lastline

# Lastline Analyst

## Advanced malware analysis for forensic and incident response teams

### Highlights

- High-resolution analysis to counteract malware evasion techniques
- Safe execution and analysis of malware samples
- Detailed, easy-to-understand reports reveal hidden malware behavior
- Analyzes executable files, MS Office documents, PDF documents, Java, Javascript, Flash and Web code
- Turn-key, no-configuration deployment
- Easy-to-use web-based console
- Flexible data access and export via API
- Deploy on premise or host in Lastline's cloud

### Overview

Lastline Analyst provides threat analysts and incident response teams with an advanced malware analysis system to safely execute malware samples, dissect their actions and understand their behavior. Lastline Analyst is built on top of years of research to identify and analyze evasive malware and web threats.

Lastline Analyst can be used to analyze malicious components used in advanced, targeted and zero-day attacks safely, efficiently and with complete privacy.

### Look Inside Modern Malware

Lastline Analyst is a component of the Lastline Breach Detection System, an advanced malware analysis environment that provides security researchers and analysts with complete visibility into the actions of analyzed malware. The Lastline malware analysis engine relies on full-system emulation (rather than virtualization or bare-metal execution) to inspect every single instruction executed by the sample under analysis. This method of inspection enables more in-depth and sophisticated analysis, such as tracking data flows and counteracting evasion techniques. In addition, the Lastline Analyst supports the analysis of malicious web sites and identification of web-based exploits including obfuscated JavaScript.

### Discover Malware Behavior

Lastline Analyst enables researchers to submit files and URLs for further analysis. Lastline identifies critical malware behavior, focusing on the malware's interaction with the operating system and the network. The malware under examination runs inside a realistic environment, pre-configured with popular applications and data (password files, decoy documents), which elicits the full set of behaviors from malware. Lastline Analyst presents the malware behavior in detailed, in-depth reports that include all artifacts discovered in the course of the analysis, such as additional executables or captured network traffic.



**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

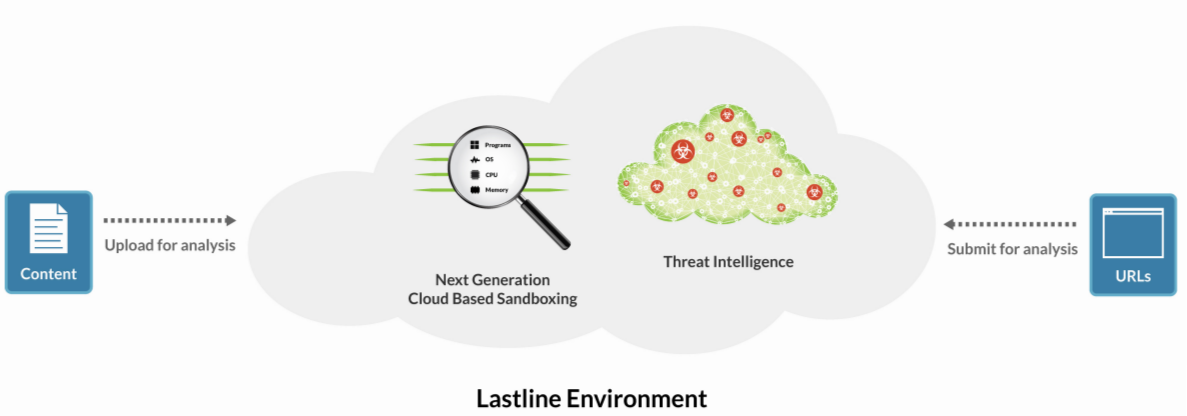
www.lastline.com

## Identify Indicators of Compromise

Lastline Analyst supplies researchers with the detailed indicator of compromise (IOC) data 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 malware accesses
- **System IOCs –** Process dumps, files and registry keys that malware writes, malware filename, command line and hash information
- **Network IOCs –** IP addresses and domains the malware connects to, TCP/UDP port activity, DNS requests and network packet capture

The Lastline Knowledge Base (LLKB), Lastline's complete and structured repository of malware data, can be used to complement Lastline Analyst by providing search tools to query through any combination of malware attributes.




**Lastline Environment**

## Flexible Hosted and On-premise Options

Lastline Analyst can be accessed through either an on-premise solution or through a hosted option. If your Enterprise is restricted by strict privacy laws and policies, deploy on-premise and install in your data center. Network behavior models associated with malware will be regularly downloaded from Lastline. Alternatively, choose the hosted deployment model and quickly deploy in Lastline's cloud.

### About Lastline, Inc.

Lastline is innovating the way companies detect active breaches caused by advanced persistent threats and evasive malware with its software-based Breach Detection Platform. Lastline's open architecture integrates advanced threat defenses and intelligence into existing operational workflows and security systems. Inspection of suspicious objects occurs at scale in real-time using a full-system emulation approach to sandboxing that is superior to virtual machine-based and OS emulation techniques. Lastline's technology correlates network and object analysis to achieve timely breach confirmation and incident response. Lastline was built by the creators of Anubis and Wepawet, who have pioneered novel malware detection techniques, alongside industry veterans with decades of experience focused specifically on advanced breach weaponry and tactics.

Lastline is headquartered in Redwood City, California with offices throughout North America, Europe and Asia. Lastline's platform is used by global managed security service providers, Global 2000 enterprises, and leading security vendors worldwide. To learn more, visit www.lastline.com.



**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