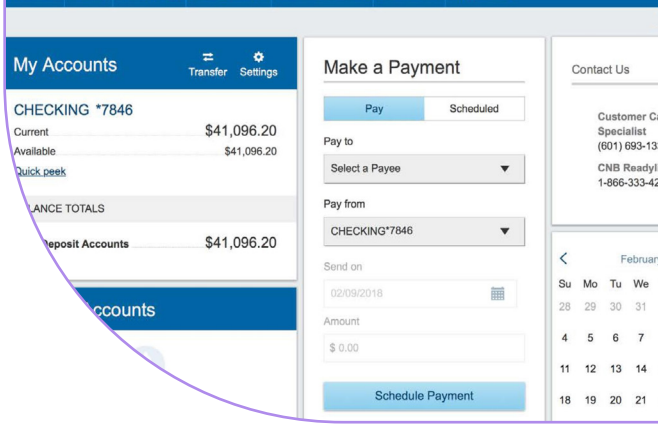
SALT



Financial Services

CASE STUDY

For over 150 years, this Fortune 500 financial services company has been an international leader in providing integrated financial solutions, including checking, savings, time and deposit accounts, private banking, loans and lines of credit, credit cards, cash and wealth management, online banking, electronic check deposit, and other services. The company's more than 500 employees serve the bank's 76,000 customers.

As the company expands services to customers, APIs allow the team to customize the customer experience, including features such as the ability to integrate bank accounts with bookkeeping software or accessing investment account information. Using APIs makes it easier for the bank to give each customer a unique experience, picking the programs and apps that best suit their needs. "We view our identity as a service platform," says the company's CISO. "A lot of our customers are accessing a variety of financial apps from FinTech innovators, and those companies are only as good as the data they can ingest, crunch, and spit back out. Our customers need to have access to their financial data through an API, so they can use whatever FinTech tool they want."

In financial services, security is paramount. When the company started work on its Internet-facing mobile app, the security team quickly realized that depending on tools like Web Application Firewalls (WAFs) was neither a scalable solution nor would it detect API attacks. "Ultimately, good security depends on the detection and response capabilities," explained the CISO. "But we also wanted to shift prevention more to the left – all the way to development and design. Ideally, we wanted one tool for both the shift left features and the runtime detection and response." The company found that combination of capabilities in the Salt Security API Protection Platform.

Salt was able to provide the company's security and development teams with continuous, real-world insights about API vulnerabilities or gaps that that weren't caught in pre-production scanning or testing. Salt builds a deep understanding of the unique context of the bank's APIs and how they're being used – and misused – in production environments. "We want developers focused on functionality," says the CISO, "and Salt lets them do that." The

FORTUNE 500
FINANCIAL SERVICES COMPANY

This international financial services leader provides integrated financial solutions to its 76,000 customers. As the company expands its API-based services, the team is focused on building security into every stage of development and design, and into runtime and response.

Infrastructure
Imperva WAF Cloud, MuleSoft, F5, Azure Cloud, on-prem

tangible and relevant insights Salt provides enables the company's developers to quickly and easily increase their own security awareness and improve development best practices, so they minimize future API vulnerabilities.

In addition, Salt provides the runtime detection and response capabilities essential to shutting down attackers. The platform delivers a complete view of all attacker activity, correlating and associating dispersed activities with a single user, despite attackers' efforts to use varying IDs, IP addresses, and devices to propagate their attacks. This approach reduces investigation times and helps the bank's teams respond to attacks with confidence.

Top API security use cases for this bank:

- **full API discovery:** Salt gives the bank's teams a full and continuously updated inventory of all its APIs and the sensitive data they expose.
- **attack prevention:** protecting its customers' financial data is critical to the bank, and Salt finds and stops attackers before they can succeed with account misuse or data exfiltration.
- **remediation insights:** Salt helps the bank's developers focus on new functionality by providing details on API vulnerabilities they can implement quickly to harden their APIs.

> **APIs are so lucrative for attackers today, and they create a huge playground for attackers. Banks with WAFs and API gateways are successfully getting attacked all the time – we needed to do more, and Salt has the context to protect our custom APIs."**
>
> **– CISO**

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.

CS-FIN1-20210415

Request a demo today!

info@salt.security

www.salt.security