Lastline Defender

Network Detection and Response Platform

Lastline Defender™ is a 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.

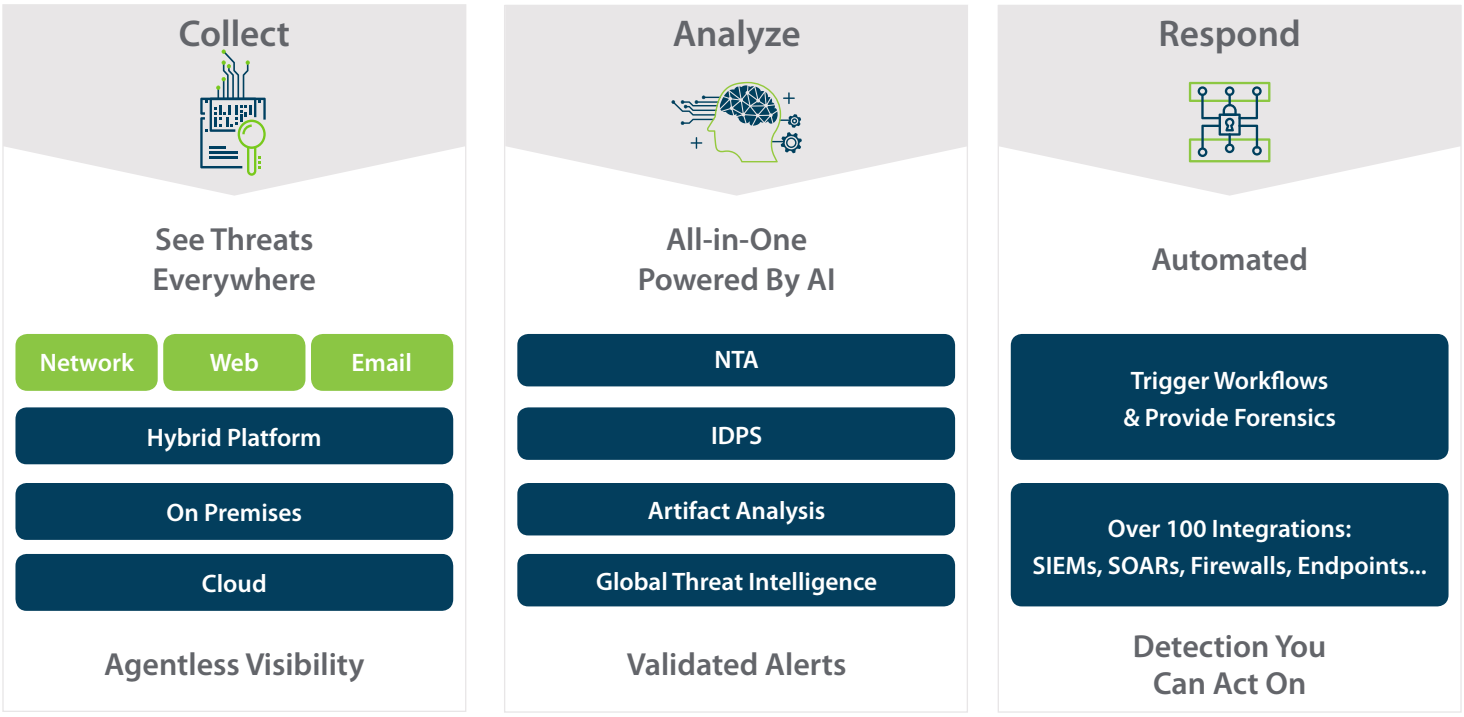

Figure 1: Lastline Defender Network Detection and Response Platform

Agentless Visibility for Your Entire Network

You can protect network, web, and email traffic with Lastline Defender's agentless, cloud-based architecture. Lastline® Sensors provide comprehensive visibility into traffic that crosses your network perimeter ("north/south") as well as traffic that moves laterally inside your perimeter ("east/west"), for both your on-premises network and cloud infrastructure.

Install an unlimited number of Lastline Sensors in your on-premises network, as physical and virtual appliances, anywhere you need visibility. Deploy Sensors as AMI images to extend Lastline Defender protection to your AWS environment.

Validated Alerts With an All-In-One Platform Powered by Artificial Intelligence

The Lastline Defender NDR platform uses a combination of four complementary technologies powered by artificial intelligence to detect and analyze the advanced threats that other tools miss, while significantly reducing false positives:

Powered by Artificial Intelligence

Network Traffic Analysis (NTA)
Detects anomalous activity and malicious behavior as it moves laterally across your network

Intrusion Detection and Prevention (IDPS)
Detects and prevents known threats entering your network

Artifact Analysis
Detects malicious content attempting to enter your network via the web, email, or file transfers

Global Threat Intelligence
Updates Lastline Defender's detection and analysis capabilities in real time

The Industry's Most Accurate Threat Detection

Lastline Defender's NTA applies unsupervised Machine Learning (ML) to your network traffic to detect protocol and traffic anomalies, and uses supervised ML to automatically create classifiers that recognize malicious network behaviors and previously unknown malware.

Lastline applies AI to the malicious behaviors and malware samples collected from customers and partners across our Global Threat Intelligence Network to automatically create new IDPS signatures and push them out to all Lastline Sensors at machine scale.

The patented Artifact Analysis deconstructs every behavior engineered into a file, attachment or URL to determine if it is malicious. Lastline Defender sees all instructions that a program executes, all memory content, and all operating system activity.

The Industry's Highest Fidelity Alerts

SOC teams are often overwhelmed by the high volume of low-fidelity alerts generated by their security controls. The unique combination of NTA, IDPS, and Artifact Analysis, all powered by AI, eliminates most false positives and delivers unmatched alert accuracy.

The result is that Lastline Defender reduces massive amounts of network data down to a just a handful of intrusions (Fig 2) so that your analysts can spend their time solving real incidents and protecting your organization, not chasing false positives all day long.

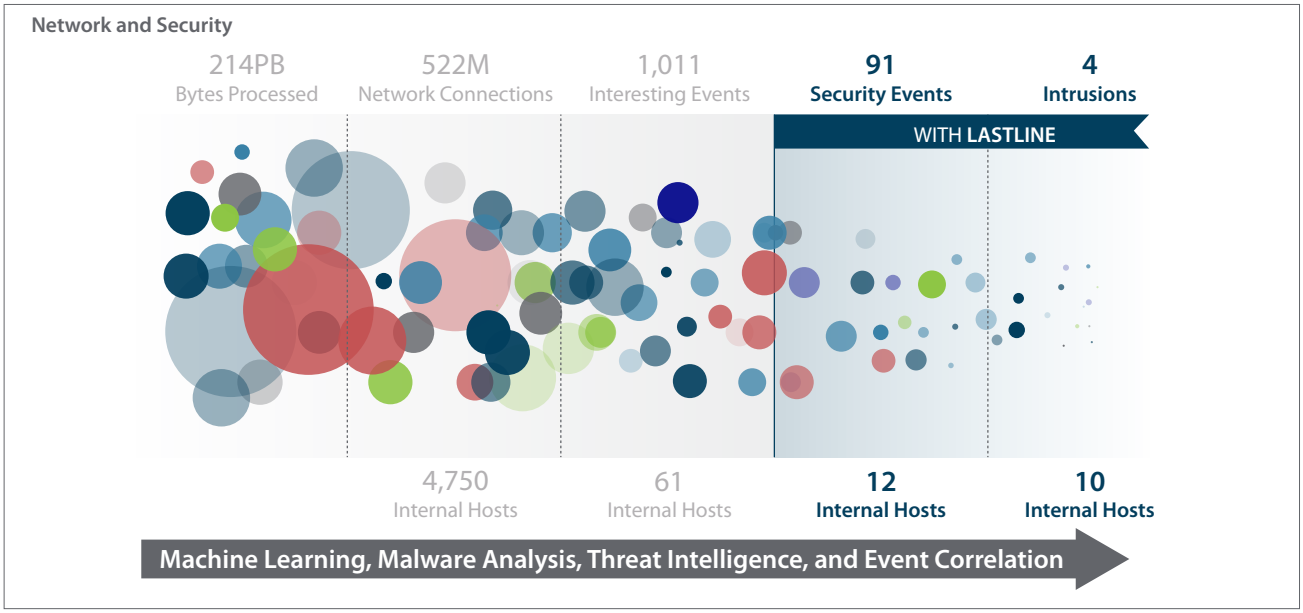

Figure 2: Lastline Defender reduced 214 PB of data analyzed in one month in one network to only 4 intrusions affecting 10 hosts.

Visualize the Entire Attack Chain

Lastline Defender classifies malicious activity into different stages (Fig. 3) to identify the risk associated with each stage of the attack. It also generates a dynamic intrusion blueprint (Fig. 4) and detailed timeline of a threat as it enters and moves laterally across your on-premises and cloud network. These visualizations give your SOC the information it needs to quickly understand the scope of the attack and prioritize response.

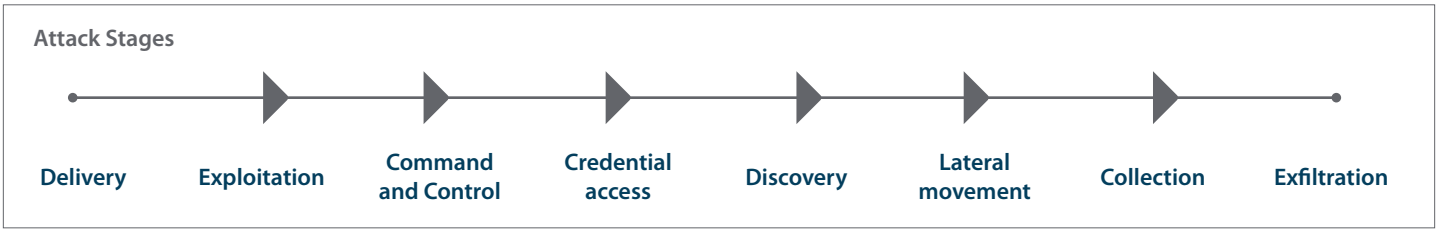

Figure 3: Lastline Defender Helps your SOC team quickly understand the attack stage

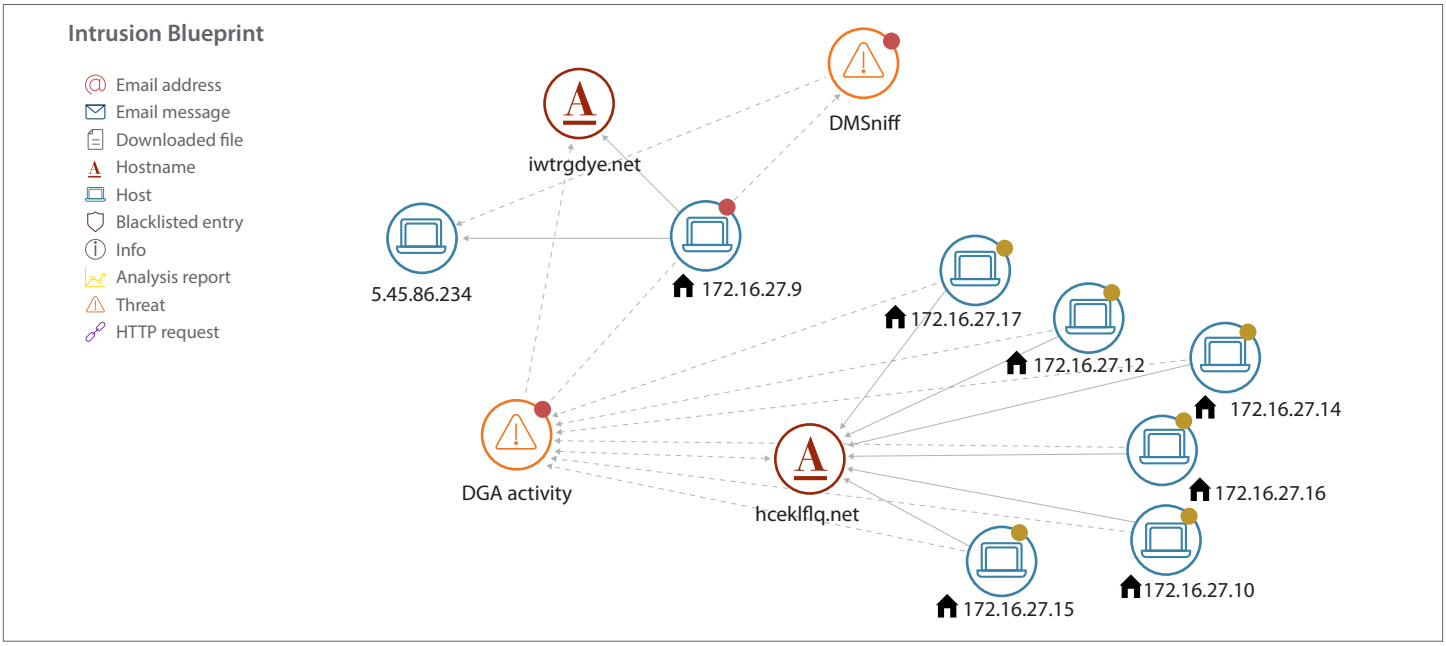

Figure 4: Lastline Defender shows an attack's progress in your network including compromised systems and communication with external systems.

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 objects and anomalous activity:

- Deploy Lastline Sensors in blocking mode to stop malicious content and communication at the perimeter or internally, in both on-premises and cloud environments
- Integrate Lastline Defender with your third-party products such as SIEM, SOAR, endpoint protection and firewalls, custom applications, and incident response workflows throughout your organization

When integrating with your existing controls, you have the choice of using built-in integration offered by our technology partners or using our robust APIs to optimize your current technologies, staff, and processes. Your existing security controls can automatically send unknown objects for analysis and receive actionable threat intelligence in return, before a threat can disrupt your business.

Certified Hardware Specifications for On-Premises Deployment

	1G Sensor	10G Sensor	Data Node	Manager	Detection Engine
Base Model	Dell PowerEdge R440				
Processor(s)	1 Xeon® Silver 4114	2 Xeon® Silver 4114	1 Xeon® Silver 4116	1 Xeon® Silver 4114	1 Xeon® Silver 4114
RAM	32 GB	128 GB	64 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 SAS HDD (10K 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	10	1
Internal Controller	PERC H730p				
Network Adapter	Intel I350 Quad port	Intel X710-DA2	Onboard	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	-

* Cluster N number of components to scale as needed. Performance varies by object type.
** Apply pre-filter to quickly determine maliciousness and submit unknown files for detailed analysis by Deep Content Inspection
*** Supported Intel NIC required for throughput over 200 Mbps
Note: Performance values are based on "standard" profile. Values may vary depending on your environment.

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

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