sonraí SECURITY

Case Study

US Bank Transforms Enterprise Cloud Security

TOP 10 US BANK

This publicly traded and rapidly growing large financial institution is one of the world's largest banks serving millions of customers operating globally. With a clear commitment to investing in cybersecurity, this agile team decided to bring together colleagues from critical functions across the bank to increase their effectiveness in protecting and responding to potential cloud security threats.

The Problem

This customer had over 40 team members across the organization responsible for securely migrating workloads to public cloud. To complement the security functionality provided by Azure, the bank was looking for an out-of-the box solution that could provide automated security and compliance controls, as well as visibility into its infrastructure to enable their DevOps teams to quickly build applications.

Being highly aware of the dangers of data breaches in the financial industry, the team wanted to be sure that critical data was not at risk for unauthorized access and/or exposure. Recognizing that any time a change of configuration occurs, gaps can develop and accumulate over time. They wanted to be sure that they had effective configuration drift detection, whether the change was a result of microservices, users, or even third-party applications.

Worried that a misconfiguration could lead to unauthorized data exposure in their cloud, the team began looking for a solution to complement their growing cloud needs. Their infosec maturity already highlighted that when there are too many alerts, which meant critical warning signs were being missed, so the bank needed a solution that could continuously monitor for deviations to their security baseline, and intelligently manage alerts to ensure that the issues went directly to the teams responsible for addressing them, as well as to leverage automation wherever possible. For this team, monitoring needed to include details regarding the who, what, when, and where of data access from all sources.

After reviewing several cloud security platform solutions, this large financial institute decided on Sonrai Dig to meet their identity and data governance needs.

"We need to move quickly without losing security. Sonrai gives us both speed and security."

Technology Product Owner
Public Cloud Compliance

The Goals

Maximize Efficiency
This enterprise bank had rapidly growing workloads and needed efficiencies for resource allocation, streamlined collaboration and coordination across multiple teams. Additionally, the team needed to manage the complexity of thousands of identities and their data access rights in their cloud. Their goal was to simplify the views of their cloud and reduce complexity in managing drift.

Increase Security
The bank wanted to continuously monitor third-party integrations to stay on top of issues. To enable the ability for third-party providers to maintain the applications that are critical to them, the team needed to administer databases, configure resources, monitor security perimeters, and perform other important tasks to ensure business continuity. Due to their roles and tasks, the bank wanted to continuously monitor to be sure they had the correct effective permissions and privileged access to critical information.

Reduce Risk
The bank's team wanted to eliminate all potential identity risks. Graphing all trust relationships between identities and their permissions was required to improve tracking, reporting, and monitoring of all identities.

The Results

Identity and access risks were easily identified and systematically removed leveraging Sonrai Dig. This financial enterprise required the ability to move from proof-of-concept to production quickly and without complexity. They leveraged the value in gaining comprehensive visibility into their groups, policies, identities, roles, accounts, permissions, and trust relationships across all of their cloud accounts. Dig integrated seamlessly with out-of-the-box identity risk frameworks and delivered the visibility within days of all "effective permissions" for data and identities and helped to remediate uncovered risks.

This bank wanted to address demands associated with controlling and managing privileged access and improve processes related to managing privileged identities. The team had a set of policies that were unique to their business and wanted to ensure these policies were put in place to restrict the creation or change of risky cloud services and eliminate the possibility of risks being created in the first place. Leveraging the flexibility of Sonrai Dig, the bank was able to build in their unique governance and security frameworks ensuring data stays secure and in their cloud. With Dig, this team can now see any unwanted changes that occur, actions that can be triggered to remediate the issue, and then eliminate risk.

This customer was able to gain complete visibility across their public clouds. Sonrai Dig enables the bank's operations teams to own security while also providing a "big picture" view to security and audit teams, as well as corporate and executive management. Complete visibility helped them reduce risk and reduce response times by resolving issues proactively. Dig's continuous monitoring extended to 3rd party sources (such as Data Bricks and Hashicorp Vault), meaning the bank can identify possible data exposure risks based on secrets stored in these services.

This customer's plan is to continue expanding and growing their cloud footprint while maintaining security and compliance across existing and new workloads.

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

sonraisecurity.com | info@sonraisecurity.com | 646.389.2262

sonraí SECURITY