SALT

API Security for Financial Services Companies

The changing API landscape in Financial Services

Financial services companies have relied on APIs for years, but over the past couple years, APIs have played an increasingly critical role in fueling digital transformation and innovation. Three recent changes have compounded the risk that APIs present:

- Increased use of APIs, growing the attack surface
- Greater exposure of sensitive data
- More frequent API changes thanks to agile development

Attacks targeting APIs are on the rise

Attackers have realized that APIs make an attractive target. The financial services industry has seen a steep rise in the volume and sophistication of API attacks, typically motivated by these common goals:

- Fraudulent transactions
- Data exfiltration
- Service disruption

Financial services companies have employed multiple layers of security solutions and practices, including WAFs and API gateways, but remain unable to detect or prevent API attacks, because traditional application security tools miss the vast majority of attacks targeting APIs.

> ***By 2022, API abuses will move from infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications."***
>
> Gartner

What's needed to protect APIs

Discovering APIs

Shadow APIs, and the sensitive data they expose, put financial services companies at risk. Continuous discovery of new and changed APIs is essential to protecting data and services.

Stopping API attacks

Preventing API attacks requires deep understanding of unique API logic and behavior, both of which depend on the use of big data, machine learning (ML), and artificial intelligence (AI).

Eliminating vulnerabilities

Efficient remediation relies on DevOps teams getting clear, prioritized, and actionable insights about how attackers have successfully probed APIs.

The Salt Security API Protection Platform

Discover all your APIs

Inventory all your APIs and eliminate blind spots

- Dynamically inventory all APIs, including shadow, zombie, new, and changed APIs
- Catalog exposed PII and other sensitive data to meet PSD2, PCI-DSS, GDPR, and CCPA

Stop attacks

Stop attackers early during reconnaissance

- Correlate anomalous activity to identify attackers
- Pinpoint attacks early, during the reconnaissance phase, and shut down the attacker
- Cut incident response from hours to minutes with a comprehensive attack timeline view

Remediate vulnerabilities

Eliminate API vulnerabilities at their source

- Share remediation details with DevOps to eliminate vulnerabilities in APIs
- Continuously harden APIs during development to ensure security doesn't slow application rollout

> ***"APIs underlie our FusionFabric.cloud platform, and Salt Security helps us protect the data and services exchanged between the producers (FinTechs) and consumers (financial institutions) of it. Salt Security detects and alerts on fraudulent or malicious acticvity and provides the remediation details we need to constantly improve our API security posture."***

Nir Valtman,
head of product and data security

FINASTRA

Salt Security financial services customers include:

FINASTRA

ally

cross river

BV

celsius network

Payoneer

CITY NATIONAL BANK
AN RBC COMPANY

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.

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

SALT