lastline®

SOLUTION GUIDE

AI-Powered Protection for Financial Services Networks

Industry Overview: At the Center of the Bullseye

According to Forbes, financial services firms fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries, and the typical American financial services firm is attacked one billion times per year. In addition, the introduction of new data breach legislation such as GDPR and the California Consumer Privacy Act now require organizations to significantly strengthen their ability to detect and respond to cyberthreats. At the same time, financial services firms are embracing decentralizing their networks and migrating their IT workloads to the cloud, increasing their data protection challenges.

Security Controls Need to Keep Pace

One of the greatest obstacles to securing data the financial services industry faces is the advanced threats that evade detection and operate at will in a network. Attackers engineer the threats to avoid detection, even by next-generation security technologies. For instance, many nation-state actors are now launching targeted attacks that come with payloads that are designed to infiltrate a specific financial institution's network. These threats are developed after patient research of the target organization, its security controls, and those of its network of service providers and vendors. These supply chain attacks enable bad actors to target small, specialized service providers as a means of penetrating larger and better protected financial services companies.

Another reason why these advanced attacks evade detection is the sheer the volume of attacks that financial services security teams face. Their organizations experience thousands of attacks targeting employees, critical infrastructure, systems, and applications every day. This places tremendous strain on the teams, who are likely already working with limited resources in the fight against cybercriminals. Indeed, most regional and branch locations lack advanced security controls; those measures that they do have are notorious for not detecting attacks or for generating false positives when they do generate an alert. The result is that any legitimate alerts of malicious behavior are buried under a mountain of data from across the network.

Some businesses have therefore turned to Network Detection and Response (NDR) or Network Traffic Analysis (NTA) products to enhance their defense-in-depth security strategy and monitor the network for advanced threats and anomalous behavior that other security controls miss. NTA and NDR tools that utilize AI offer the potential for keeping up with the massive volume of data and identifying malicious behavior more accurately through the use of machine learning (ML). Unfortunately, even those technologies that leverage AI more often than not generate low fidelity, probabilistic alerts. This is because simply applying AI techniques to network traffic will eventually find anomalous patterns of behavior within the network traffic, because that's what AI is designed to do. And it is virtually impossible for most AI-based tools to distinguish between malicious or benign anomalies because they lack the context needed to make that decision.

Solution: AI-Powered Network Security

Therefore, in the fight against cyberthreats, financial services companies can't rely on just any AI-based product. Lastline Defender™ is a Network Detection and Response (NDR) platform that detects and contains sophisticated threats before they disrupt your business. It relies on AI and other technologies to deliver the cybersecurity industry's highest fidelity insights into advanced threats entering or operating in your entire network, enabling your security team to respond faster and more effectively to threats.

"Lastline [detected] 4x more attacks than the incumbent solution, reducing challenging response work…the analysis quality is outstanding."

The Lastline Defender platform uses a unique combination of three complementary techniques to detect the advanced threats that other tools miss:

1. Leveraging the Lastline Global Threat Intelligence Network to scan traffic metadata and payloads for variants of known threats
2. Applying unsupervised ML to network traffic to detect protocol and traffic anomalies along with other indicators of compromise
3. Using supervised ML to automatically create classifiers that recognize malicious network behaviors and previously unknown malware.

Together, these three techniques deliver unmatched visibility of malicious behavior across the entire attack chain, enabling under-resourced security teams to stop advanced attacks at multiple stages in the attack chain before they result in a data breach. The Lastline Defender platform monitors network traffic entering and exiting the network ("North-South"), traffic within the network ("East-West"), as well as host activity on the network. It detects the initial network penetration, the malicious activity of the threat as it moves laterally across the network, the anomalous behavior of compromised systems, the large transfers of data across the network, and the external communication with the attacker.

And, as financial organizations migrate workloads to the public cloud, security teams need the same detection and response capabilities for their cloud environments as well. Bad actors target unsecured servers and vulnerable applications, as well as steal credentials to gain access to public cloud platforms. Once they have access, the attackers can launch new instances and move laterally to initiate attacks on other workloads, ultimately harvesting and exporting data. The Lastline Defender platform provides the same ability to stop threats entering or operating within public cloud environments as it offers for on-premises networks, enabling faster and more effective protection of the entire network.

Results

There are four main benefits for financial services organizations to using the Lastline Defender platform over other AI-powered NTA solutions:

1. **Visibility** – The Lastline Defender platform enables the security team to visualize every stage of the attack chain as an attack progresses across the network from initial compromise to data exfiltration for both on-premises and cloud environments
2. **Accuracy** – The Lastline Defender platform offers the highest fidelity detection on the market today, as proven by earning the highest score in NSS Labs' breach detection group test for the last four years
3. **Knowledge** – Backed by our deep expertise on malicious behaviors and the findings of our Global Threat Intelligence Network, the Lastline Defender platform eliminates the need for extensive research by incident response teams
4. **Speed** – Lastline automates network protection by enabling the blocking of threats at multiple stages of the attack chain with its high-fidelity insights and very low false positives. Security teams can also integrate Lastline's high-fidelity insights into incident response workflows and custom applications throughout the organization, whether on-premises or in the cloud, to accelerate and simplify incident response.

Experience the Lastline Advantage

For more information please visit www.lastline.com

Lastline Corporate Headquarters
203 Redwood Shores Parkway, Suite 500
Redwood City, CA 94065

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