sonraí SECURITY

Case Study

Fortune 100 Insurance Company Selects Sonrai Dig

Fortune 100 Insurance

This international Fortune 100 financial services company with more than 40,000 employees provides a range of insurance, investment, and wealth management products and services.

The Problem

This enterprise's Cloud Center of Excellence (CCOE) team wanted to quickly assess their thousands of AWS resources on an ongoing basis for security and compliance risks to meet auditing standards. To ensure they were meeting regulatory compliance and quarterly audits, the team needed complete visibility into their cloud. They needed a solution that could efficiently and continuously provide identity and data governance across their multiple public clouds while meeting strict regulatory standards for audits.

Working with tens of thousands of resources in their public cloud, this team struggled to document its internal controls—availability, security and confidentiality, and integrity—including its ability to prove the transmit and access of information securely to authorized parties.

Facing the real consequences of poor audit examination results and the possibility of the FDIC and FFIEC limiting this organization's ability to function, their accreditation was at risk. The cloud and security teams wanted to ensure that their most sensitive "crown-jewel" data of its mission-critical apps were protected by the best security technologies available on the market. A cloud security solution that could go across their multi-cloud deployment to baseline and continuously monitor for deviations identity to data relationships was needed to help the organization minimize security risks.

> ***"I want the business to release what they need to without worrying about technology."***
>
> Director of Cloud Infrastructure Architecture

The Goals

Enforce Compliance

The team needed to be very confident that they could meet their audit requirements to minimize risk for their customers and to ensure continuous compliance for their quarterly FDIC and FFIEC audits. They wanted to monitor for over-privileged identities, manually created identities, dormant identities, and any identities outside of their governance and security baselines. Additionally, any violations around data access and resource configuration needed to be reported and remediated in a timely manner. The CCOE team was not enabled to analyze public cloud audit data, quickly and efficiently.

Reduce Risk

Our customer wanted to quickly assess tens of thousands of AWS resources in their environment on an ongoing basis for security and compliance risks by finding all data stored in multiple clouds, classifying the type of data that was found, setting the baseline for identity access, and finally, continuously detecting deviations to that baseline.

The Results

Sonrai Dig enabled the CCOE team to establish a baseline and continuously monitor identities and data across all multiple public cloud resources. Dig includes built-in workflows for reviewing events with options to automatically initiate remediations for undesirable variations and trends. Or Dig can use a built-in workflow to prevent identity and data issues from happening in the first place. This enabled the teams to automatically route issues, reports, and actions to the right teams.

With comprehensive visibility into their groups, policies, identities, roles, accounts, permissions, and trust relationships across all cloud accounts, dev teams, and disparate cloud platforms, the CCOE team has been able to consistently provide the appropriate audit reports.

Sonrai Dig identified problems at their source. Risks were identified and removed, and compliance and platform posture gaps were quickly addressed.
In addition to powerful graphing technology that allows customers to review security posture continually (24/7/365), Sonrai also allowed this enterprise's admins to take the necessary actions to rapidly mitigate risk.

Sonrai Dig allowed this customer to de-risk their public cloud of identity and data concerns while meeting the audit examination and accreditation reporting. With all of these risks identified and removed, activity monitoring improved across their AWS environment. Through identifying interactions and originating identities, Dig was able to identify and continuously monitor all trust relationships across all accounts giving the team comfort that any unusual activity against sensitive data would be immediately flagged and remediated.

Want to see Sonrai Dig in action? Request a demo today.