One Main Financial

DEVO + OneMain Financial

BACKGROUND

OneMain Financial operates in the consumer finance and insurance industries. Its business primarily focuses on providing personal loans and optional insurance products to customers with limited access to traditional lenders, such as banks and credit card companies. OneMain had approximately 1,500 branch offices in 44 states as of 2022.

OneMain Financial was previously using LogRhythm. The team was working across many different business units and LogRhythm was unable to effectively ingest and bring together the organizations cloud data sources for proper analysis and to ensure monitoring and compliance within industry regulations. The lack of visibility across these environments led to inefficiencies within their security team. Additionally,OneMain was struggling to effectively perform alerting and threat hunting with LogRhythm. As their renewal date approached, they began seeking a replacement to modernize their SOC.

CHALLENGE

OneMain Financial decided two years ago to replace its legacy SIEM solution in a new system it planned to implement. This was due to numerous issues, primarily that the technology had fallen behind the market and would be unable to meet its needs for auditing as well as any forensic investigations. The growing company needed a next-gen SIEM that could centralize its on-premises and cloud security data and deliver a single set of security analytics on AWS. In addition, OneMain Financial needed holistic insights into its homegrown applications—100 in total—along with its traditional security sources. These requirements were integral to their ongoing digital transformation initiatives.

DEVO

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.

SOLUTION

Ultimately, the team realized that two companies —Devo and AWS—met all of the requirements for the global next-gen SIEM solution. That choice was reinforced by seeing Devo Security Operations in use at one of the world's largest cybersecurity infrastructure vendors, and a referral from a leading industry analyst. Those recommendations, following a rigorous proof of concept (POC), led to the selection of the Devo Platform and AWS as their cloud provider.

RESULT

When it comes to network, endpoint, and cloud visibility, Devo and AWS made it easy to see all of that. Devo's dashboard made it possible. Instead of having to jump from system to system, OneMain Financial can see all of their web traffic and endpoint stats, and notifications to anything that is suspicious. It raises the level of confidence when they need to take action, compared to their last tool. When a forensic investigation moves forward and OneMain Financial has to do a deeper dive, all that data is there in AWS that allows OneMain Financial to query in real-time.

Monitoring core set of network devices and key systems. Collecting log traffic from their S3 buckets and using it as a platform to correlate and set up alerts to monitor and hunt for suspicious activity have all been invaluable to their continued success. OneMain Financial has an environment size of 14,000 users globally and with 20,000 endpoints being able to query data from our S3 buckets as far back as 400+ days where the competitors can only retain days from 90 days to 6 months.

The powerful combination of Devo and AWS enables OneMain Financial to detect threats, perform forensic analysis, and audit their environments for compliance in real-time at scale.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142