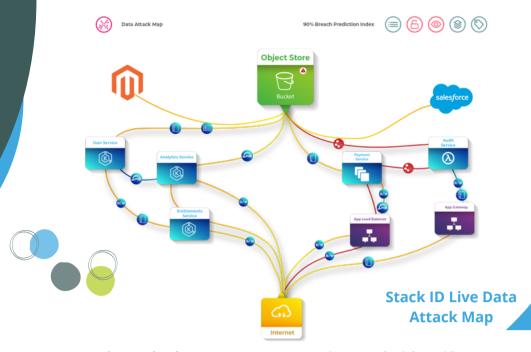
In the dynamic and ungoverned Cloud DevOps environment, Security and Cloud teams cannot answer fundamental questions:

- Who has access to what?
- Who is accessing what?



With Stack Identity, you can continuously identify, quantify and eliminate unwanted, unused, or invisible access to cloud infrastructure and data before an attacker can exploit it.

1

Baseline Inventory of IDs & Data

Baseline all identities, cloud infrastructure and data resources, roles, policies, permissions, entitlements, configurations.

2

Gain Continuous Visibility

See what access and entitlements are being used, across your entire cloud environment.

3

Uncover Vulnerabilities

Reveal exploitable, secondary or chained access that allows lateral movement to data and cloud resources. 4

Prioritize and Remediate

Quickly and effectively act on risks of identities, policies, permissions across all cloud identities, resources and data,.

Why Stack Identity?

Within 60 minutes of onboarding our platform, you can see a prioritized view of your cloud data and IAM risks.

We monitor all your cloud identity interactions continuously and in real time, to give you visibility into who is accessing what cloud data and give you control to lock down access.

Use Cases

- Eliminate unused identities and roles by limiting over provisioned roles, permissions
- Limit over provisioned roles, permissions
- Stop sensitive data exfiltration through invisible or risky access paths and policies
- Prioritize risks across all access & attack paths between identities and cloud infrastructure and data.

www.stackidentity.com

