Lastline Defender for Customer-Managed Email

Network Detection and Response Platform

Lastline Defender™ for Customer Managed Email is part of Lastline Defender, a comprehensive Network Detection and Response (NDR) platform that detects and contains sophisticated threats before they disrupt your business. It delivers the cybersecurity industry's highest fidelity insights into advanced threats entering or operating in your entire network, enabling your security team to respond faster and more effectively to threats.

Advanced Email Threats Continue to Evade Detection

Most email security controls are only marginally effective in combating advanced threats such as ransomware, phishing, fileless malware, and keyloggers. Email-based attacks have been the number one source of threats for years and succeed because threat actors are able to develop new techniques that bypass both traditional and next-generation email security controls.

Attackers understand the limitations of tools that rely on signatures and use a range of transformation techniques to alter the signature of a file, including:

- Code permutation to make slight alterations to critical elements of malicious code
- Registry alteration to avoid detection by 3rd party tools
- Code insertion or other constructs to change the file hash in order to overcome simplistic detection mechanisms used by most vendors
- Code obfuscation techniques to hide malicious code

Some malicious code can recognize when it's in a virtual environment such as a sandbox. It avoids taking malicious actions until it's released from the virtual environment and allowed to enter the network. The malware uses a range of techniques to identify virtual environments, including:

- Examining registry keys for values that are unique to virtual environments
- Looking for the installation of software packages that are unique to virtual environments
- Checking for processes and services that are unique to virtual environments
- Examining specific hardware parameters that are unique to virtual environments.

Unmatched Email Threat Visibility Powered by AI

Lastline Defender works with your existing email system, whether it is in the cloud or on-premises, to provide high-fidelity visibility and optional blocking of sophisticated email threats attempting to enter your network. Lastline Defender analyzes attachments, message headers, and the body of the email and examines the destination of any URLs in the email body or attachments for malicious content and behavior.

Lastline's patented, AI-powered analytics performs several functions to deconstruct an unknown file or link and provides visibility the SOC Teams lacks by providing detection capabilities that can:

- Imitates a complete operating system, including the hardware, software and network environment in order to deliver unmatched visibility into any malicious behavior engineered into a file or email message
- Identifying all programs and services invoked, all operating system functions, and all kernel activity
- Analyzing the actions of every malicious behavior, including all CPU instructions, memory locations accessed and content, peripherals used, and network connections made.

High-Fidelity Alerts Eliminate Blind Spots

Lastline Defender correlates activity to link isolated events into an attack chain so that your SOC team can see the complete scope and objective of an attack. This eliminates the need for your SOC team to try to piece together siloed, incomplete alerts.

Lastline Defenders provides your SOC team or email security administrator with the tools they need to:

- Understand the inbound threats targeting their users
- Recognize the impact on a particular email campaign
- Understand the impact of email threats within the context of network threats when using the full Lastline Defender NDR platform

Detection You Can Act On

You can rely on Lastline Defender's high-fidelity insights to automate response and eliminate time-consuming manual investigations of unknown files and anomalous activity in your email:

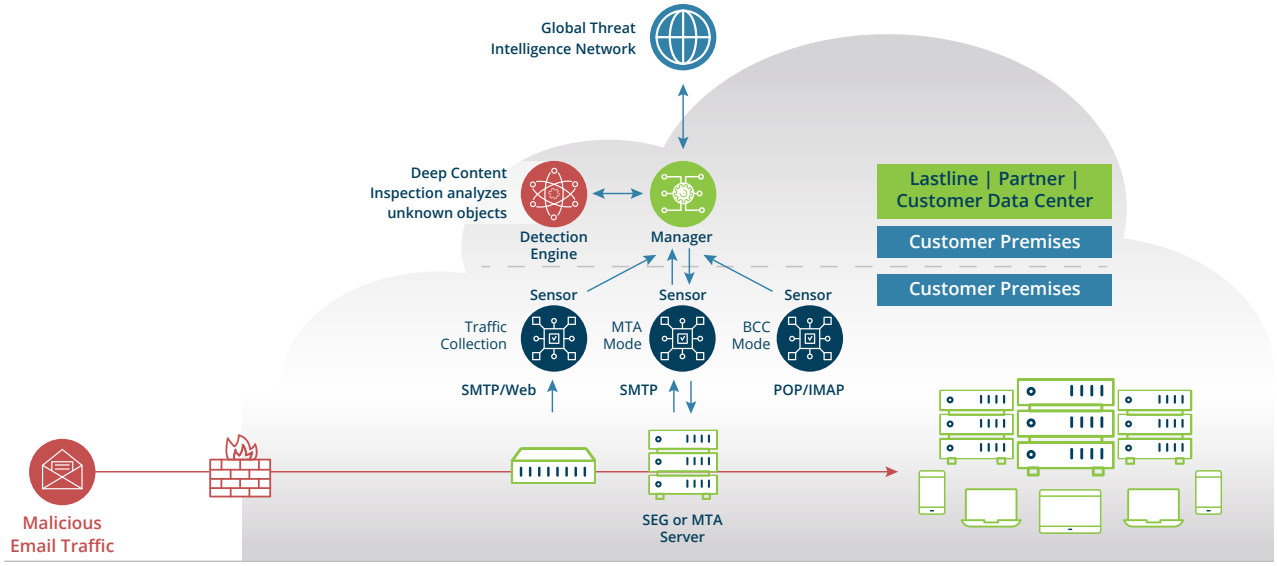
- Deploy Lastline Sensors in BCC mode to stop malicious content at the perimeter.
- Integrate Lastline Defender with your third-party products such as SEG, SIEM, SOAR, custom applications, and incident response workflows throughout your organization to automate response to email-based threats.

When integrating Lastline Defender with your existing email protection and other security controls, you have the choice of using built-in integration offered by our technology partners or using our robust APIs to optimize your existing technologies, staff, and processes.

Improved Email Security without Complexity

Lastline Defender gives you the ability to protect your on-premises or hosted email service with a complementary layer of defense to enhance your existing investments regardless of where they live--on premises or in the cloud.

The Lastline architecture delivers maximum protection while giving you deployment flexibility and low TCO.



You have several options to complement your email system with Lastline Defender:

- **MTP Monitoring Mode** – Monitor Simple Mail Transfer Protocol (SMTP) traffic on a network segment and analyze attachments for all inbound emails
- **MTA Mode** – Route emails to the Lastline Defender Sensor with or without email delivery
- **BCC Mode** – Forward emails to an account and allow the Sensor to retrieve them via IMAP or POP

Option	Detect or Block?	In-Line?
SMTP Monitoring	Detect Only	No
MTA Mode with Email Delivery	Detect and Block	Yes
MTA Mode without Email Delivery	Detect Only	No
BCC Mode	Detect Only	No

Upgrade Your Email Protection Today

It takes only a few minutes to add Lastline Defender for Customer Managed Email protection to your email systems. Once you do, you'll be protecting your users from sophisticated threats attempting to disrupt your business. Lastline Defender for Cloud Email delivers the cybersecurity industry's highest fidelity insights into advanced threats targeting email systems, enabling your security team to respond faster and more effectively.

	1G Sensor	10G Sensor	Manager	Detection Engine
Base Model	**Dell PowerEdge R440**			
Processor(s)	1 Xeon® Silver 4114	2 Xeon® Silver 4114	1 Xeon® Silver 4114	1 Xeon® Silver 4114
RAM	32 GB	128 GB	64 GB	64 GB
Hard Disk Drive	2 x 1 TB, 3.5 SATA HDD (7.2K RPM)	2 x 1 TB, 3.5 SATA HDD (7.2K RPM)	4 x 2 TB, 3.5 SATA HDD (7.2K RPM)	2 x 1 TB, 3.5 SATA HDD (7.2K RPM)
Software RAID	1	1	10	1
Internal Controller	PERC H730p			
Network Adapter	Intel I350 Quad port	Intel X710-DA2	Onboard	Onboard
Support Plan	ProSupport Enterprise			
Form Factor	1U Rack-Mount			
Weight	43.87 lbs (19.9 Kg)			
Dimensions (Width x Depth x Height)	17.1" x 25.9" x 1.7" (43.4 x 65.7 x 4.3 cm)			
Enclosure	Fits 19-inch Rack			
Monitoring Ports	(4) 1 GbE Ports***	(up to 4) 1 GbE (up to 2) 10 GbE Ports***	-	-
Management Port	1 GbE Port			
AC Input Voltage/Current	100~240 VAC / 6.5 A-3.5 A			
Power Supply	Dual Hot Plug Power 450 W			
Operating Temp	10° C to 35° C (50° F to 95° F)			
Network Performance	Up to 1 GB Traffic	Up to 4 GB Traffic	-	-
Objects Per Day**	Up to 100,000 per day*		-	-
Files Analyzed	-	-	-	Up to 10,000 per day*
Scalability of Engines	-	-	Up to 30 Engines per Manager	-
Scalability of Sensors	-	-	Up to 200 Sensors per Manager	-

Lastline Corporate Headquarters
1825 S. Grant Street, Suite 635
San Mateo, CA 94402

Americas: +1 (877) 671 3239
www.lastline.com
info@lastline.com

© 2020 Lastline, Inc. All rights reserved. Lastline and the Lastline logo are registered trademarks, and Lastline Defender is a trademark, of Lastline, Inc. All other trademarks are the property of their respective owners. Lastline technology is protected by U.S. Patents 8910285 and 9361459. Additional patents pending. | v.012020