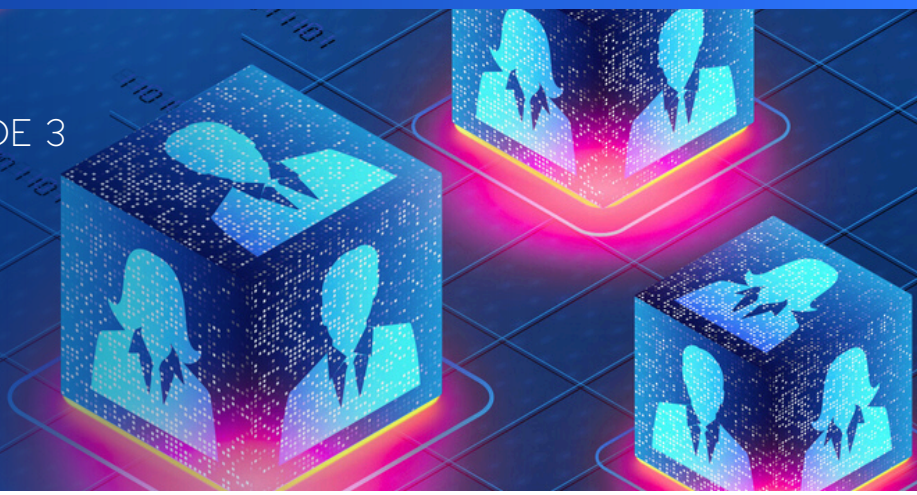
A GATHID LABS SERIES: EPISODE 3

Gathid: Bringing Simplicity to AD Complexity



Unifying Active Directory Identity Governance Across On-Prem and Cloud

As businesses race toward digital transformation, hybrid identity environments have become the standard. Many organizations continue to rely on on-premises Active Directory (AD) for managing user access, while also leveraging cloud identity providers like one or more Entra ID and/or Okta (and/or other) instances. This hybrid approach brings fresh challenges for IT teams, who must balance security and compliance across multiple identity platforms.

This article dives into the world of hybrid identity governance, the complexity of fragmented access management, and how organizations can leverage better visibility and actionable insights between on-prem and cloud IDP architecture with the help of Gathid.

The Challenge of Hybrid Identity Environments

When AD was first implemented, cloud computing was still a gleam in the IT world's eye. Back then, on-premises IT ecosystems had controlled network perimeters and clearly defined authentication pathways.

Fast-forward to today, and organizations are embracing cloud-first strategies with SaaS applications, cloud-based infrastructure, and remote work policies. This shift has led to a hybrid identity environment, where AD and cloud platforms work together—sometimes smoothly, but often not without a few bumps.

This hybrid environment brings several challenges for IT and security teams:

- **Inconsistent Security Policies**: Without a unified strategy, different security standards may govern on-prem and cloud-based identities, opening up potential enforcement gaps.
- **Weak Authentication Mechanisms**: Legacy AD authentication struggles to support modern security features, like passwordless authentication or adaptive MFA, leaving organizations exposed.
- **Difficulty Tracking User Activity**: With identities spread across platforms, it's a struggle to get full visibility on who has access to what, and what they're actually doing with it.

The Risks of Poorly Managed Hybrid Identity Governance

At the rate of growth that we have experienced over the past few decades, fragmented systems and accounts without context to the human identities that are accountable for them, can lead to serious security and compliance risks. Cybercriminals love to exploit inconsistencies in identity security between on-prem and cloud environments to sneak into systems undetected. Here are some common risks:

- **Stale (Dormant) Accounts**: If AD and cloud identity providers aren't properly synced, deprovisioning can fail, leaving old accounts with lingering access to sensitive systems .
- **Unowned and Orphaned Accounts**: Enabled accounts unable to be mapped, managed or reviewed with context from HR (and other people information management systems) ownership with whom they exist pose significant insider threat risk.
- **Privilege Creep Across Platforms**: Without centralized oversight, users accumulate excessive permissions as they move through roles or projects. This creates a broad attack surface that bad actors can exploit.
- **Compliance Failures**: Regulations like GDPR, HIPAA, and SOX require strict identity controls and audit trails. A disconnected approach to identity governance increases the likelihood of audit failures, costly fines, and damage to your organization's reputation.

The fallout from a fragmented identity strategy goes beyond security breaches—it also creates operational inefficiencies. IT teams waste valuable time reconciling access, investigating inconsistencies, and scrambling to fix compliance issues that could have been avoided.

How Gathid Bridges the On-Prem and Cloud Identity Gap

Organizations need a solution that connects the dots between on-prem AD and cloud identity systems. Enter Gathid—the smart, automated way to unify identity governance, ensuring security, compliance, and streamlined operations.

Here's how Gathid works its magic:

- **Visibility Across Identity Environments**: Security teams can gain a clear view of all user identities, permissions, and activity across AD, Entra ID, and other cloud identity platforms—no more guessing!
- **User Lifecycle Management**: Gathid offers IT teams visibility across user accounts and groups across applications, eliminating orphaned accounts and reducing manual work.

- **Zero-Trust Enforcement**: By standardizing access policies and continuously validating trust levels, Gathid helps develop and deliver a context driven least-privilege model in your hybrid environment, keeping access to the essentials.
- **Continuous Risk Monitoring**: Gathid detects and flags identity and access risks every day—including privilege escalation, policy violations, and dormant account notifications—so you can stay ahead of potential threats.

With Gathid, organizations can integrate AD with cloud identity providers, centralizing visibility over identity and access governance while minimizing risks and simplifying management.

Conclusion

The shift to hybrid IT environments may be a challenge, but it's also an opportunity to rethink identity governance. Treating on-prem AD and cloud identities as separate systems leads to security gaps, operational hiccups, and compliance headaches. But with a modern identity governance framework powered by Gathid, businesses can eliminate these divides, ensuring secure, efficient, and compliant access management.

By adopting a proactive, unified approach to identity governance, organizations can future-proof their security strategy, enabling the agility and security needed to thrive in an increasingly cloud-centric world.

Schedule a Demo | Learn More | Read Online