

Lastline Detonator: Make Your Endpoint and Network Security Tools More Effective

Add Advanced Malware Detection to Existing Security Tools

Lastline® Detonator integrates Lastline’s unique advanced malware detection capabilities seamlessly into your existing security products. You can quickly instrument your network, endpoint, and custom applications to detect and respond to advanced threats.

The Threat Visibility You Need

Lastline Detonator detects the advanced malware that is engineered to defeat “advanced” or “next-generation” enterprise security tools like sandboxes, firewalls and intrusion prevention. Lastline Detonator delivers complete visibility into advanced malware, enabling your security team to respond rapidly to malicious activity before it results in a damaging data breach.

Your third-party products automatically submit unknown files to Lastline’s threat detection engine for analysis, deployed on-premise or in Lastline’s cloud. It evaluates those files for malicious content, and provides you with the threat information to incorporate the results into workflows and policies. You receive high-level, actionable threat intelligence as well as detailed host and network indicators of compromise (IoCs).

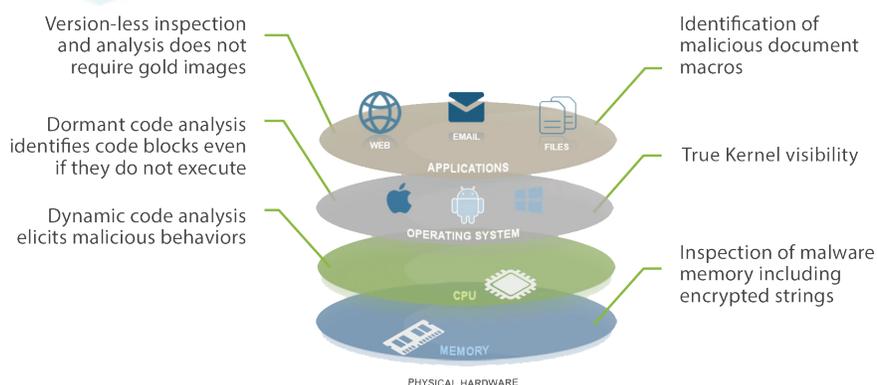
Unmatched Detection with Deep Content Inspection

Lastline’s detection engine provides complete visibility into the malware behavior that other technologies miss. It uses Deep Content Inspection™, a unique isolation and inspection environment that simulates an entire host (including the CPU, system memory, and all devices) to analyze malware. Deep Content Inspection interacts with the malware to observe all the actions a malicious object might take.

The Lastline detection engine provides complete visibility into all aspects of the malware. It interacts with the malware to elicit malicious behavior, including identifying dormant code and documenting all CPU instructions executed. It also identifies the memory (RAM) locations accessed by the artifact being analyzed.

Other malware detection technologies like sandboxes only have visibility down to the operating system level. They can inspect content and identify potentially malicious code, but they can’t interact with the malware like the Lastline detection engine can. As a result, they have significantly lower detection rates and higher false positives, in addition to being easily identified and evaded by advanced malware (advanced threats evade other sandboxing technologies by recognizing sandbox environment or using kernel-level exploits).

DEEP CONTENT INSPECTION DELIVERS UNMATCHED VISIBILITY



Global Threat Intelligence Network

The Global Threat Intelligence Network automatically shares the malware characteristics, behaviors and associated IoCs of every malicious object curated and analyzed by Lastline with all Lastline customers and partners.

We quickly analyze all new objects and share the results of the analysis across our entire network. This allows for faster detection and analysis of previously unseen threats as well as reducing the time for you to respond to malicious activity.

Lastline continuously updates the Threat Intelligence Network in real-time with intelligence from partner and customer environments around the world.

Flexible Cloud and On-Premise Options

You can access Lastline Detonator through either an on-premise deployment or the Lastline cloud, giving you maximum flexibility to meet your unique requirements. For example, if you have to meet strict data privacy laws and policies, you can deploy Lastline Detonator on-premise in your data center.

Your deployment will regularly download threat intelligence updates from Lastline, to ensure your threat detection capabilities are armed with the most recent threat data.

GLOBAL THREAT INTELLIGENCE NETWORK SUBSCRIPTION INCLUDES:

- Active command and control (C&C) servers
- Objects with zero-day exploits
- Toxic websites and malware distribution points
- Other malware information useful to defend against threats specific to your organization

Lastline continuously updates the Threat Intelligence Network in real-time with intelligence from partner and customer environments around the world.

Experience the Lastline Advantage

For more information please visit www.lastline.com

LASTLINE CORPORATE HEADQUARTERS
203 REDWOOD SHORES PARKWAY
SUITE 620
REDWOOD CITY, CA 94065

AMERICAS: +1 (877) 671 3239
EMEA: +44 (0) 207 749 5156
APAC: +65 6829 2207
WWW.LASTLINE.COM

