Lastline Defender for Cloud

Network Detection and Response for Public Cloud Workloads

Lastline Defender™ is a Network Detection and Response (NDR) platform that detects and contains sophisticated threats before they disrupt your business, for both on-premises networks and cloud environments. 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.

Public Cloud Workloads at Risk

Infrastructure-as-a-Service (IaaS) environments such as AWS and Azure are under attack. The complexity of migrating workloads into a shared responsibility security environment leaves organizations with critical gaps in their security. Bad actors target public clouds since they know that these often have weaker protection than the on-premises data center.

Attackers employ a range of techniques to penetrate your public cloud infrastructure, launch new instances, and move laterally to attack other workloads, ultimately harvesting your data. These techniques include:

- Targeting your servers in public subnets in your virtual public cloud (VPC) in AWS or virtual network (VNet) in Azure.
- Exploiting a misconfigured server with open ports to gain a foothold in your internet-facing assets.
- Elevating privileges and performing reconnaissance on your network to identify higher-value targets.
- Moving laterally in your public cloud to find servers in your private subnet which you thought were safe (because they do not have a route to the internet).
- Exfiltrating financial information, personally identifiable information (PII) and other sensitive data.

Agentless Visibility of Threats Entering or Moving Laterally within Cloud Workloads

Lastline Defender™ is the first native cloud NDR platform that delivers unmatched visibility of advanced threats in both your internal (east/west) and internet-facing (north/south) network traffic. You can deploy Lastline's industry-leading AI-powered NDR technology to protect your public cloud workloads, without the need to deploy agents or collectors.

Lastline Defender provides immediate visibility into threats and intrusions across your public cloud workloads, enabling you to detect and contain sophisticated threats before they disrupt your business:

Exploits Targeting Cloud Workloads

Prevent attacks against vulnerable applications and services in public clouds.

Malicious Lateral Traffic

Detect when an attacker scans for other workloads, prevent discovery of additional services, and block lateral movement and connection to an unusual port.

Data Exfiltration

Detect and block anomalous data access before a bad actor can exfiltrate the data.

Validated Alerts with an All-In-One Platform

The Lastline Defender NDR platform uses a combination of four complementary technologies powered by artificial intelligence (AI) to detect and analyze 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

File 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

Securing Your Workloads

To prevent data exfiltration, you need the ability to see both the initial stages of an attack on an asset in your public cloud and the subsequent lateral movement as it spreads. Lastline Defender gives you the option to deploy the Lastline Sensor as an in-line perimeter sensor, in-line content inspection sensor, or VPC Flow Log analyzer for comprehensive threat detection and response:

- **Perimeter:** Delivers full packet (DPI) visibility into any malicious content in the ingress/egress ("north/south") traffic between the internet and your cloud workloads.
- **VPC Traffic Mirroring:** Inspects traffic between VPCs ("east/west") as well as within a VPC for malicious content.
- **VPC Flow Log Analysis:** Analyzes VPC flows for network anomalies, connection anomalies, and data transfer anomalies.

The Industry's Most Accurate Threat Detection

Lastline Defender's Network Traffic Analysis (NTA) applies unsupervised Machine Learning (ML) to your network traffic to detect protocol and traffic anomalies, and uses supervised ML to classify this data as either benign or malicious behaviors. It applies AI to malicious behaviors and malware samples collected from customers and partners across our Global Threat Intelligence Network to automatically create new Intrusion Detection and Prevent Systems (IDPS) signatures for previously unknown malware and push them out to all Lastline Sensors at machine scale. The patented File 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.

High-Fidelity Alerts Eliminate Alert Fatigue

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 File Analysis technologies, continuously updated by Global Threat Intelligence and 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 (Figure 1) so that your analysts can spend their time solving real incidents and protecting your organization, not chasing false positives all day long.

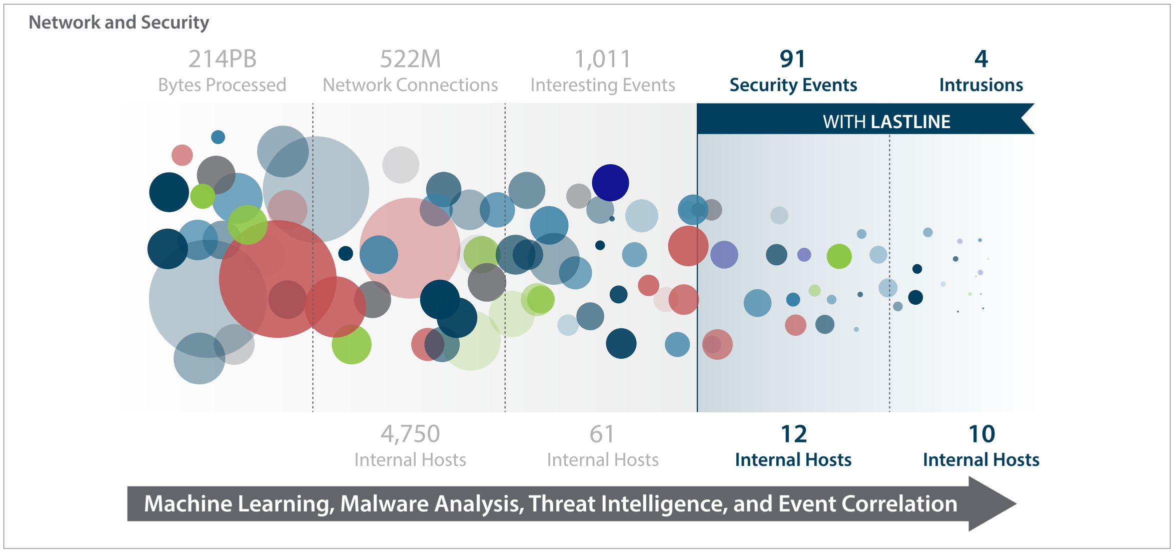


Figure 1: Lastline Defender reduced 214 PB of data analyzed in one month in one network to only 4 intrusions affecting 10 hosts.

Visualize the Entire Attack Chain

Lastline Defender generates a range of threat data visualizations that give your SOC the information it needs to quickly understand the scope of the attack and prioritize response, including:

- **Intrusion Blueprint**—A dynamic map (Figure 2) of an advanced threat as it moves laterally across your cloud and on-premises and environments. It enables your security team to quickly understand the scope of the network breach by providing complete visibility of all activity generated by an attack, including:
    - Traffic crossing your perimeter and moving laterally in your network
    - Compromised systems
    - Communication between local and external systems
    - Data sets accessed and harvested
- **Threats and Hosts**—An at-a-glance summary (Figure 3) of an intrusion shows active threats and affected hosts.
- **Attack Stages**—Classification of malicious activity into different stages (Figure 3) to highlight the risk associated with each stage of the attack and prioritize response.

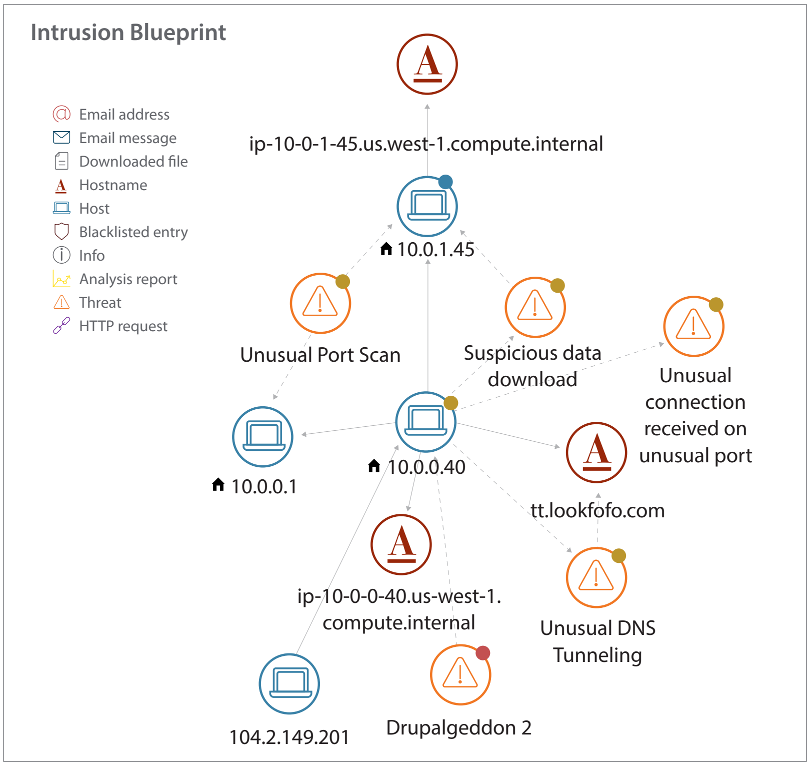
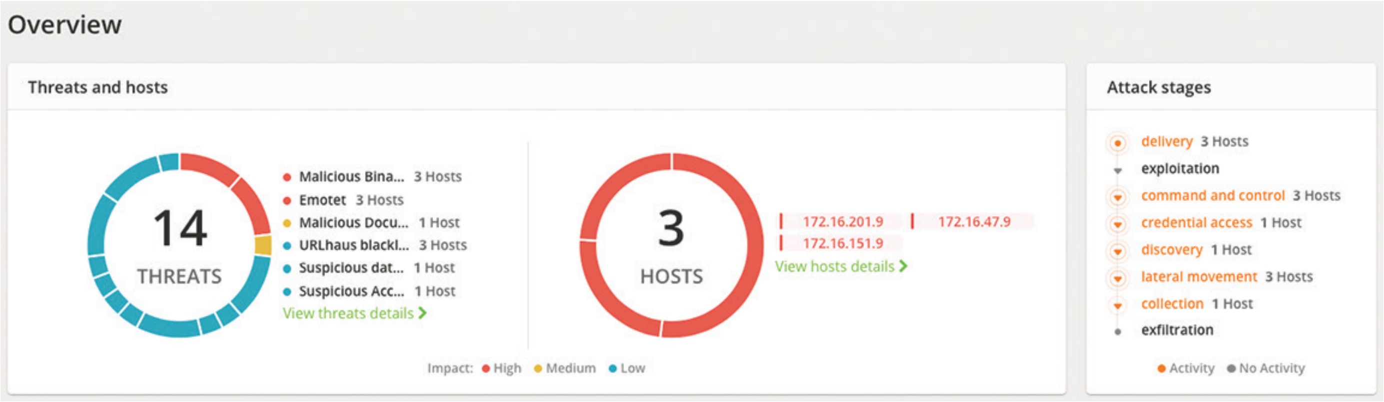


Figure 2: Lastline Defender shows an attack's progress in your on-premises network and cloud workloads including compromised systems and communication with external systems.



Overview

Threats and hosts

14 THREATS

- Malicious Bina... 3 Hosts
- Emotet 3 Hosts
- Malicious Docu... 1 Host
- URLhaus blackl... 3 Hosts
- Suspicious dat... 1 Host
- Suspicious Acc... 1 Host

View threats details ›

3 HOSTS

172.16.201.9 | 172.16.47.9 | 172.16.151.9

View hosts details ›

Impact: ● High ● Medium ● Low

Attack stages

- delivery 3 Hosts
- exploitation
- command and control 3 Hosts
- credential access 1 Host
- discovery 1 Host
- lateral movement 3 Hosts
- collection 1 Host
- exfiltration

● Activity ● No Activity

Figure 3: Lastline Defender creates an summary for every intrusion showing active threats, affected hosts, and attack stages.

Automate Response

Lastline Defender makes your existing technologies, staff, and processes more effective by being able to integrate with your existing security controls and workflows. You can rely on Lastline Defender's high-fidelity insights to automate threat response and eliminate time-consuming manual investigations of anomalous activity and potentially malicious files and links in cloud and on-premises traffic:

- Deploy Lastline Sensors in blocking mode to stop malicious content and communication, at the perimeter or on internal segments
- 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.
    - Lastline Defender gives you the choice of using built-in integration offered by our technology partners or using our robust APIs. 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.

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

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