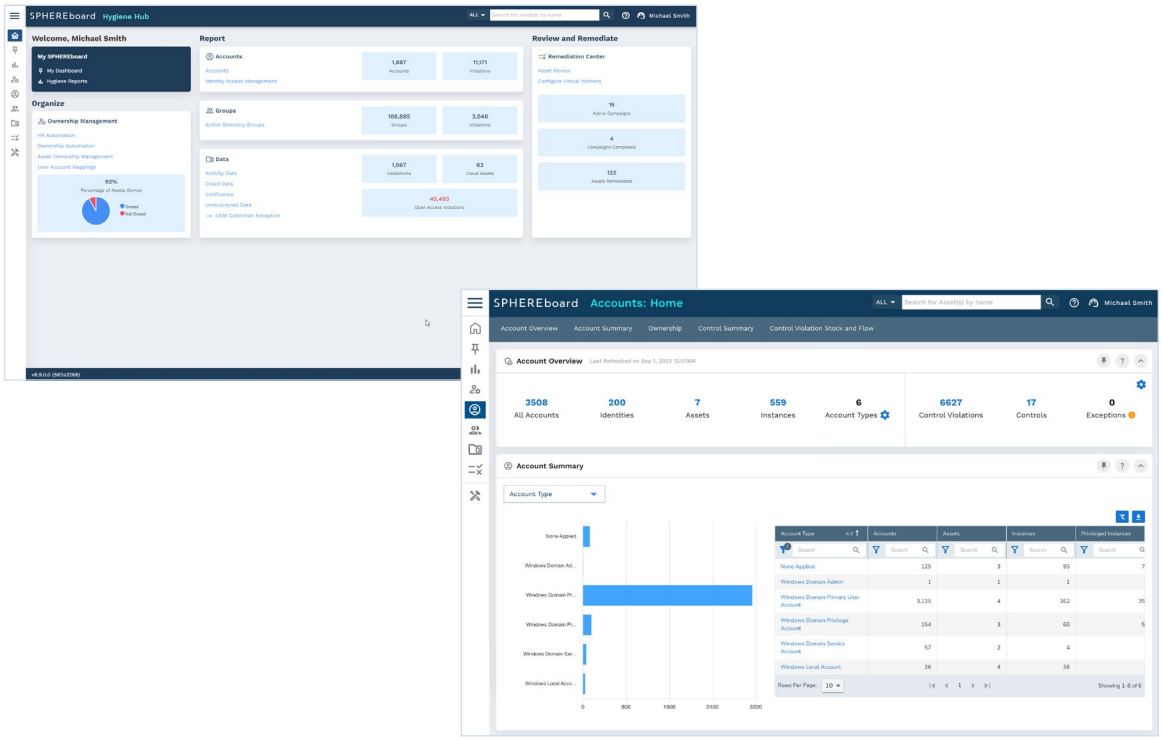
 

## The Solution

SPHEREboard has automated the key requirements that drive Identity Hygiene for modern enterprise environments. We know it's best not to hinder a company's ability to be productive and competitive, and instead to layer security solutions to provide the necessary protections.

By providing an identity lens to the data problem, SPHEREboard uniquely hones in on these requirements:

- **Discovery is the focus**. Given the complexity of your M365 systems and the associated end-user and privileged access, you need to gain deep visibility into the environment.
- **Remediate the issues**. Make sure you can fix the issues you find without negatively impacting the ability of your business to continue to operate and generate revenue.
- **Sustain the process**. Stem the flow of new issues, as you resolve the stock of issues found, making sure your M365 environment has proper hygiene policies that are enforced with the necessary controls.
- **Don't forget about Active Directory and Azure**. These systems control your accounts, passwords and how permissions are applied through groups.
  - Security groups (including mail-enabled security groups) and distribution lists should be incorporated into the remediation approach, as they group users and are often the root cause of overly permissive access and information being shared with the wrong parties.
  - Focusing on AD expands the risk-reduction approach to not just M365, but any cloud or on-prem application that leverages AD!
- **Bottom line: organizations must enforce a Least Privilege Access model**. The ultimate goal is to limit admin privileges while focusing on the data and minimizing the accounts that have access.



## Automate the Process with SPHEREboard.

Managing a least privilege access program at a large organization is a huge undertaking. The time and resources required just to make a small dent is significant. This is why we developed our SPHEREboard platform to automate this process.

SPHEREboard can drastically increase the velocity of your ongoing discovery and remediation efforts:

### Discover:

Gain visibility over your M365 environment.

- **Know your inventory**. Continuously scan and report on what exists across the environment. Find the at-risk assets and their entitlements across your M365 instance, including SharePoint sites, OneDrive details, and even Teams channels.
- **Identify ownership**. Identify and catalogue who is the authoritative source for making critical decisions around what exists and who should have access. In addition to providing a chain of accountability, ownership enables issues to be addressed and changes to be made while keeping business disruption at a minimum.
- **Visualize security issues**. Get a holistic view of your entire environment to immediately understand both broad-stroke issues, such as wide-open access to SharePoint sites, and granular concerns, like pinpointing instances where document sharing is creating toxic combinations.

### Remediate:

Address the risk you find in real time.

- **Declutter the mess**. Identify and retire stale data and orphaned accounts from production systems.
- **Secure privileged accounts**. Protect important administrative account needs while still defending these highly privileged accounts by onboarding credentials into an organization's vaulting solution with effective password rotations.
- **Remove excessive access**. Based on where open, excessive, and non-standard access exist, campaign with owners, gain approval to limit access, and remediate without fear of business disruption.

### Sustain:

Maintain an ongoing evergreen state.

- **Conduct routine access reviews**. Improve M365 entitlement reviews by ensuring you are contacting the right owner and presenting accurate and complete permission sets in a simple way. This will increase response rates and reduce risk more broadly.
- **Monitor controls and react to violations**. Automate the business rules that define your M365 controls and highlight the violations of these controls for immediate resolution.
- **Ongoing M365 Identity Hygiene**. Now that you have automated the identity and access process, your team can reallocate resources to other tasks!

## 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. We work through an identity lens that protects an organization's accounts, data, and infrastructure. Our solutions deliver immediate time-to-value by leveraging automation to discover, remediate and secure identities, now and forever.

Driven by our core values of passion, empathy, and authenticity, our vision drives us to continually innovate, helping our clients to sleep better knowing their attack surface is drastically reduced, thwarting the plans of bad actors every single day.

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.

SPHERE