lastline

Case Study

Major Card Processor Turns to Lastline For More Accurate Threat Detection and Response

The Challenge

Data breaches continue to barrage the financial services industry, especially card processors. Organized crime targets these firms with highly sophisticated attacks designed to harvest credit card data. This high-value data is then sold very profitably on forums on the dark web.

The cost per breach is high for financial firms. The average data breach cost per record breached in the financial industry is approximately 50 percent higher than for other industries. Lack of visibility, lack of automation, and the growing volume of sophisticated attacker activity continue to besiege these organizations' defenders.

The card processor was using virtualized sandbox technology that failed to detect attacks early in the kill chain. Advanced attacker tools were able to circumvent these "legacy" sandboxes and enable successful penetration of the networks. Further, this card processor was faced with a continual increase in cybersecurity expense for basic integrations, which still failed to give them the visibility they required. The result was the continued growth of uncorrelated security alerts that required manual review, limited triage by the security operations center (SOC) team, and a growing number of threats that were successfully entering their networks.

The company began multiple initiatives to identify better alternatives for threat detection and analysis. There was also an executive mandate to increase automation to lower the cost of operations and accelerate response. Further, they found that the cost of the necessary integrations they required had become prohibitive, despite not delivering the value they were promised. Like many other financial services firms, they wanted to reduce the excessive triage associated with wrongly prioritized alerts so that their team could focus on the most dangerous threats.

The Solution

This card processor was introduced to Lastline® at a major security conference. The relationship grew quickly and included a detailed requirements review, during which the Lastline team developed a comprehensive understanding of the card processor's environment and the high-priority challenges they faced. This card processor decided to move rapidly, without the offered trial, to a complete deployment of Lastline to protect both email and web activity.

This card processor deployed three complete instances of Lastline within its systems and networks. Two of those instances reside in data centers, while the third resides in a carefully managed lab test environment. This third deployment is especially crucial, as the financial services provider commonly uses it to test patches and updates to make sure there's no disruption in its production environments. The cybersecurity teams also use the Lastline lab test deployment to measure its response to malware in the lab to better understand the threat and strengthen their assets in critical production environments.

Executive Summary

Industry

Banking and credit card services

Company

- Major banking, payments, and card processor
- Based in the United States
- Tens of million customers

Challenge

- Excessive manual workflow, legacy security technology, and lack of integration resulted in undetected attacks
- Limited ability to scale security staff
- Executive mandate to automate response to attacks

Results

- Accelerated and simplified the organization's incident response processes
- Provided a real-time view into advanced threats
- Greatly increased network visibility into web and email-based activity

Lastline's comprehensive analysis, powered by machine learning and expert systems, delivers a complete and highly correlated view of malicious behavior engineered into threats. Lastline's success with email and web have positioned the company for expanded deployment to protect against additional network-based threats, both on-premise and in the cloud.

> *"Lastline's solutions have dramatically increased our network visibility"*

The Results

Lastline's AI-powered network detection and response (NDR) platform provided visibility into threats that had successfully evaded the company's "legacy" security technology. This significantly reduced the number of attacks that successfully entered the network and enabled the SOC team to more rapidly respond to those threats that did get through.

Lastline's detection accuracy meant the company could automate the response to many threats, eliminating the need to manually analyze and respond to threat, and satisfying the executive mandate for this capability. Improved detection and the automatic correlation of activity from across the network dramatically reduced the number of false positives, enabling the limited SOC team to focus on a significantly shorter list of the most dangerous events.

Lastline Defender™ also significantly improved detection and response of advanced threats by enabling the customer to deploy an unlimited number of lightweight, agentless Sensors across its network. The user-based pricing made it easy to deploy Lastline everywhere the customer wanted increased visibility.

> *"Lastline Defender provided us with a level of visibility to which we've never had access. It gave us a way to peer into the dark corners of our network. Not only that, but it provided us visibility over the CEO's workstation, new business units as well as business transactions between those units."*

About Lastline

Lastline's Network Detection and Response platform delivers the visibility security professionals need to detect and contain sophisticated cyberthreats, on premises or in the cloud. The company's software protects network, email, cloud, and web infrastructures, minimizing the risk of a damaging and costly breach that results in the loss of data, customers, and reputation. Headquartered in Redwood City, California with offices throughout North America, Europe, and Asia, Lastline's technology is used by Global 5000 enterprises, is offered directly and through resellers and security service providers, and is integrated into leading third-party security technologies worldwide.

Request a Lastline demo today

Lastline, Inc.
1825 S. Grant Street, Suite 635
San Mateo, CA 94402

Americas: +1 877 671 3239
www.lastline.com
info@lastline.com