lastline®

CASE STUDY

Lastline Helps Tech Leader Gain Visibility of Complex Network Threats

The Challenge

One of the biggest digital security challenges facing organizations today is how to obtain network visibility. They need to be able to see this network traffic. Otherwise, there's no way to detect and block threats that are seeking to use their network for malicious ends.

This obstacle was especially pertinent for an industrial and engineering technology organization that serves hundreds of customers in over 60 locations worldwide. Through a series of acquisitions, the network topology of this technology leader grew in size and complexity. Its network took on multiple legacy pathways, for instance, and strict customer segmentation resulted in different access control lists and network traffic flows. Needless to say, the organization was struggling to figure out what exactly was going on inside of its network.

It wasn't long before the tech leader realized something needed to change. On the one hand, the organization knew it needed to monitor its complex network topology as well as protect customer data and IP stored on-premises in offices located across the United States and internationally, all while complying with government-specific regulations. On the other hand, it knew it would be difficult to navigate the ongoing skills shortage in digital security and ultimately get the right people in the right positions. Therefore, in order to make security less cumbersome, the company decided it would use technology to empower analysts to respond to potential security threats as quickly as possible.

In this mindset, the technology leader contacted Lastline® after learning of the company's reputation and of its Lastline Defender solution. The organization evaluated Lastline via a Proof of Concept (POC) implementation and found its security solutions met its criteria, particularly in terms of ease of implementation. As a result, it decided to implement Lastline Defender across its complex, multi-national network.

"Our POC implementation of Lastline Defender was by far among the easiest and fastest technologies which I've tested in the past five years."

EXECUTIVE SUMMARY

Industry
Industrial and engineering technology organization

Company
A technology leader with over 10,000 employees that offers a full suite of design, engineering, and staffing solutions for a wide variety of industries spanning aerospace and defense, automotive, and industrial.

Challenge
Gain visibility of complex network topology in order to effectively defend against threats

Serving hundreds of customers in over 60 locations worldwide

Results
POC of Lastline Defender™ quickly provided visibility into data flows

Solution responded appropriately to test malware deployed in network

Full migration to production environment forthcoming

Scoring of Lastline Defender (1 - 5)

Ease of Deployment	★★★★★
Satisfaction (Full migration outstanding)	★★★★
Value for Money	★★★★★

The Solution

For the POC, the company deployed sensors and installed several servers. Within a matter of days, the organization began seeing data flows, which improved its visibility of its network overall.

"Lastline's malware detection capabilities add value because they helped us pinpoint where risks are much more quickly than if you were just leveraging logs and sifting through correlated data, such as what's provided by a SIEM. And Lastline Defender's ease of use can't be beat, either. I found this particular POC implementation to be the easiest and fastest of these technologies I've tested in the past five years."

Results

After deploying Lastline Defender, the organization put out a fake piece of malware to see how the technology would respond. The security team was pleased to see the software take the necessary and appropriate action against the test malware. Given these results, the company is confident that it will gain even more visibility as it begins moving Lastline Defender to the rest of its production systems.

"Lastline's solution was quick to provide results of a particular issue that an analyst would have otherwise needed to pinpoint. Basically, everything can be automated with Lastline, so you can get data back in a manageable form and report out what you need to report. This has saved us a lot of time so far—likely an hour at least per each scenario."

Summary

If you don't have network visibility, there's no way you can know what you don't know. That's a scary thought.

Overall, most people feel that their existing tools give them the needed visibility. But this visibility is oftentimes insufficient. While organizations might have some visibility with certain tools, they might not have complete visibility unless they're knowledgeable of their entire infrastructure and are capturing all of those data flows. Things change constantly on the network, and when that happens, blind spots are created. That explains why organizations need a simple yet sophisticated piece of technology like Lastline Defender that can help them obtain comprehensive visibility into network activity and malicious network behavior.

"If you're looking to get good network visibility with a solution that's easy to deploy and uses little-to-no bandwidth, Lastline's solution will get you there very quickly."

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.

Request a demonstration today, or visit www.lastline.com to learn more.

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

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