DATA SHEET

Lastline Analyst: Give Your Incident Responders the Information They Need

Comprehensive Analysis of Advanced Malware

Lastline® Analyst is a complete malware analysis system for your threat analysts and incident response teams. It safely executes malware samples, analyzes URLs, and provides complete visibility into malicious behavior.

Your threat researchers can use Lastline Analyst to analyze malicious objects used in advanced, targeted and zero-day attacks safely and efficiently.

Complete Visibility

Lastline Analyst enables your researchers to submit files (including pcaps) and URLs to the Lastline detection engine for comprehensive analysis. It identifies malicious behavior and fileless web threats. It catalogs the malware's interaction with the operating system, processes and applications, as well as the network.

Lastline Analyst presents the malware behavior in detailed, in-depth reports that include all artifacts discovered during the analysis, such as additional executables and captured network traffic.

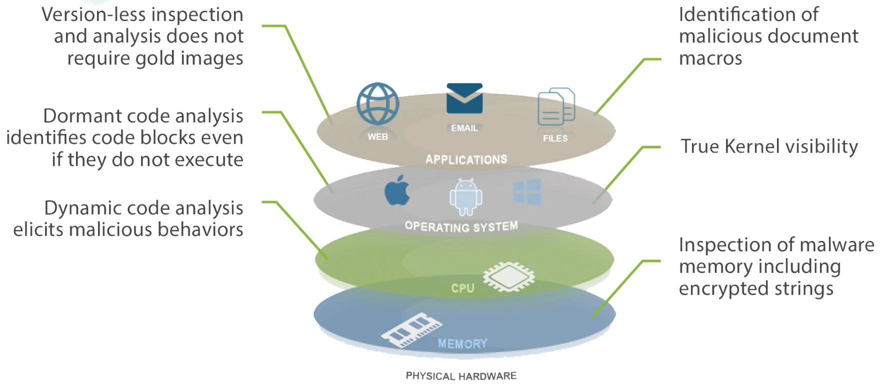
Unmatched Detection with Deep Content Inspection

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



Version-less inspection and analysis does not require gold images

Dormant code analysis identifies code blocks even if they do not execute

Dynamic code analysis elicits malicious behaviors

Identification of malicious document macros

True Kernel visibility

Inspection of malware memory including encrypted strings

Identify Indicators of Compromise

Lastline Analyst supplies your researchers with the detailed indicators of compromise (IoCs) they require when researching a piece of malware. Critical malware attributes provided by Lastline Analyst include:

- **Malware Information** – Malware name and category, evasive actions, mutex activity, contents of the malware memory, applicable screenshots, files and registry keys that the malware accesses
- **System IoCs –** Process dumps, files and registry keys that the malware writes, malware filename, command line and hash information
- **Network IoCs** – IP addresses and domains to which the malware connects, TCP/UDP port activity, DNS requests and network packet capture

Global Threat Intelligence Network

In addition, your threat analysts and incident response team can subscribe to the Lastline Global Threat Intelligence Network, for faster response to previously unseen threats. It contains the malware characteristics, behaviors, and associated IoCs of every malicious object curated and analyzed by Lastline.

Flexible Cloud and On-Premise Options

You can access Lastline Analyst through either an on-premise deployment or the Lastline cloud, giving you maximum flexibility to meet your unique requirements.

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

lastline™