sonraí SECURITY

Case Study

Top Bank Reduces Risk, Increases Security, and Enforces Compliance

Top 5 Canadian Bank

This leading provider of financial services supports the most significant corporations, institutional investors, asset managers, PE firms, and governments in personal and commercial banking operations.

The Problem

This Tier 1 bank decided to modernize its infrastructure and shift away from the old enterprise network and data-center approach in favor of a move to public cloud, leveraging a multi-cloud strategy. To ensure the safety of their data, their security program also required a fundamental change. This transformation required a solution that could efficiently and continuously provide identity and data governance across their multiple public clouds. Working at the speed of the cloud, they also realized that they needed a solution that provides intelligent workflow and automation capabilities to ensure that when an issue is identified it is remediated quickly.

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 technologies available on the market. A cloud security platform was needed to help the organization minimize security risk and eliminate any unnecessary infrastructure risk that could lead to the exposure of sensitive data. Additionally, this solution would be a key aspect of the audit and compliance program and help meet the international financial regulations required for business across multiple continents.

With protecting crown jewel data and securing workloads as a top concern, this multinational financial services company began evaluating cloud security tools. Evaluating the market for a solution seemed to be a challenge itself. They were unable to gain strict visibility around the bank's cloud App accounts that held sensitive data, including PII. Additionally, it seemed too many of the cloud security tools were built to send alerts to a centralized team, which was the paradigm in the world they were leaving behind. They knew that the issues in cloud needed to be looked at by many different teams based on the projects they aligned to and needed a platform that could offer this at the level of sophistication of their business.

"Our security team demanded extensive governance around sensitive data for all AWS and Azure deployments. With Sonrai we verify all identity and data controls are in place and working. We can demonstrate that our risk in the cloud is equivalent or less than our on-premise data centers."

-Head of Cloud

The Goals

Reduce Risk
The company needed to find all data stored in the cloud, classify it, identify not just which identities (people and non-people) could access it but also baseline access patterns and detect deviations continuously. Additionally, they needed to be able to monitor for re-classification of data from higher levels to lower.

Increase Security
The team wanted to track movement between data stores and outside of appropriate zones, as well as be alerted to failed attempts to move data without proper authorization. Most importantly, they wanted to be able to do this with cloud identity and local DB accounts. The goal was to baseline normal activity and flag if anomalous access has been detected.

Enforce Compliance
Monitor for over-privileged identities, manually created identities, dormant identities, identities with elevated permissions. Detect Separation of Duties violations around data resource access and the resource configuration. Finally, translate and apply enterprise platform governance policies and controls to the new multi-cloud infrastructure.

"Sonrai reduced time to approve new app deployment process to pass critical cloud controls from 2 weeks to 1 day."
-Head Of Cloud

The Results

Identity and access risks were easily identified and systematically removed leveraging Sonrai Dig. This enterprise bank had established some controls for managing roles and privileges in the cloud. However, they saw tons of value in gaining comprehensive visibility into their groups, policies, identities, roles, accounts, permissions, and trust relationships across all cloud accounts, dev teams and disparate cloud platforms. Dig integrated seamlessly and with out-of-the-box identity risk frameworks, delivered visibility within days of all 'effective permissions' for data and identities and helped to remediate uncovered risks.

With risks identified and removed, activity monitoring also improved across their environments. By understanding interactions and originating identities, Dig was able to identify and relentlessly monitor all trust relationships across all accounts giving comfort that any unusual activity against sensitive data would be flagged.

Compliance and platform posture gaps were also quickly addressed as Sonrai Dig identified problems at their source. Additionally, powerful visualization capabilities allowed this customer to review security posture in real-time to discover any compromised workloads, open ports, or misconfigurations. Sonrai Dig also allowed administrators to take the necessary actions to rapidly mitigate risk. This removed reliance on a patchwork of tools needed for monitoring, remediation, or enforcement, thus bringing agility to the security and compliance workflow.

Next up for this customer will be to leverage the classification capability of Sonrai Dig to confirm data classifications and discover any unclassified PII. Also, the bank plans to use the role-based access capabilities to roll Sonrai Dig out to all development teams so that problems and solutions are flagged right to the source.

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

sonraisecurity.com | info@sonraisecurity.com | 646.389.2262

sonraí SECURITY