StackIdentity

Breaking the Cycle of Poor Identity Governance – How to Escape the Legacy Trap with Real-Time, AI-Driven Access Management

WHITE PAPER

Introduction: The Dissonance Between Spending and Outcome

Enterprises spend millions on identity governance solutions from industry leaders like SailPoint, Saviynt, and Microsoft. Yet, despite this investment, many have amassed massive identity attack surfaces due to poor governance practices. This dissonance between spending and outcome is a byproduct of identity governance gaps that plague many organizations. Microsoft environments—such as Active Directory (AD), Entra ID, Azure subscriptions, and Microsoft SQL Server—primely illustrate how these governance gaps have become a breeding ground for identity attacks and ransomware campaigns.

As identity-based attacks continue to rise, the need for real-time governance powered by AI and automation has never been more urgent. Attackers aren't waiting for quarterly audits, and enterprises can no longer afford to rely on outdated governance approaches.

The Problem: The "Hydra" of Identity Governance

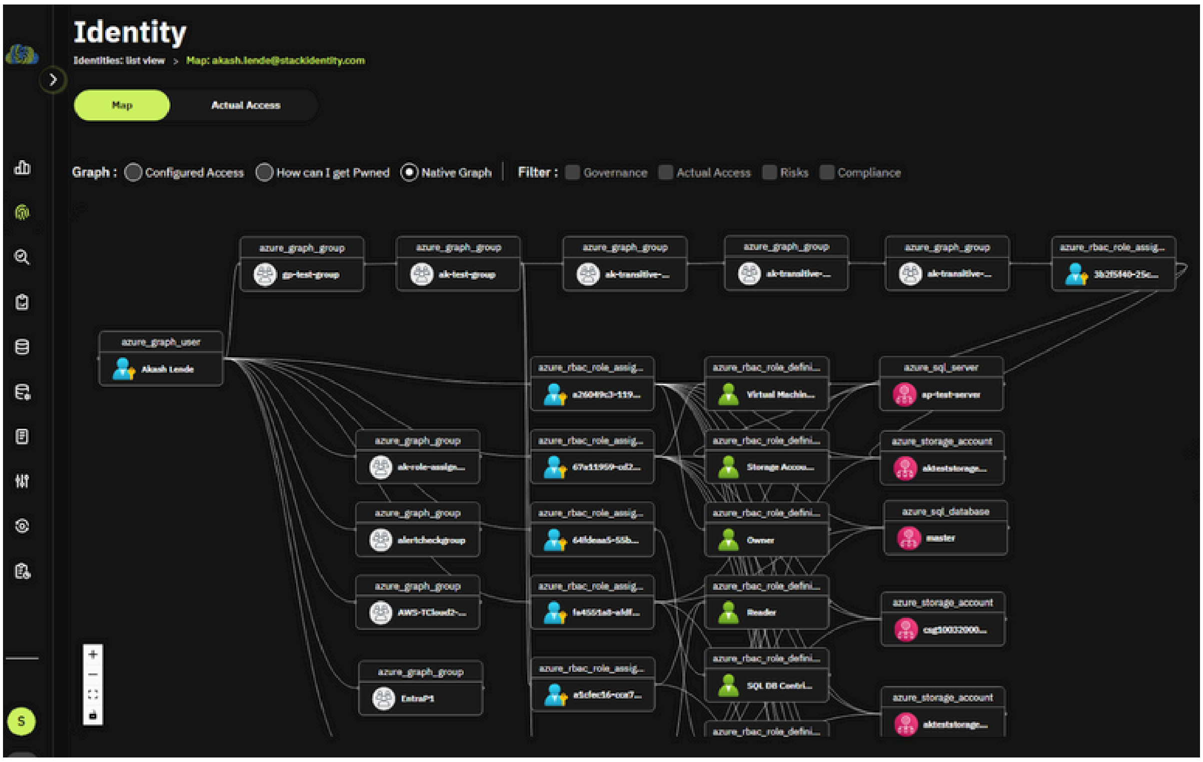
In today’s enterprise, identity governance is akin to taming a five-headed hydra—particularly in environments built around Microsoft technologies. The complex web of groups, sub-groups, nested groups, roles, and policies has spiraled out of control, creating numerous attack vectors for adversaries to exploit.

A Focus on Microsoft Environments

- Active Directory and Entra ID: Legacy constructs like groups and roles have accumulated for years, remaining untouched out of fear of disrupting business processes. AD sync with Entra ID propagates this complexity, making governance more challenging.
- Azure Subscriptions & Microsoft SQL Servers: Permissions management in cloud and hybrid environments introduces nested permissions that create significant blind spots for security teams.
- Microsoft BI & Other Platforms: Previously locked-down data systems are now opened to new AI-powered applications, complicating identity governance.

The Hydra Monster

- Groups, Sub-Groups, Nested Groups, Roles, and Policies: Unraveling the permissions web within Microsoft ecosystems is time-consuming, complex, and error-prone.
- Stakeholder Dissatisfaction: Business teams, managers, IT security, and auditors are dissatisfied with the inefficiencies and risks generated by legacy governance models.
- Generative AI as a New Attack Surface: As enterprises adopt generative AI, previously secured data is exposed to these models, multiplying identity-based attack vectors.



Identity

Identities: list view > Map: akash.lende@stackidentity.com

Map | Actual Access

Graph : ○ Configured Access ○ How can I get Pwned ● Native Graph | Filter : □ Governance □ Actual Access □ Risks □ Compliance

Hydra of Identity Governance in Microsoft Environments

The "As Is" Situation: The State of Identity Governance

Despite substantial investment, enterprises face ongoing challenges with identity governance:

Complexity Overload: Managing interrelationships between groups, sub-groups, nested groups, roles, and permissions in Microsoft environments has become an enormous challenge. Administrators are afraid to remove old permissions, resulting in "permission hoarding."

Rubber Stamp Governance: Opaque permissions lead to a governance system driven by compliance, not security. Managers approve access they don't fully understand, perpetuating access risk.

Attack Surface Expansion: Every legacy group or permission adds a new attack surface for bad actors, enabling ransomware attacks and unauthorized access.

Worsening Over Time: The problem is getting worse as permission sprawl continues to grow, compounding security risks year-over-year.

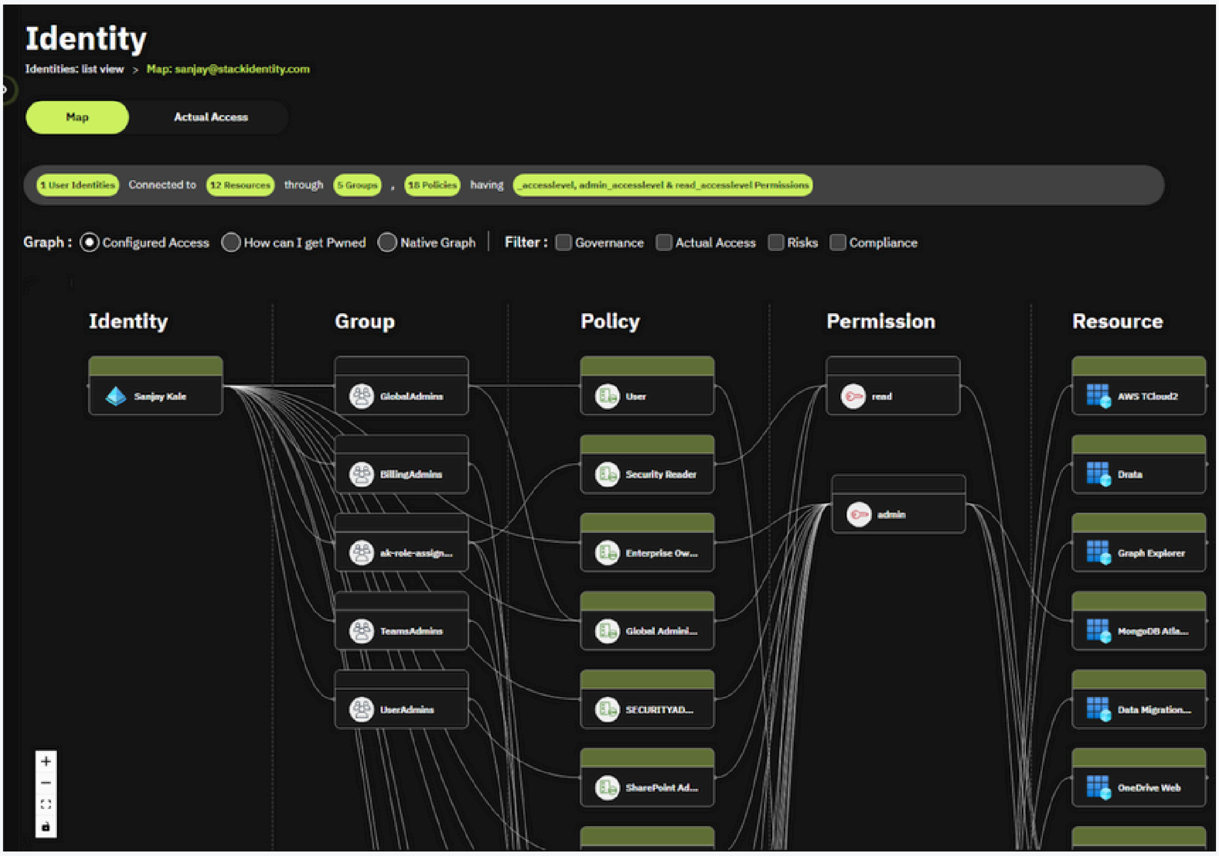
The "To Be" Situation: The Case for Real-Time Access Management

Enterprises must transition from manual, quarterly audits to real-time, AI-driven access management, where risks are automatically identified and remediated.

1. You Cannot Govern What You Cannot See: Gain Deep Contextual Visibility

- AI-Driven Authorization Graphs: Unravel the complexity of identity systems with Stack Identity's Authorization Graph. This tool visualizes relationships between identities, groups, sub-groups, roles, and permissions.

- Contextual Questions:
  - Who has access to what?
  - How is access being granted?
  - What actions can someone take with their access?
  - Is the access being used and is it truly necessary?
  - What will the impact of removing this access?



Identity

Identities: list view > Map: sanjay@stackidentity.com

1 User Identities Connected to 12 Resources through 5 Groups , 18 Policies having _accesslevel, admin_accesslevel & read_accesslevel Permissions

Graph : ● Configured Access ○ How can I get Pwned ○ Native Graph | Filter : □ Governance □ Actual Access □ Risks □ Compliance

AI-Driven Authorization Graph from Stack Identity

2. Transform Context into Action: Real-Time Risk Reduction

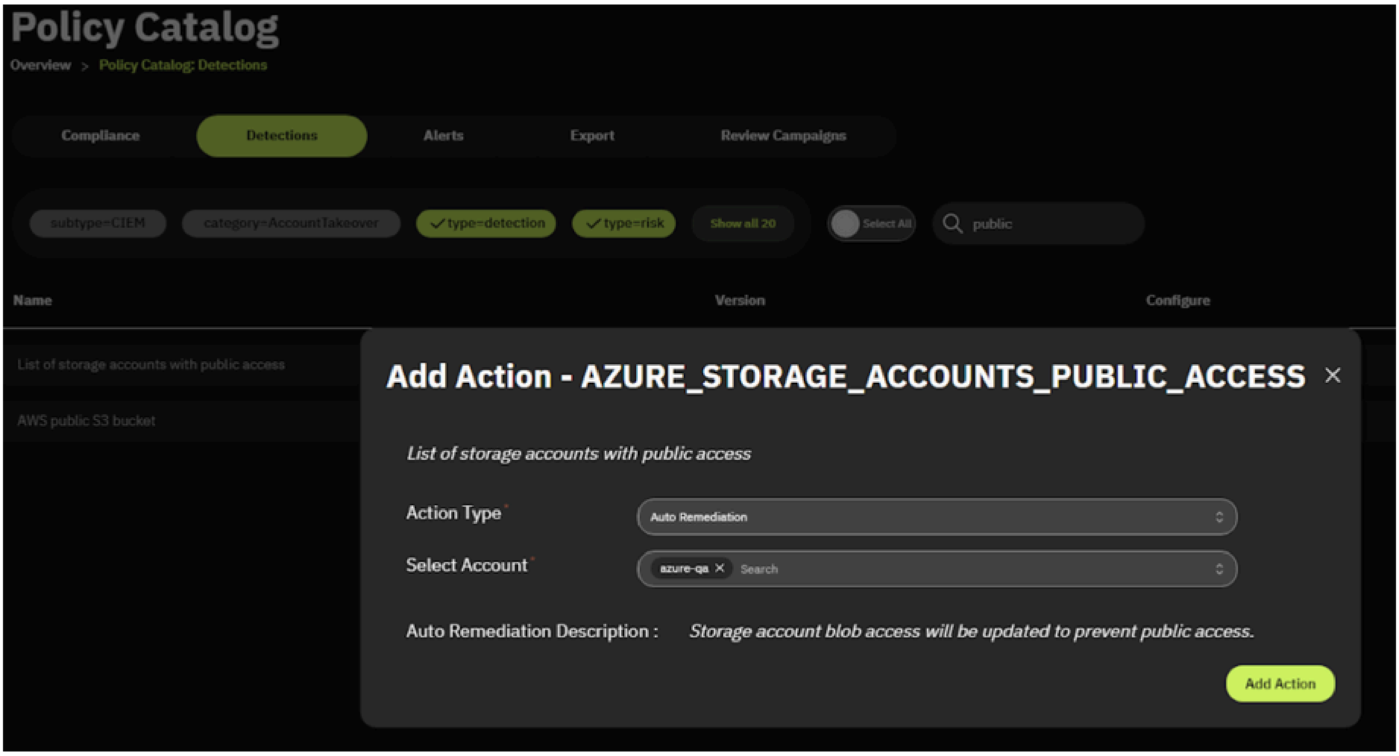
- Eliminate Permission Debt: Identify and remove dormant, orphaned, and excessive permissions in real time.
- Tackle Nested Groups and Sub-Groups: Use AI to uncover hidden hierarchies and streamline group management.
- Move to Just-In-Time (JIT) Access: Replace "standing access" with JIT and Just Enough Access (JEA) policies.

3. Automate for Continuous Security: Let AI Do the Heavy Lifting

In many enterprises, identity governance actions trigger manual intervention, resulting in a flood of Jira or ServiceNow tickets, which only adds to a growing backlog. These tickets demand human attention, further slowing down the governance process and drowning teams in repetitive tasks, while risk accumulates.

With Stack Identity's AI-driven governance, enterprises can eliminate the need for manual intervention. Deep contextual understanding allows for automated remediation, meaning risks are not just identified but immediately resolved without creating another ticket.

- AI-Powered Continuous Access Reviews: Automate risk-based actions by leveraging AI to review access continuously. AI can assess and automatically remediate access risks based on policies and risk scores.
- Automated Self-Service: Empower end-users with self-service workflows. AI can make real-time decisions about access requests, freeing IT teams from unnecessary ticket triage.
- Automated Risk Remediation: Context from Stack Identity ensures that remediation actions—like removing dormant or excessive permissions—are executed automatically without impacting business processes.



Name	Version	Configure
List of storage accounts with public access		
AWS public S3 bucket		

Add Action - AZURE_STORAGE_ACCOUNTS_PUBLIC_ACCESS ×

List of storage accounts with public access

Action Type*: Auto Remediation

Select Account*: azure-qa ×

Auto Remediation Description : *Storage account blob access will be updated to prevent public access.*

Automated Risk Remediation Flow with Stack Identity

How to Get Started in Microsoft Environments

1. **Build the Access Baseline**: Gather data on access and permission usage to create a comprehensive view of current access risks. Use tools like Stack Identity's Authorization Graph to visualize and understand permission structures.

2. **Target Dynamic, Over-Permissioned Environments**: Focus on high-risk areas such as cloud environments, privileged access, and hybrid infrastructures where permission sprawl is rampant.

3. **Implement Just-In-Time (JIT) and Just Enough Access (JEA)**: Transition from standing access to JIT policies, ensuring users only have access when needed.

4. **Automate for Scale**: Deploy AI and automation to handle routine access requests and continuous reviews, eliminating the need for manual intervention.

Conclusion: The Time for Real-Time Governance is Now

Identity governance in Microsoft environments is fundamentally broken. Enterprises have spent millions on legacy IGA products that fail to address the complexity and scale of modern access management challenges. Meanwhile, their attack surfaces grow larger every day.

Don't spend money on legacy IGA products. Instead, demand real-time, AI-driven access management that gives you the visibility and control you need to secure your enterprise.

With Stack Identity, you can:

- Eliminate permission debt
- Automate risk remediation
- Implement Just-In-Time access
- Stop drowning in tickets and backlogs

Take action today. Talk to Stack Identity to arrange an Identity Hygiene Risk Assessment for your Microsoft environment.