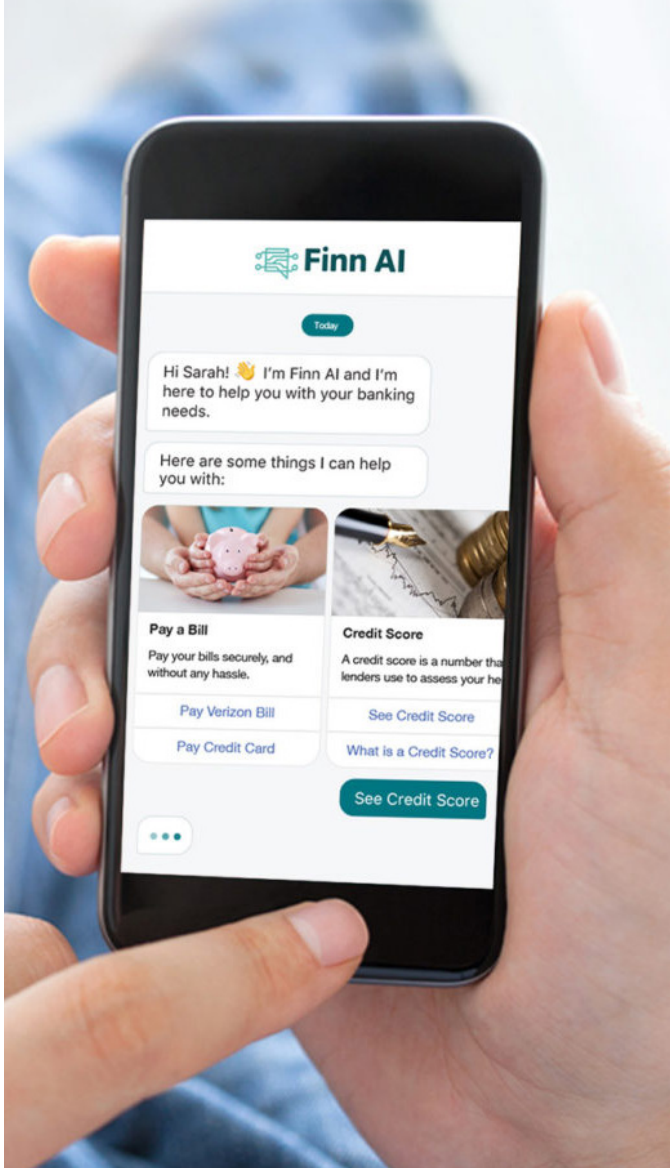
Signal Sciences

Detecting and Preventing Attacks Against Business Critical APIs



CHALLENGE

Finn AI needed visibility into API discovery attempts by malicious threat actors, as well as the ability to stop unusual activity against those same APIs that enable customers to use their natural language processing technology.

Finn AI uses natural language processing (NLP) to provide conversational AI technology to banks and financial institutions, allowing bank customers to manage personal finances with simple conversations, either through voice or text-based interactions.

Without a client-side frontend, the Finn AI attack surface is relatively small. However, their business-critical APIs still require effective visibility into API discovery and attempts by attackers to deliver malicious payloads against them.

Finn AI sought secure protection that would install easily and scale effectively while being light on resources, along with protection against OWASP Top 10 and zero-day exploit attempts.

"Signal Sciences provides us with the ability to peer behind the curtain, allowing us to see what's happening at the application layer. When our customers deployed penetration clients to test Finn AI for compliance validation, they weren't able to get any of their penetration tests past Signal Sciences while it was enabled."

Robin Monks, Director of Engineering

SOLUTION

Finn AI acts as middleware, working between the commercial frontends and SDKs of a bank's apps, including mobile apps. With Node.js as the core of their middleware, Finn AI selected Signal Sciences to run alongside it for effective inspection of API requests.

Finn AI operates within Amazon Web Services, so legacy WAF offerings that lacked a cloud-native focus were not considered. "As a cloud-native offering, it made sense to deploy Signal Sciences," said Robin Monks, Director of Engineering. "We liked the approach they use to evolve a machine learning-based approach as protection against zero-day attacks."

Additional benefits include:

Visibility across the attack surface and a proactive defense

Aside from stopping attacks that evade other network layer tools, Finn AI relies on Signal Sciences to uncover the mass and types of attacks malicious actors attempt to use against their APIs. For example, during SOCII compliance penetration testing, the Finn AI team could detect that testers were using endpoint scanners. Additional information was available in the data provided, relative to those attempts.

Maximize IT staff utilization while building security resilience

Maintaining security-focus within an agile development team meant finding a tool that could provide feedback on persistent attack attempts, while being easy to use. With Signal Sciences, Finn AI leverages new attack insights to improve their security posture across their IT stack, including hardening the configuration of the DDoS and network firewalls in place.

Actionable alert feedback that solidifies security posture

Feedback loops via alerts sent to various DevOps tools like Slack and Jira allow Finn AI to better analyze the attack surface. The reporting and dashboards are key to the discovery of new traffic anomalies for examination. The Finn AI DevOps team also uses the Signal Sciences dashboards to provide proof to their Board of Directors that steps have been taken to detect and stop automated attacks.

> "Signal Sciences helped us to quickly optimize the tool for use in production. We've seen excellent improvements over time as they adapt to changing security requirements. This makes for an excellent return on investment as there's been no need to purchase additional appsec tools as threats emerge."
>
> **Robin Monks,** Director of Engineering