

Fortune 500 Financial Services Institution makes the switch to Devo



SUMMARY

This fortune 500 financial services company is based in Evansville, IN. The company provides consumer lending products to finance life events such as debt consolidation, home improvement, auto repair, medical procedures, and other major expenses.

The team was previously using LogRhythm for their SIEM, but visibility and ingestion issues inhibited the team from completing necessary tasks and threatened the organization's security posture. The security team switched to Devo to improve ingestion and parsing while providing environment coverage. With their LogRhythm contract up for renewal, Devo was able to migrate the team's data and get them up and running in **under 20 days**.

PROBLEM

Prior to Devo, the team was working across many business units. LogRhythm could not effectively ingest and consolidate the organization's cloud data sources for proper analysis. The lack of visibility across environments led to inefficiencies within the security team. Analysts were unable to perform effective alerting and threat hunting.

As a financial services institution, the team is legally required to protect its customer assets. The team was in a position where they did not feel they could provide 100% protection to their customer base. The threat landscape had broadened as attackers became more sophisticated. With their LogRhythm contract up for renewal, they needed to find a new solution that better secured critical assets.

SOLUTION

This fortune 500 financial institution was drawn to the Devo Platform because it is a modern, cloud-native SIEM that would provide simple integration and data migration. Devo allowed the team to successfully onboard and parse all necessary sources across the organization's endpoints.

Before adopting Devo, the company's environment was flooded with alerts. After implementing Devo, the teams were able to consolidate workloads and reduce noise – **resulting in 1 Devo alert for every 4 LogRhythm alerts**.

INDUSTRY

- Financial Services

ENVIRONMENT

- US-based company
- 1400 branches across 44 states
- 10.3 million customers served since 2010

SECURITY CHALLENGES

- Lack of visibility
- Inability to ingest all necessary data sources
- Need to provide increased security to customer assets

SOLUTION

- The Devo Platform

KEY BENEFITS

- Reduced noise from alerting
- Reduced analyst burnout
- Full visibility into environment across teams
- Access to a hands-on support team 24/7

Devo Platform also centralized several business units within a single pane of glass to improve visibility and give analysts the necessary tools to remediate threats. Devo also provides the team with access to 24/7 support. The organization's Head of Technology Operations and Engineering explained:

“
The Devo brand is about protecting data, and they've partnered with us and understand the problem statement they want to solve. Genuinely aligned with the fact that if you really want to solve your problems, partner with Devo.
”

THE RESULT

After switching to Devo, the team gained more visibility into their data – allowing them to protect customer assets and better understand their environment.



Devo
255 Main Street
Suite 702
Cambridge, MA 02142

© 2023 Devo All Rights Reserved

Devo is the only cloud-native security analytics platform that combines the power of people and intelligent automation to confidently defend expanding attack surfaces. An ally in keeping your organization secure, Devo augments security teams with AI – enabling you to continuously scale SOC efficiency, increase the speed of threat detection and response, and gain greater clarity to empower bold action, minimize risk, and maximize outcomes. Learn more at www.devo.com.