lastline

Case Study

World-Renowned Innovator Turns to Lastline to Help Protect Global Infrastructure

The Challenge

Continuous innovation has made this multinational giant one of the world's most recognizable names in both commercial and consumer domains. The company's revenues—annually running at many tens of billions of dollars—are derived from a diverse portfolio of products and solutions, including aerospace, automation, safety and materials technologies.

With several hundred thousand endpoints, spread around the globe, the company's attack surface is vast, complex and continuously changing. Protecting the huge volumes of personal information and commercially sensitive data spread across the entire infrastructure has become a company-critical objective. To combat the continually escalating barrage of cyber-related threats, a centralized team of security experts was assembled to safeguard the corporation's digital assets.

The manager of the cyber security team gave insight into the magnitude of the challenge that his group faces, "We've created almost 30,000 firewall rules and process about 400 terabytes of event-related data each year."

To deliver homogenized protection across its expansive global environment, the company uses the NIST security framework – from the US-based National Institute of Standards and Technologies – as one of the foundation layers of its security strategy. "We combine the NIST requirements, along with our own internally-created standards and other compliance and regulatory mandates, to ensure that we have comprehensive coverage across the entire infrastructure and across all threat vectors," the team manager confirmed.

The Solution – A Long-Standing Relationship with Lastline

A key component in the company's security architecture has been the ability to quarantine code and move it to an environment where the intentions of malware can be investigated without risk to the rest of the infrastructure. "Lastline has been our go-to solution for detonating and analyzing files since 2014," the manager stated.

The Lastline solution provides cyber security teams with a completely safe environment to submit files and URLs for comprehensive evaluation. The Lastline detection engines utilizes Deep Content Inspection™ to simulate an entire host environment and trigger any embedded malicious behaviors. Examination results are summarized in an in-depth report that itemizes the malware's interactions with all elements of the replicated environment, including CPU, memory, networking and storage.

Executive Summary

Industry

Engineering and manufacturing

Company

Multinational conglomerate

Challenge

Create ability to isolate and safely investigate potential malware occurring anywhere across global infrastructure

Results

Malicious content comprehensively analyzed in cloud-based simulated host environment

"Lastline is a solution that delivers what we need, without any complications or unnecessary overhead: It really adds value."

- Cyber Security Team Manager, Multinational Conglomerate

"I view Lastline like a Swiss Army knife: It has great capabilities and functionality."

The Results

Flexible And Efficient

One of the key factors in the company's many decades of success has been strategic growth: achieved organically and through acquisitions. The effect of this is that every component in the NIST-compliant security stack has to be able to accommodate a constantly changing environment. "We have a very dynamic infrastructure and Lastline seamlessly handles the volatility," reflected the manager. "It also offers flexible deployment options: We have the cloud version and it is ideally suited for our global operations. It's extremely scalable."

"For a corporation of our scale, our cyber security team is very modestly sized: This means that all the tools we use have to be easy to support and maintain. We feel very aligned with Lastline and how the solution has evolved. The Lastline cloud implementation only requires minimal support: For a lean team like ours, this is a critical attribute."

Ease of Use

The results of each analysis delivered to security specialists by the Lastline solution contain all the artifacts and discovered attributes, including any additional executables, indicators of compromise, targeted services, and related network traffic. However, despite its sophistication, Lastline is refreshingly simple to use: "We've had several new team members join us in the past few months and they have all become fully proficient with it in an impressively short period of time," reflected the manager.

"Our Lastline team is always very receptive to feedback and willing to answer questions: They make us feel that we have chosen the right product and the right set of people to work with. Lastline is a solution that delivers what we need, without any complications or unnecessary overhead: It really adds value."

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. Headquartered 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