SALT

Financial Services

CASE STUDY

This leading digital financial services company is an award-winning online bank offering a full suite of banking products including home loans, savings, money-market, checking, certificates of deposit (CDs), individual retirement accounts (IRAs), securities-brokerage and investment-advisory services, and capital for equity sponsors and middle-market companies.

The company's vision is to change the online banking landscape with innovative digital experiences, relying on API-based services to deliver those experiences. The bank quickly realized that its existing web application firewalls (WAFs), bot mitigation tools, and API gateways all fell short in protecting these vital APIs.

As with so many DevOps-oriented companies, the bank initially spent a lot of energy looking for ways to secure APIs in dev and testing cycles. It soon became apparent that this approach was hampering rapid app dev practices. According to the company's lead security engineer, "We were spending more time identifying, prioritizing, and remediating security gaps in pre-production, and we came to the realization that while shift-left is important, it's not the full solution. We needed to incorporate runtime protection to really protect ourselves."

The company engaged with Salt Security in an effort to get the best of both worlds: continuous, real-world insights about API vulnerabilities or gaps that developers could address and runtime detection and response capabilities essential to shutting down attackers. "What's unique about Salt," explains the engineer, "is that this approach isn't CVE-based – it's behavioral. If a bad actor tries something new, we can catch it, even if we've never seen it before."

Salt provides remediation insights for dev teams to strengthen API security. "Salt lets our teams embrace microservices because they know the pipeline is safe," says the lead security engineer. A variety of teams at the bank are deriving significant value from the Salt platform:

anonymous
DIGITAL FINANCIAL SERVICES

A leading FinTech company is changing the way their customers bank, integrating innovative digital experiences for home loans, IRAs, checking and savings, and more.

Infrastructure
A hybrid cloud platform supports cloud-native application development; Devops processes increase collaboration, innovation, and efficiency.

- **Vulnerability Management Team –** to define vulnerabilities and evaluate risk
- **Fraud Prevention Team –** to provide investigative data as an interaction biometric, baselining legitimate behavior and identifying attackers in real time
- **InfoSec Team –** to discover all APIs and exposed data
- **API Development Team** - to prioritize remediations
- **Compliance and Regulatory Team –** to document the full catalog of personally identifiable information (PII) accessed via APIs

Salt Security automatically maps all sensitive data and PII, detecting new data introduced throughout the development process, from staging to production. This approach ensures and validates that API changes are not exposing customers' sensitive data or sharing sensitive data with third-party vendors without the security team's full awareness. It also ensures that an API change does not violate existing compliance and privacy regulation requirements, eliminating the need for manual auditing.

"We asked the question, 'What if a protection tool could just stay caught up with us?' and Salt answered," says the security engineer. "The development team doesn't have to update Swagger, and the vulnerability management team doesn't worry about how to scan every endpoint. Salt lets developers move as fast as they want, with all the tools they want."

Top API security use cases for this leading bank:

- **attack prevention:** Salt identifies and stops attacks missed by the company's WAF and API gateway including the OWASP API Security Top 10.
- **remediation insights:** Salt creates remediation insights that dev teams use to eliminate API vulnerabilities and improve security.
- **compliance:** Salt identifies shadow (unknown) and zombie (outdated) APIs as well as exposure of sensitive data such as PII.

> **We asked the question, 'What if a protection tool could just stay caught up with us?' and Salt answered. Salt lets developers move as fast as they want, with all the tools they want."**
>
> **– Lead security engineer**

SALT

Salt Security protects the APIs that form the core of every modern application. Its patented API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. By correlating activities across millions of APIs and users over time, Salt delivers deep context with real-time analysis and continuous insights for API discovery, attack prevention, and shift-left practices. Deployed in minutes and seamlessly integrated within existing systems, the Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives.

Request a demo today!

info@salt.security

www.salt.security