lastline

Case Study

Accuracy and Value of Lastline Defender Prove Compelling for Prominent U.S. Department of Defense Contractor

Headquartered on the U.S. east coast, this high-profile Department of Defense contractor delivers many hundreds of millions of dollars of solutions and services to all branches of the country's armed forces as well as friendly governments around the globe. As a major supplier of some the world's most innovative and impactful military systems, the company is always a target for sophisticated, well-funded commercial and nation-state cyber criminals.

Out With The Old

Staying ahead of the onslaught of cyber attacks requires perpetual diligence to ensure that the optimal defenses are always in place. The company had routinely relied on protection from industry traditionalist FireEye but an ongoing initiative to up-level its security posture caused questions to be raised about continuing to preserve the status quo.

The DoD contractor's director of corporate security explained, "We are constantly trying to gain better visibility into our network and endpoints. We got to the point where we started to remove the FireEye services because they just weren't keeping up with our growing set of requirements to increase security hygiene across our infrastructure."

Lastline In, FireEye Out

By the summer of 2018, the only FireEye component left in the contractor's environment was for securing email traffic. With planning taking place for the new budgetary year, a decision had to be made to either keep the one remaining FireEye appliance or replace it with an alternative platform. "We approached our MSSP for possible solutions to protect our email channels and the recommendation was that we look at Lastline," recalled the director.

Having confirmed the reasons behind the MSSP's endorsement, the contractor's security team executed a POC to make a direct comparison of Lastline Defender and FireEye. "When we looked at the two solutions side-by-side, we could tell that Lastline was hitting everything that FireEye was catching, but with a better false positive rate," the director noted.

He continued, "When we then started talking about pricing, Lastline Defender came out significantly more cost effective. Not only that, it offered us a lot more flexibility to easily expand the protection across our environment as we grow. With FireEye we were always having to cut a check for a new appliance or sensor; the Lastline pricing model enables us to immediately extend the deployment as much as we want without always having to go through a procurement cycle."

> *"We decided that deploying Lastline in place of FireEye was the perfect solution for us."*

A Need For Visibility, Flexibility And Scalability

Following the success of implementing Lastline Defender for email protection, attention was given to further leveraging the solution's comprehensive capabilities to protect the contractor's extensive network infrastructure. The director of corporate security elaborated, "A big driver was that we have a long history of acquiring other companies. we now use Lastline also to quickly get visibility into the acquisition target's network before we commit to a full integration. We are frequently able to pinpoint questionable traffic that would otherwise have gone unseen and are then able to address the source of the vulnerability before the domain gets added to our own network."

Executive Summary

Industry

Government

Company

U.S. Department of Defense Contractor

Description

Leading supplier of products and services to military forces and intelligence agencies around the world

Challenge

Replace FireEye appliances with an easy to deploy, high-fidelity solution for email and network protection

Solution

Lastline Defender

Results

Elevated visibility and accuracy across infrastructure, plus flexible, scalable deployment capabilities

"We decided that deploying Lastline in place of FireEye was the perfect solution for us."

-Director of Corporate Security, Large U.S. Department of Defense Contractor

Together As One

Lastline Defender offers a choice of deployment options that enable customers to tailor implementations to suit the characteristics of each environment. "We opted to go with virtual appliances for our primary datacenters: Implementation was straightforward, and we were able to get operational really quickly," described the director. "The unified console brings everything together and works seamlessly across the different sensors and threat vectors."

As a veteran of the IT and security world, the director of corporate security has experience with many vendors. He reflected, "It has just been wonderful working with our account team. With multiple companies that I've worked within the past, there always seems to be a honeymoon period where you initially get a lot of attention but the relationship frequently goes stale. With Lastline, the team has always been very engaged and aligned with what we're doing and where we want to go. Partnering with Lastline has been great."

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. Heaadquartered 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

© 2019 Lastline, Inc. All rights reserved. Lastline and the Lastline logo are registered trademarks, and Lastline Defender is a trademark, of Lastline, Inc. All other trademarks are the property of their respective owners. Lastline technology is protected by U.S. Patents 8910285 and 9361459. Additional patents pending. | v.102019