Synack

CASE STUDY

Varo

Synack continuous pentesting helps Varo become a full-fledged online bank

As Varo prepared to spin out from its sponsorship bank model, they engaged Synack to help improve vulnerability testing and demonstrate their security preparedness to banking regulators.

Situation

Varo Bank was founded in 2015 as Varo Money, an app-based online bank operating within the US Bancorp sponsorship system. Varo's goal was to build the business until they could operate on their own as a fully-fledged bank. To earn a banking charter, Varo had to show regulators that they had a secure operation as specified by the Federal Financial Institutions Examination Council (FFIEC). As the customer base grew rapidly, so did the infrastructure and the effort required to keep it secure. They used automated scanning and added point-in-time pentesting, but they were not satisfied with the results.

Problem

As Varo's business and headcount grew, they had to either perform testing in-house or find support from a third-party. They found performing pentesting solely in-house was not a long-term solution. Demand for highly skilled candidates and a shortage of qualified candidates proved difficult for hiring. Varo was using a relatively new technology, the GraphQL query language, to ingest data. GraphQL is a proven solution to aggregate data from multiple sources, specify data, and describe data at scale. However, newer technologies also have fewer years of security testing to harden them.

Results

- Using Vulnerability Burndown charts in the Synack platform, Varo was able to demonstrate vulnerability testing trends to regulators, something that was not possible with point-in-time testing.
- Reports demonstrated their speed at addressing findings to regulators with Synack platform data, which was also not possible with point-in-time testing.
- Pentest reports with consistent results demonstrated how the security team was performing to internal stakeholders.
- Varo Bank became the first U.S. consumer fintech to receive a national bank charter from the Office of the Comptroller of the Currency in August 2020, in part due to Synack testing data.

"We particularly liked being able to interact with researchers on our schedule when we had questions. With a regular pen test, we would have lost access to the testers when the test was over."

SAL DAZZO – DIRECTOR OF ENGINEERING, VARO BANK

Solution

Varo reviewed a few different vendors for continuous pentesting capabilities, and Synack stood out with its Synack365 offering. Synack maintained a map of current cloud resources to allow for agile pentesting, which proved compatible with Varo's frequent app updates. Synack's reporting and follow-up consults also impressed Varo. They found that reports from Synack were more thorough than what they had been getting from their existing pentesting. Varo was able to interact directly with Synack researchers regarding remediation and have back-and-forth communication with Synack researchers about reports.

Point-in-time testing would quickly become out of date, but Synack's continuous, on-demand model gave Varo confidence that each software release was scrutinized by bounty-seeking researchers. Synack also assigned custom missions to SRT members that specifically addressed security testing for GraphQL. Pentesting results were used internally by developers and QA and related security bugs steadily reduced in number.