CASE STUDY

Global Bank Hardens Defense with AI to Counter Network-Based Adversaries

The Challenge

How does one stop advanced threats? It's not that easy when you're in the financial services industry. Cyber attacks cost financial services firms more to address than firms in any other industry — this is estimated at $18 million per firm. In context, the typical American financial services firm is attacked one billion times per year. Financial organizations experience thousands of attacks targeting employees every day as well as advanced threats targeting their critical infrastructure, systems, and applications.

The risks involving these attacks become even greater for global banking organizations. These large financial entities need to ensure that their security controls are keeping pace with the onslaught of digital threats. Strategies to defend the perimeter with layers of defense-in-depth, which worked well in the past, are no longer reliable. Current events show us that attackers are penetrating these financial networks at an increasing rate. This brings high vulnerability banking applications, SWIFT financial networks, and automated teller machine networks (ATMs) within the reach of bad actors.

Cyber defenders know that it is almost a certainty that an adversary will penetrate an internal network. The challenge today is to rapidly detect them within the networks and then shut them down. Today your strategy must evolve to meet these tough adversaries.

Legacy security tools are often not capable of detecting all of these incoming threats. Most of these systems utilize rules to set the boundary between activity which is acceptable, and that which should generate an alert. If the boundary conditions are set too tightly, then adversaries will penetrate the network. If the boundary conditions are set too loosely, then the volume of alerts is usually unmanageable. This leaves it up to the security teams to spend scarce resources investigating a multitude of false positive activity indicating potential attacks, which wastes lots of time and distracts you from the real threats which you have not yet found.

EXECUTIVE SUMMARY

Industry

Financial Services

Company

Fortune Global 1000 Company

Environment

50,000 employees in North America, Europe, Asia, Latin America

Challenge

- Stop advanced threats that bypass existing perimeter security controls
- Improve visibility of attacks already inside network

Results

- Deployed Lastline Defender™ in blocking mode to stop malicious web traffic and email content before it enters the global network
- Deployed Lastline Defender for network traffic analysis (NTA) to identify lateral movement
- Validated Lastline's AI-powered detection and response

> ***"Lastline helps us sleep better at night — we know that Lastline will detect it"***

One leading financial services company included on the Fortune Global 1000 list deployed various defense-in-depth technologies to counter this problem. These solutions include a next-generation firewall (NGFW), web proxy, anti-spam mail filter, and IPS. But even together, these and other utilities failed to provide an adequate level of protection. They were concerned that attackers could penetrate the network and remain undetected for unacceptably long periods of time. The security operations team (SOC) and the suite of products they deployed could not keep up with the volume of alerts generated by existing tools. They no longer had confidence in those tools' ability to accurately detect all of the threats targeting the bank.

The financial services firm needed a more capable solution to help meet and defeat the advanced threats targeting its network. It was important that the chosen solution provides the necessary protection without disrupting business-critical operations. After considerable research, they decided to deploy a technology utilizing AI-based detection and response technology. This would substantially save their security operations team time in rapidly identifying the active and dangerous threats potentially already within their networks.

The Solution

The bank chose Lastline Defender based on its proven threat detection and response capabilities, powered by supervised and unsupervised machine learning. They deployed the solution in three phases. In the first phase, they used Lastline Defender to detect malicious content hidden within incoming emails, thereby serving as a supplement to its mail server security and anti-spam tools. Lastline Defender was initially deployed in monitoring mode only, but was switched by their security team to blocking mode after the AI-powered solution demonstrated high accuracy and broad detection capabilities.

For the second phase, the bank used Lastline Defender to detect malicious web traffic that bypassed their NGFW and web proxy. As with the first stage, the organization ultimately set Lastline Defender to blocking mode after initially configuring it to only monitor for threats. They did this after they validated that Lastline Defender would not impact legitimate traffic. Lastline Defender technology also demonstrated high competence in detecting sophisticated threats engineered to evade detection by next-generation products, such as fileless malware and polymorphic keyloggers like Emotet.

In the last phase, the financial services firm has expanded the use of Lastline Defender to detect lateral movement in the network by any existing or new threats. These network-resident threats were constantly being introduced by visiting contractors, employees compromised by phishing attacks perhaps via their personal email, or in some cases by visiting malicious websites from home. Lastline Defender generated significantly fewer false positives than the other NTA products evaluated by the team. This high accuracy was extremely important to enable the blocking of internal traffic and reduce the time required by the security team to investigate many spurious alerts.

Results

The financial services firm currently has Lastline Sensors deployed throughout its global network. The security team values the flexibility of Lastline's user-based pricing, which enables it to deploy Sensors across its global network for maximum protection. This arrangement has provided the organization with unparalleled visibility into the complete series of events within an attack chain. For example, Lastline has allowed the firm to see every stage within any given attack — whether a user clicked on the email or executed the attachment, what happened after the attachment executed, whether the compromised host established communication with an external host, whether the attack involved additional accounts or hosts, and any data sets accessed.

Such visibility has also significantly reduced the organization's time-to-respond. Its reliance on the more accurate assessments provided by Lastline Defender to actively block threats before they enter the network has drastically reduced the number of threats entering its network. And Lastline's high-fidelity analysis has freed security professionals from the burden of following up on false positives generated by other tools. Indeed, the financial services firm has already validated Lastline Defender's low false positive rate, which has inspired peace of mind in Lastline's capability to detect and stop legitimate attacks without affecting business operations.

Looking Ahead to the Cloud

The financial services firm is also in the initial stages of migrating some of its workloads to the public cloud. Lastline Defender will be able to keep pace with the organization during this migration because it delivers the same AI-powered NTA protection against threats trying to enter or operate within the cloud environment as it does with on-premises networks. The bank will be able to benefit from unmatched visibility and protection of its entire network, on-premises and cloud, from a single management console.

Harden Your Defense Today

Attackers use different paths to compromise and move around your network. It is critical for a threat detection solution to monitor them all and deliver complete visibility into the entire attack chain, without burying your security team in false positives. Lastline Defender's AI-powered security provides unmatched protection from threats that cross your network perimeter as well as move laterally inside the network for both on-premises and cloud environments.

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

lastline®