lastline

Case Study

Agile Defense Protects High-Profile Department of Defense Agency with Lastline Defender Suite

Reston, Virginia-based Agile Defense is an IT services provider predominantly focused on U.S. government clients, such as the Department of Defense (DoD), and civil agencies, including the Department of State and Department of the Interior. Founded in 1998, the privately held company is renowned for its innovative application of information technology.

Its broad portfolio of highly sensitive government contracts makes Agile Defense a prized target for cyber criminals around the world. Among the many strategies and multiple layers of defense implemented by the company to protect the assets of its clients is the assignment of a designated security manager to key projects.

Filling The Gaps

One of Agile Defense's clients, and the subject of this case study, is a high-profile DoD agency. Brian "Stretch" Meyer – an Agile Defense security manager contractually assigned to the account – describes his responsibilities: "I own the security lifecycle for the unclassified infrastructure at the agency, from the compliance team, to the 24/7 SOC, through to our cyber security engineers and information defense team."

As the designated security manager, Meyer also is accountable for ensuring that there are no gaps or unidentified vulnerabilities in the defenses of his assigned agency. The NIST and MITRE ATT&CK cyber security frameworks are utilized to determine readiness, with a focus on security controls and associated assessment procedures.

In addition to the classified work it does on highly secretive DoD projects, the agency also participates in many initiatives that are unclassified – and operates many public-facing servers that are used for hosting its numerous websites. "We have to ensure that anything that comes into the agency's building – such as files, email messages, and attachments – cannot move laterally to gain access into the network," stated Meyer. "However, if something does break through, it is imperative that we can isolate it quickly and rapidly understand where it's been and what it was attempting to do."

Enter Lastline Defender

The Lastline Defender suite has become one of the security professional's go-to solutions. He commented, "We use Lastline to look at everything that's happening across the agency's network layer. It intercepts all the traffic that comes into their email servers and we force potentially malicious executables through Lastline to determine their intent before any damage can take place."

He noted, "A lot of people still don't have effective security for their email channel. Lastline helps us to do a really good job at knowing what's coming in and out of the agency's mail gates."

Green Light for Lastline

For Agile Defense, working with government agencies dictates that the selection of any solution or service needs to be a highly structured and defensible process. The company has to document its evaluation criteria and demonstrate that the selected option was irrefutably the best candidate when measured against the requirements.

The selection process typically involves an initial phase of market research, followed by a period of due diligence to find the strongest candidates. Lastline Defender was selected for the final group of solutions, being joined by a leading sandbox solution and a leading firewall offering.

Although not an Agile Defense employee at the time of the evaluation, Meyer familiarized himself with archived documentation from the comparison testing. "We defined multiple categories to assess the qualities of each candidate, but the key questions were:

- How proficiently does the product use threat intelligence?
- Could it determine root cause?
- Did it give us visibility into the lateral movement of spreading infections?
- Would it integrate into the existing security stack?"

Executive Summary

Industry

Government

Company

Agile Defense/ High-Profile Department of Defense Agency

Description

IT consulting provider offering security solutions, network engineering and system integration services to U.S. government agencies and departments.

Challenge

Enhance capability to support rapid resolution of potential threat activities across agency's infrastructure

Solution

Lastline Defender

Results

Attained ability to expediently detect, contain and remediate threats through heightened visibility and accuracy

"There is no doubt in my mind that Lastline helps us keep ahead of the threat curve."

- Brian "Stretch" Meyer, Security Manager, Agile Defense

Use Case	Leading Sandbox	Lastline	Leading Firewall
API Integration with custom apps	✓	✓	✓
Enterprise Email Submissions (Inline)	✗	✓	✓
Enterprise Email Submissions (Passive)	✓	✓	✓
Enterprise Web Inspection	✓	✓	✗
Manual Submission	✓	✓	✓
File Analysis Capabilities	**Leading Sandbox**	**Lastline**	**Leading Firewall**
CPU Level Inspection	✗	✓	✗
PCAP Inspection	✗	✓	✓
Win10 and MacOS Sandbox	✓	✓	✗
Export STIX IoC Data	✗	✓	✓
Ability to Hash Latent Functions/Behaviors	✗	✓	✗
Max File Size > 10MB	✓	✓	✓
Ability to Handle Nested Zip Files	✓	✓	✓
Integrates with Existing Security Stack	✗	✓	✓

"Seeing the solid column of green squares made it immediately obvious that Lastline had prevailed over its two competitors! There were a handful of tests where all three passed but the majority of rows graphically demonstrated the superiority of Lastline Defender against the competition."- Brian "Stretch" Meyer

SIEM Integration Accelerates Workflow

The alerts generated by Lastline Defender are channeled into the agency's SEIM and the SOC team uses the dashboard to view the indicators and prioritize what they work on first. "One of the beauties of Lastline is that its network analysis provides us with all the data and metadata needed to get full visibility into any lateral movement and understand exactly what's occurring throughout our infrastructure," enthused Meyer.

Expediency is always a priority when dealing with potential breaches. "Without Lastline, we'd have to manually search the agency's entire email system and then look at the logs for each portal. With Lastline, because we get a copy of all the data going across the network, it immediately reveals the path the file took and quickly enables us to recreate the full lifecycle of the threat. Lastline makes it possible to complete a cleanup action within 10 to 15 minutes, whereas before it could have taken hours."

He continued, "In addition to its network analysis capabilities, we frequently use Lastline Defender for file analysis. If we're ever unsure about a file or executable, we just shoot it to Lastline and get a detailed report of exactly what the code intended to do. We don't have any other tool that can do this."

Ease-Of-Use

As with any SOC team, the agency's analysts come with a wide range of experience: "A lot of tools are ambiguous and hard to understand, especially for newer or less knowledgeable members of the group," Meyer observed. "However, the Lastline user interface makes it really easy for everyone to know what they're looking at. There's even a visualization capability that produces a bubble chart to identify everything a malicious file has touched and the route it took as it traversed our environment."

A Great Company To Do Business With

"One of the ways Lastline differentiates itself from the competition is that the company is very good about listening to its customers. We've shared ideas about various capabilities we'd like to see in the future and the requests have been quickly worked into the development lifecycle," recounted Meyer. "Lastline is also very approachable and easy to work with. The staff has really helped with architecting how to successfully deploy Lastline Defender in the agency's very unique environment."

Meyer concluded, "There is no doubt in my mind that Lastline helps us keep ahead of the threat curve."

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

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