Innovation Alert: The Challenge of "Shadow Access"

IN TODAY'S DYNAMIC DIGITAL LANDSCAPE, THE CONVERGENCE OF TWO SIGNIFICANT TRENDS DEMANDS OUR IMMEDIATE ATTENTION

Trend 1: The Data Deluge

Zettabytes of data are stored in the cloud or in on-premises systems. What's alarming is the somewhat reckless sharing of this data.

Applications, cloud services, 3rd party entities, and even sophisticated AI are gaining access at an astonishing rate. For instance, AWS alone boasts over 15,000 permissions, and this number continues to grow on a daily basis.

Trend 2: The Complexity Challenge

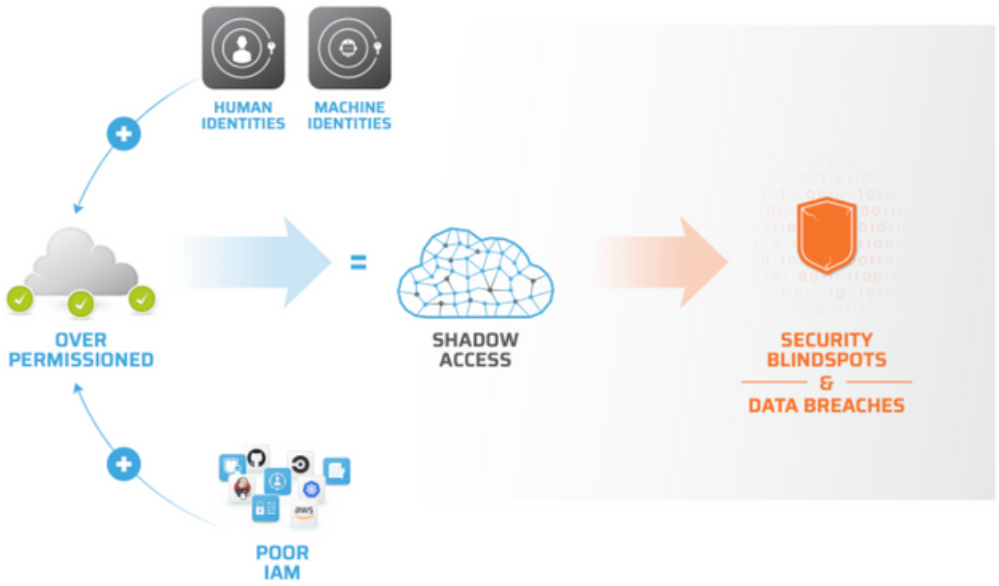
Enter the intricate world of Cloud IAM, complicated further by the proliferation of automated processes.

This web of permissions raises questions of:

- Who has access to what?
- Who is actively using these permissions?
- Are they authorized for such access?
- What unauthorized activities are happening beneath the surface?

This intersection of trends creates a new threat vector: Shadow Access

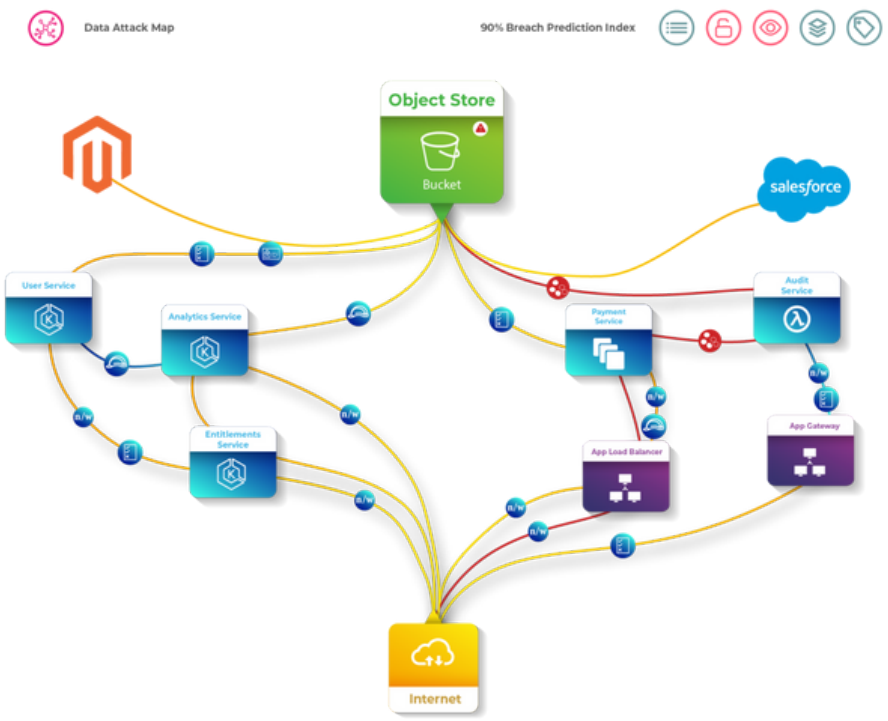
Enabled by the two trends above, Shadow Access lurks unnoticed and unmonitored, posing a significant risk to your organization's vital assets.



Shadow Access permeates every cloud environment and leads to data breaches, compliance violations, operational disruptions, and security vulnerabilities. Malicious actors often leverage unmonitored Shadow Access to infiltrate systems and exfiltrate data.

Find exploitable shadow access in < 60 minutes

Stack ID Live Data Attack Map

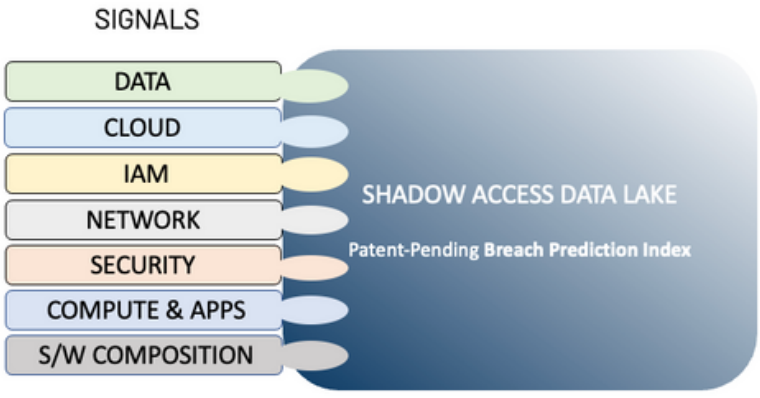


With Stack Identity, you can **continuously identify, quantify, and eliminate shadow access** to cloud services and data **before an attacker can exploit it.**

Auto Discovery of Shadow Access Patterns

Our platform detects ten different types of Shadow Access patterns - invisible access, excessive access, unwanted access, privilege escalation access, third-party access, Saas access, data recovery access, risky identities, toxic combinations, and impersonation access.

Unified Identity & Access Risk Management Platform

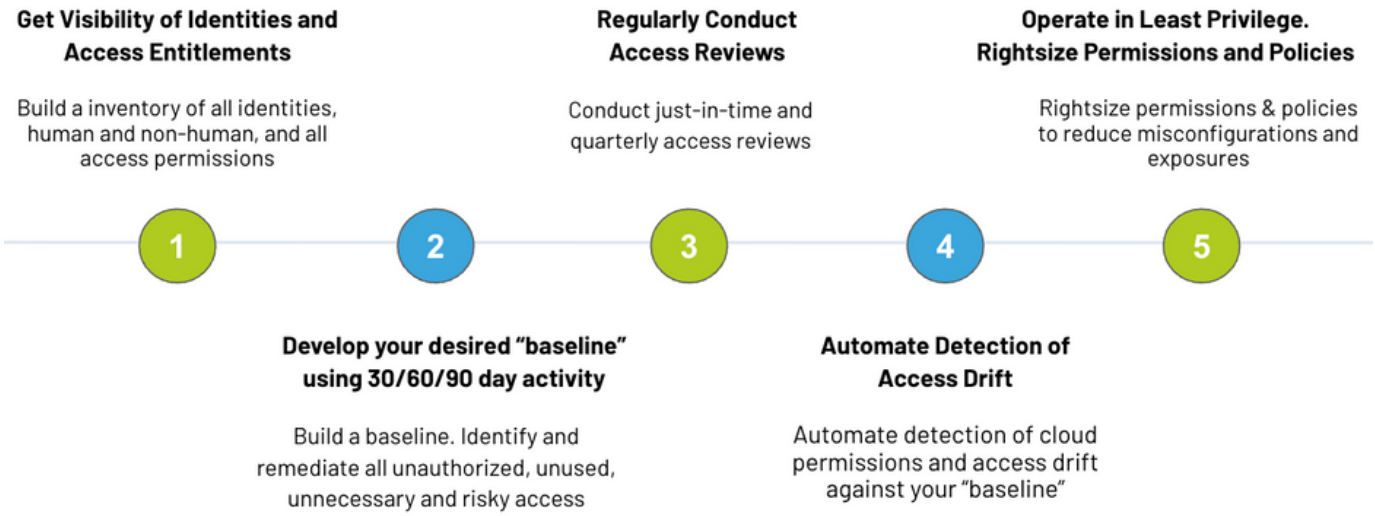


USES CASES

1. Centralized Visibility & Visualization
2. Modernize Access Reviews
3. Prioritization of Data Risks
4. IAM Governance for Data Security
5. Query Analytics for compliance automation

The platform takes a comprehensive and streamlined approach, integrating Cloud Identity and Entitlement Management (CIEM), Cloud Identity Governance and Administration (Cloud IGA), Data Access Governance, and Cloud Access Controls. It empowers organizations to regain control of their digital environment. With it, they can assess, review, remediate, and automatically redesign their cloud access controls across their data, applications, and interactions with third parties.

Stack Identity Enables Best Practices to Address Shadow Access



The issue of Shadow Access is real: it is an unintended but unavoidable result of DevOps processes. It is imperative to take action now to reveal the hidden vulnerabilities of identity and access lurking unnoticed and unmonitored, posing a significant cloud security risk to your organization's vital assets.

Take control of your shadow access risks and fix all your gaps across the identity security lifecycle:

Find and Fix IAM Risks | **Secure Cloud Data** | **Modernize Access**

Automate Governance and Compliance | **Operate in Least Privileged**

Visit us at www.stackidentity.com to learn how to take back control of your Shadow Access.

STACK IDENTITY