SALT

Finastra
Case Study

Finastra is the largest pure-play software vendor that serves the entire financial services industry. The company works with more than 8,600 customers, including 90 of the top 100 banks globally. Finastra builds and deploys innovative, next-generation technology on its open Fusion software architecture and cloud ecosystem, delivering mission-critical solutions for financial institutions of all sizes, on premises or in the cloud. The company's broad portfolio of financial software solutions spans retail banking, transaction banking, lending, and treasury and capital markets. APIs are the key enabler for connecting these diverse partners to data and services across the Finastra platforms.

Mali Gorantla, Finastra's head of product and data security, was looking for a way to ensure the security of these APIs. Initially the team investigated building an internal solution. "This is a machine learning problem, and I was sure that we could solve it in-house," he explains. "Once we identified the requirements including models, UI, tracking down false positives, and building in the DevOps functionality, our TCO ended up being almost 3x what we would pay with an external solution – it made much better sense to buy vs. build."

Finastra began evaluating different API security platforms. The team understood the limitations of WAFs – the extensive tuning required to get any protection and the fundamental limitations around context. "WAFs see the world one transaction at a time – they have no notion of user context, and no notion of changes over time," says Gorantla.

"We were asking, how can we investigate incidents when they occur? Many vendors were focused on showing us logs, but that's too late, and they don't give you context. To properly protect APIs, we need to see behavior over time and understand the usage patterns for all our APIs."

FINASTRA

Finastra provides its FusionFabric.cloud SaaS platform to develop and deliver a portfolio of financial software and mission-critical solutions for financial institutions of all sizes, on premises or in the cloud.

Headquarters London

Founded 2017

Infrastructure Microsoft Azure

www.finastra.com

> *"We see everything we need directly in the Salt dashboard, so we can triage events more efficiently. We've improved our mean time to respond 10 fold, and we're using the Salt platform to automatically block API attacks."*
>
> **Mali Gorantla,**
> **head of product and data security, Finastra**

After testing multiple solutions, the team found Salt Security provided the context Finastra needed to identify all the APIs running in the company's environments, identify and block attackers, and share insights for the development teams to harden their APIs. "We were able to see this rich context in the Salt dashboard within a couple of hours."

The Salt approach to API data discovery is comprehensive – the system deploys out of band and collects an enormous amount of data on APIs, including the sensitive data they expose, across all application environments. Salt funnels that data into its big data engine and applies AI and ML to learn and dynamically update API patterns. Salt identifies abnormal behavior and uses that rich context to quickly ascertain if the behavior is different because an API changed or is different because it's malicious.

"We see everything we need directly in the Salt dashboard, so we can triage events more efficiently," says Gorantla. "We've improved our mean time to respond 10 fold, and we're using the Salt platform to automatically block API attacks."

Top use cases for Finastra:

- **full API discovery:** Salt gives Finastra a continuous inventory of all its APIs, with rich details such as parameter information and where requests and responses include sensitive data
- **automatic attack prevention:** Finastra is able to tap Salt to block API attacks without needing human intervention
- **compliance:** Finastra uses the Salt platform to continuously capture API details and enhance documentation

Salt Security protects the APIs that are at the core of every modern application. The company's API Protection Platform is the industry's first patented solution to prevent the next generation of API attacks, using behavioral protection. Deployed in minutes, the AI-powered solution automatically and continuously discovers and learns the granular behavior of a company's APIs and requires no configuration or customization to prevent API attacks.

CS-FINA-20211206

Request a demo today!
info@salt.security
www.salt.security

SALT