STACK IDENTITY

CLOUD SERVICE MANAGEMENT CASE STUDY

OBJECTIVE

Quantification of all cloud identity and access risks and vulnerabilities impacting sensitive data. This is difficult because visibility of identity and access is scattered across cloud IAM, IDP, data stores, ticketing systems and spreadsheets.

CHALLENGES

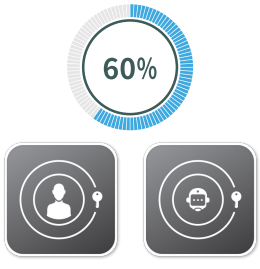
- On-prem vulnerability mgmt tool did not work for cloud
- No standardized, repeatable way to find and assess IAM data for risk, compliance and governance
- Need to replace unscalable manual processes due to fragmented data, systems and tools

BENEFITS

- A single source of truth for identity, access, data posture and governance
- Easy to use product
- Automated detections that track policy violations, the access attack surface and risky access pathways
- Quantifiable metrics tracked via company ticketing systems

SOLUTION

Stack Identity's Cloud IAM platform and live data attack map enables the ability to definitively know how many identities exist and which identities have access to what in the enterprise cloud environment. Detected and remediated IAM risks and vulnerabilities that no other product could.



"Stack Identity's cloud IAM platform identified that over 60% of existing identities in our environment needed to be right sized and have access revoked."

- CISO, SERVICE MANAGEMENT SOFTWARE