sonraí SECURITY

Industry
Finance

Region
Global

Cloud Environment
Microsoft Azure aws

CASE STUDY

Top 10 US Bank

Security plays the hero by enabling faster, completely automated workload deployment - and cloud adoption explodes.

The top US bank is the one of the largest banks in North America, serving 25 million customers in 64 lines of business with locations around the globe. The bank is also among the world's leading online financial services firms, with approximately 11 million active online and mobile customers.

The Problem

The CIO declared they needed an industry leading customer experience, and that meant going all-in on the cloud.

Improvement of the bank's web and mobile customer experience meant more rapid cloud development and workload deployment. But their exacting standards around customer data protection were slowing this transition down.

The hurdles to rapid cloud adoption were myriad. Commitments to customer data security and audit requirements demanded an extremely custom posture management. The security team tried to support this with existing tooling, using a first-generation CSPM, a SIEM, and log management tools to get a full record of who could access what data, and when. But these tools didn't understand cloud actions and resource data well enough - ie, was this new action in Azure a delete action, a list action, a create action? Was an AWS service control policy going to override this new action? Who could make edits to this database, and what edits were made between scans? Was a resource deployed and then quickly removed? They didn't have these answers, and since their security policies weren't updated as the cloud was updated, controls became obsolete as Azure innovated further and more services were brought online.

The Solution

Commitment to customer data security and audit requirements demand an extremely custom posture management. They wanted an extremely secure cloud but had to fully embrace it. So their answer was automation.

The cloud team had a radical idea: what if our cloud just didn't get touched by humans? Their development pipeline was advanced enough with automated services that could handle every workload deployment. If there were predictable automated processes for every workload, alerts could focus on any anomalous activity - which meant fewer environment-specific controls. So any shift in the pattern of cloud actions, normally locked in by automated routines, would be flagged as a security alert.

> **"It allows us to do all of that once again, without compromising on control and security."**
>
> — Chief Information Officer

So instead of hundreds of policies looking for explicit actions - ie, a blob was created and is open to the public - the controls look for any action not created by the automated services spinning up IaC and deploying workloads.

The hurdle here would be maintenance: when CSPs release new types of actions and permissions every day they'd need their policies to understand and categorize them. Luckily, Sonrai's security model does that every day.

90% of Sonrai customers deployed have found unintended and mistaken data exposure in their cloud.

There are over 35,000 different cloud actions across the major CSPs, with 17 new ones released every day. Keeping security policies durable requires daily maintenance.

The Impact

The security team is focused on what matters, and cloud adoption is skyrocketing.

A set of simplified controls within a tailor-made framework made secure, automated deployment easier - and since Sonrai automatically keeps pace with the cloud provider's innovation, maintenance of policies is minimal. Since automation unlocks an anomaly-centric alert model, there are far fewer controls than an average large financial enterprise - meaning less alerts, less false positives, and more time on threat investigation.

More importantly, the security team has made a far-ranging impact on the business. The dev team doesn't waste valuable resources on managing cloud deployment. A data-centric approach means customer data exposure risk is minimized. And they've enabled the cloud team to meet the CIO's mandate for better customer experience - with predictable, scalable, secure deployment, workloads are hitting the cloud faster, and cloud adoption is skyrocketing.

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

sonrai SECURITY

sonraisecurity.com
info@sonraisecurity.com
646.389.2262