SentinelOne

Relay Network Doubles Visibility and Cuts Issue-Detection Time by Half

RELAY

CUSTOMER
Relay Network

INDUSTRY
Software

EMPLOYEES
51-200

COUNTRY
America

Overview

Relay Network, a B2C engagement platform provider, wanted to improve the efficiency of its security management and integrate tools more effectively to accelerate feature development. AWS Partner SentinelOne offered a comprehensive cloud security solution that seamlessly integrated with Relay Network's existing tools and Amazon Web Services (AWS) infrastructure. By implementing SentinelOne's solution, Relay Network experienced a 100 percent improvement in visibility, a 50 percent reduction in issue-detection time, and an 80 percent decrease in manual threat-detection efforts. With an enhanced security posture, Relay Network can maintain compliance standards more easily, accelerate feature development, and improve overall operational efficiency.

Opportunity

Manual Processes and Poor Integration Impede Efficiency

Relay Network, based in Radnor, Pennsylvania, specializes in providing a secure and compliant direct-to-consumer feed channel for enterprise-class healthcare and finance organizations. Its service enables businesses to create more valuable relationships with their clients through a personalized mobile engagement platform that delivers timely, multifaceted experiences, similar to scrolling on a social feed. This allows clients—such as banks, health insurance companies, and specialty pharma businesses—to provide conversations and experiences that match their customers' needs.

Equipped with tools that lacked integration and support for modern authentication methods, Relay Network faced significant challenges related to its technology infrastructure and security management. The engineering team's inability to access the necessary tools swiftly created inefficiencies in provisioning and user-interface interactions, leading them to rely on manual processes. This further complicated operations, resulting in a time-consuming and cumbersome experience for Relay Network's engineers, who were not security specialists.

Additionally, this process directly affected Relay Network's ability to serve its customers effectively. It slowed feature development and caused frequent interruptions, which required the engineering team to address security issues instead of focusing on innovation. This context switching not only delayed feature delivery, but also negatively affected overall developer satisfaction. As a result, customers experienced a slower rollout of new features and updates. These challenges hindered the company's goal of improving time to market, ultimately limiting its ability to deliver value to its clients.

Relay Network, based in Radnor, Pennsylvania, provides a secure B2C feed channel that enhances customer relationships. By combining the immediacy of text with engaging scrolling feeds, it delivers tailored content when customers need it. This approach boosts revenue, reduces service costs, and improves customer satisfaction compared to traditional communication methods.

PRODUCTS & SERVICES

- Complete Enterprise
- Cloud Workload Security
- Cloud Native Security
- Singularity Data Lake
- Purple AI

100%
improvement in visibility

Learn More →

Solution

Comprehensive Cloud Security Protects a Dynamic Infrastructure

To address its multifaceted challenges, Relay Network sought a comprehensive security solution. AWS Partner SentinelOne's position as a top-tier security provider—coupled with its ability to integrate seamlessly with Relay Network's existing tools from AWS, Snyk, PagerDuty, Jira, and GitHub—made it an attractive choice. SentinelOne's solution offered improved features over legacy vendors, at a lower cost. Most importantly, SentinelOne's deep experience with cloud-native environments and flexible options aligned well with Relay Network's infrastructure, which had been a pain point with previous security vendors.

SentinelOne's Cloud Native Application Protection Platform featured several relevant products for Relay Network. These included Cloud Workload Security for endpoint protection of cloud services, Cloud Native Security for posture management, and Cloud Data Security through Singularity Data Lake with Purple AI for threat detection. This comprehensive and integrated package allowed Relay Network to consolidate multiple security functions into a single, integrated platform. Particularly valuable was the solution's ability to handle a dynamic infrastructure, which worked with Relay Network's constant scaling and replacement of systems central to its AWS-based architecture. "All the technologies in SentinelOne's solution were an improvement over what we had, and it offered additional features that we previously didn't have at all," said Brendan Putek, director of DevOps for Relay Network. "They offered the integrations that we needed and everything that our previous systems were missing."

Relay Network's AWS infrastructure employs a core series of Amazon Elastic Compute Cloud (Amazon EC2) services for primary backend functions, layered with Amazon Elastic Container Service implementations for AWS Fargate and AWS Lambda. These services scale as needed while being immutable and ephemeral, and SentinelOne's solution was specifically designed to work seamlessly with them. It offers a lightweight approach that maximizes effectiveness for workload protection and autonomous remediation. Unlike previous vendors, SentinelOne could handle the temporary and serverless nature of AWS Fargate and AWS Lambda functions, as well as the frequent rotation of Amazon EC2 instances during deployments. This compatibility was crucial for Relay Network, as its resources are designed to be replaced regularly, either through scaling or as part of its deployment strategy.

To speed implementation, Relay Network secured the SentinelOne solution using AWS Marketplace, which offered flexible deployment options and expedited the procurement process. SentinelOne then set up integrations with Relay Network's existing tools and AWS services, including automated notifications to PagerDuty and Slack, issue creation in Jira, and integration with GitHub. The teams implemented a feature that verifies exploit paths to validate findings and reduce false positives, addressing a significant time-sink in Relay Network's previous security workflow. By integrating the Singularity Data Lake and Purple AI components, SentinelOne provides advanced threat-detection capabilities using natural language queries. This enhances the ability of Relay Network's engineers to respond quickly to potential security incidents.

> "All the technologies in SentinelOne's solution were an improvement over what we had, and it offered additional features that we previously didn't have at all.
>
> **Brendan Putek**
> Director of DevOps

Outcome

100% Visibility Improvement Expedites Threat Detection

Relay Network experienced significant improvements in visibility and operational efficiency. The integration of SentinelOne's products provided a single pane of glass for security management, allowing real-time monitoring and threat detection across Relay Network's AWS-based infrastructure. This resulted in a 100 percent improvement in visibility, and the increased speed of data collection led to more immediate security notifications. The singular viewpoint and integration of other services into the system facilitated a 50 percent reduction in time spent finding security issues, greatly improving efficiency.

The implementation of SentinelOne's Singularity Data Lake as a central data-collection location, coupled with Purple AI, revolutionized Relay Network's threat hunting and investigation processes. The ability to use natural language queries for threat detection and hunting significantly enhanced the team's ability to respond quickly to potential security incidents, decreasing manual threat-detection efforts by 80 percent. "We now have an easier way to obtain and understand findings," said Putek. "It has scaled access and ease of use across teams, and significantly reduced manual effort."

Now, as Relay Network grows, so does its ability to scale securely without adding headcount. "Leveraging the technologies we gained from SentinelOne, we can turn every engineer on our application teams into a part-time security engineer," concluded Putek. "We can now integrate security sooner in development processes, minimizing potential future issues. And with simplified detection through Purple AI, issues we do encounter are easier to find, respond to, and remediate."

These enhancements improved developer satisfaction and agility, resulting in better quality and more timely feature deployments—directly benefiting Relay Network customers. With an improved security posture, Relay Network engineers spend more time innovating and less time troubleshooting, enabling the company to maintain high compliance standards while developing new features rapidly.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733