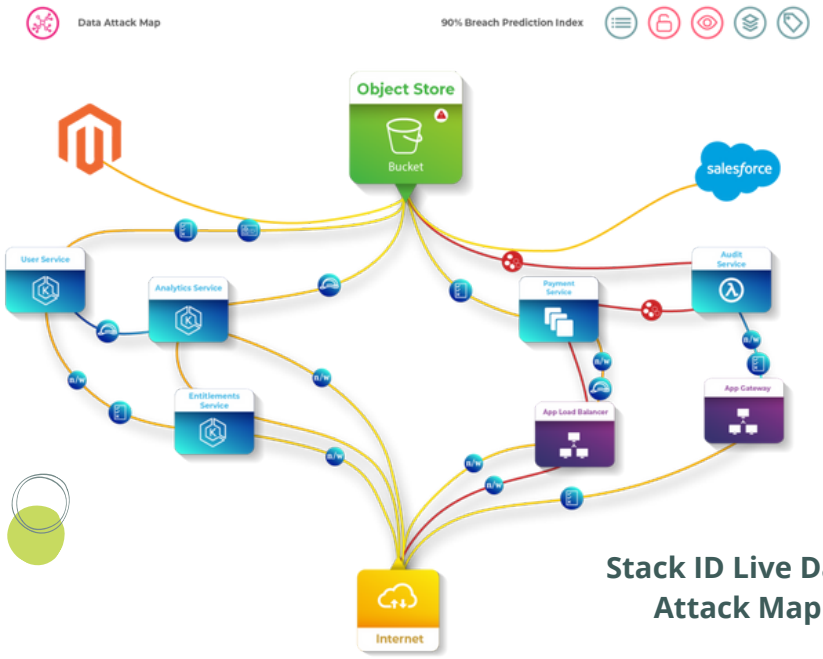
Find exploitable access to cloud data in less than 60 minutes



Stack ID Live Data Attack Map

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	2	3	4
Baseline Inventory of IDs & Data	**Gain Continuous Visibility**	**Uncover Vulnerabilities**	**Prioritize and Remediate**
Baseline all identities, cloud infrastructure and data resources, roles, policies, permissions, entitlements, configurations.	See what access and entitlements are being used, across your entire cloud environment.	Reveal exploitable, secondary or chained access that allows lateral movement to data and cloud resources.	Quickly and effectively act on risks of identities, policies, permissions across all cloud identities, resources and data,.

Stack Identity has found the following #ExploitableCloudDataAccess

- Crypto mining and malware hosting on **compromised access to S3**
- Lambda function replaced with **malicious code for an attacker's outside access**
- **Compute instance with abused IAM permissions** to exfiltrate sensitive data
- **Backdoor for an attacker** due to a compromised resource based policy
- **Invisible access for an attacker** because the AWS policy console does not show effective permissions or inherited permissions to an identity or resource

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

www.stackidentity.com

STACK IDENTITY