AN INTERVIEW WITH RITA GUREVICH, CEO AND FOUNDER, SPHERE

REDEFINING ENTERPRISE IDENTITY SECURITY

As identity-related breaches continue to plague enterprises—impacting 84% of organizations—traditional access management solutions are no longer sufficient. We recently spoke with SPHERE, a company redefining Identity Hygiene with its SPHEREboard platform. Leveraging AI, deep integration capabilities, and a risk-based approach to ownership, SPHEREboard provides a comprehensive solution beyond account discovery. We explored how SPHERE is helping organizations secure Active Directory, close privileged access gaps, and stay ahead of threats through smarter partnerships and context-driven identity intelligence.

TAG: How does SPHERE's SPHEREboard platform automate identifying and remediating identity-related risks to enhance overall identity hygiene within an organization?

SPHERE: We discover all accounts and their entitlements—but at SPHERE, we know that accounts are not identities. That distinction is critical for true Identity Hygiene. It's not enough to just see the accounts—you need to know who the humans are behind them. Who owns them? Ownership is at the core of what we do because it's one of our customers' biggest challenges. That's why we've developed powerful AI-driven features that can identify the most likely owner for every account—from straightforward cases like the BSMITH account that belongs to Barbara Smith (not Bob) to the much harder-to-trace ones like obscure local Oracle service accounts named svc_123.

TAG: With the recent enhancements in SPHEREboard 6.10.5, how do the new features improve integrations and privileged access management for enterprises?

SPHERE: We call ourselves the industry leaders in Identity Hygiene. These new features demonstrate our maturity and continued innovation. With Network Devices, for example, we're addressing an area that's often overlooked or deprioritized—yet privileged access to firewalls, switches, and routers can lead to significant outages or security breaches. Another example is our IGA Data Catalogue. We recognize that one-way integrations are no longer sufficient in a modern identity ecosystem. Identity Hygiene

We map complex nested groups, identify hidden access paths, and highlight toxic combinations that can lead to privilege escalation or policy violations.

and SPHEREboard aren't about operating a single product—they represent a holistic solution designed to give our customers complete visibility, control, and accountability across their identity landscape. It's about building a more secure environment with Identity at the Center.

TAG: Can you elaborate on SPHERE's approach to managing Active Directory (AD) hygiene and its importance in preventing security vulnerabilities?

SPHERE: Active Directory account sprawl, mismanaged groups, and stale accounts are problems almost every customer we work with reports. What sets SPHERE apart is how we approach AD—not just as a directory service but as a critical intersection of infrastructure and security. Our deep understanding of AD's inner workings allows us to go beyond surface-level cleanup.

We map complex nested groups, identify hidden access paths, and highlight toxic combinations that can lead to privilege escalation or policy violations. More importantly, we tie it all back to ownership, risk, and relevance—helping our customers focus not just on what exists in AD but what matters. Whether tightening access to sensitive systems, enforcing least privilege, or integrating AD more intelligently into broader IGA and PAM strategies, we treat Active Directory as the backbone of enterprise identity and help secure it like one.

TAG: Given SPHERE's partnerships with technology providers like CyberArk and BigID, how do these collaborations enhance your identity hygiene solutions?

SPHERE: It's all about the ecosystem. At the heart of SPHEREboard is integration—because the product simply can't operate in a silo. We rely on source data to drive analysis and take action, and that means integrations aren't just features—they're foundational.

These integrations can range from straightforward connections using public APIs to deeply embedded partnerships, like our one with CyberArk. With CyberArk, it's not just a technical handshake—it's a strategic alliance. Our teams work closely on both the business and technology side to ensure that our shared customers get more than the sum of two platforms.

Together, we accelerate PAM programs by surfacing the right data at the right time, enriching the context around privileged accounts, and identifying ownership gaps or policy violations before they become incidents. SPHEREboard helps organizations move faster—from initial discovery to meaningful risk reduction—and we keep that momentum by enabling continuous monitoring, adaptive policy enforcement, and actionable insights. It's not just about getting "done"—it's about staying ahead of risk.

TAG: Since 84% of organizations have experienced an identity-related breach, how does SPHEREboard go beyond traditional access management to proactively reduce risk and prevent future incidents?

SPHERE: We go beyond traditional access management by recognizing that access alone is just raw data—until it's enriched with deeper context. Knowing what an account can do is only part of the picture. To drive meaningful action, you need to layer in all the collected and derived intelligence: who owns the account, how the access was granted, whether it's still required, and what level of privilege it represents.

At SPHERE, we put this data through the lens of identity, ownership, and risk. We correlate access to real human identities and evaluate whether those entitlements make sense in context, including business function, peer access, and vaulting status. That's how we move from insight to action, helping organizations understand their exposure quickly and continuously reduce it.