Failed Promises of IDPS

Replace Your Ineffective IDPS with Lastline Defender

Introduction

Intrusion Detection and Prevention Systems (IDPS) have been a mainstay in security stacks for years. However, for as long as IDPS products have been deployed, they have generated complaints about alert accuracy and volume. More recent concerns speak to the technology's lack of visibility into lateral movement of an attack, inability to detect evasive threats, lack of automated response, and lack of cloud workload security. In other words, IDPS have simply failed to keep up with modern security requirements.

Don't Settle

Rather than looking to address the shortcomings of your IDPS with another stand-alone IDPS, consider a solution that combines IDPS with additional technologies to detect and respond to network threats. Gartner describes the need for an integrated approach:

> "The escalating sophistication of threats requires organizations to use multiple sources of data for threat detection and response. Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents."[1]

Lastline Network Detection and Response

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.

Lastline Defender™ includes four complementary AI-powered technologies to detect and respond to threats in both "north/south" and "east/west" traffic:

- Intrusion Detection and Prevention (IDPS) detects known threats entering your network
- Network Traffic Analysis (NTA) detects anomalous activity and malicious behavior as it moves laterally across your network
- Artifact Analysis detects malicious content attempting to enter your network via web, email, or file transfers
- Global Threat Intelligence continuously updates Lastline Defender's detection and analysis capabilities in real time

Lastline Defender delivers all four technologies in a single platform, providing the accuracy, visibility, advanced threat detection, automated response, and cloud workload security that your IDPS lacks.

[1] Market Guide for Intrusion Detection and Prevention Systems. Craig Lawson, et al, 1 July 2019

Validated Alerts

Signature-based detection can generate a flood of alerts for your SOC team to sift through to identify malicious activity. Effectively managing alerts is an almost impossible task due to the overwhelming amount of work required to maintain the IDPS and ensure it is accurately enforcing security policies.

Lastline Defender applies AI to malicious behaviors and malware samples collected from across our Global Threat Intelligence Network to automatically create new signatures and push them out to all Sensors at machine scale. We constantly review our signatures for detection accuracy.

Lastline's high-fidelity alerts and broad visibility accelerate threat response and dramatically reduces false positives and alert fatigue by leveraging AI that is automatically trained on both network traffic and malicious behaviors (Fig. 1).

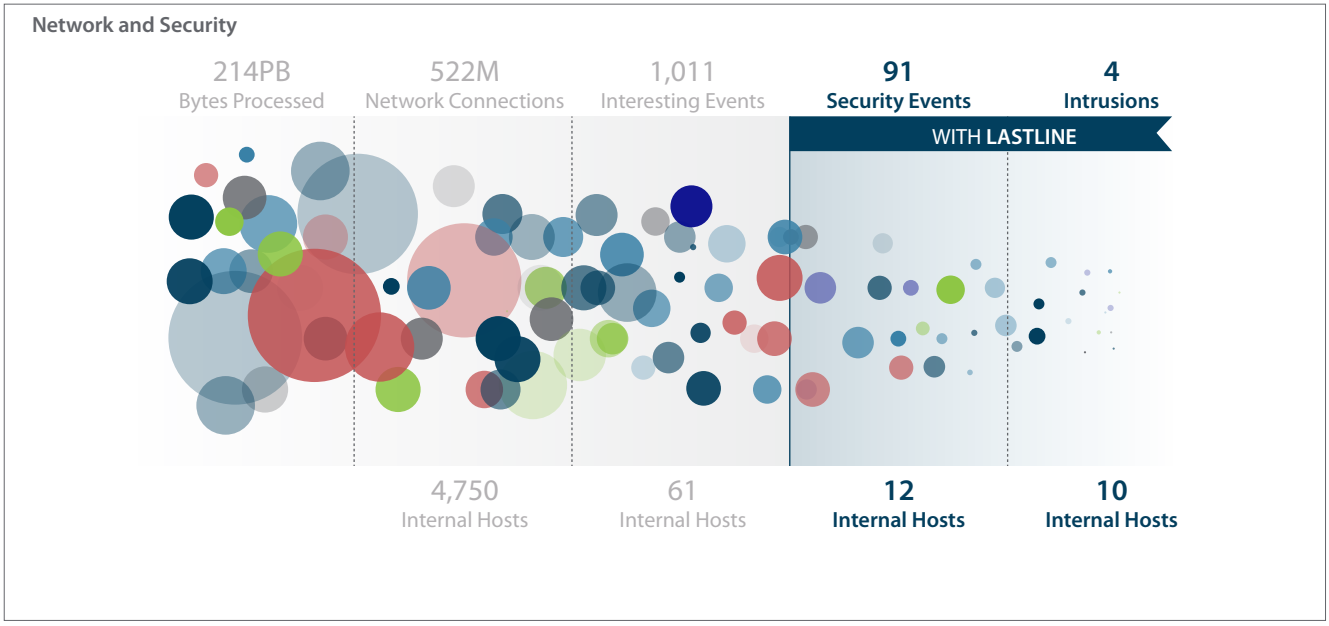

Figure 1: Lastline Defender significantly reduces the number of intrusions your SOC has to investigate (e.g., 214 PB of data analyzed in one month in one network to only 4 intrusions affecting 10 hosts)

Lateral Movement Visibility

Detecting lateral movement is now considered an essential capability for network-based security controls. Security practitioners know that attackers follow a familiar pattern: First they establish a foothold on the network and then move laterally to compromise internal servers and databases. Unfortunately, IDPS cannot identify abnormal behavior of hosts and users on the network.

Lastline Defender analyzes anomalous network traffic and device behaviors in real time to speed up notification and response. It monitors application-level network protocols and internal protocols, and aggregates network data for context and historical analysis. Lastline Defender then generates an intrusion blueprint blueprint (Fig. 2) and a timeline of a threat as it moves laterally across your network.

This visibility enables your SOC to quickly understand the scope of an intrusion by visualizing all attack activity, including:

- Attack stages
- Extent and duration of attack
- Systems compromised
- Communication between local and external systems
- Data sets accessed and harvested

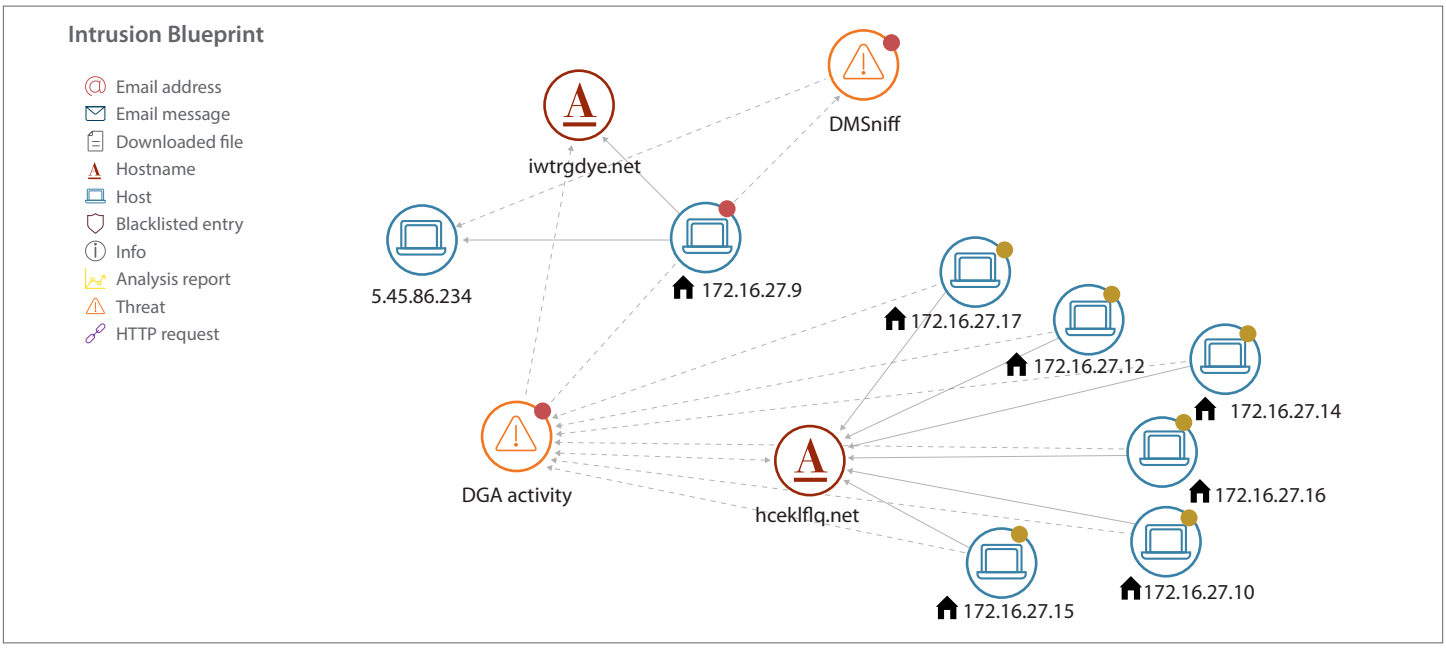

Figure 2: Lastline Defender shows an attack's progress in your network including compromised systems and communication with external systems.

Advanced Threat Detection

Bad actors engineer threats to evade detection. IDPS are vulnerable to evasion techniques such as packers and polymorphic code because they lack real-time traffic analysis to detect and analyze new threats.

The Defender Platform uses a combination of AI-powered capabilities to detect the advanced threats that other tools miss and significantly reduce false positives:

- Apply unsupervised Machine Learning (ML) to detect protocol and traffic anomalies
- Use supervised ML to automatically create classifiers that recognize malicious network behaviors and previously unknown malware
- Leverage the threat knowledge from our Global Threat Intelligence Network to scan traffic metadata and payloads for variants of known threats

In addition to detecting the threats that other IDPS cannot, Lastline Defender delivers the context your IDPS lacks. It automatically links threats moving laterally across your network with threats crossing your perimeter, increasing accuracy while reducing the dependency for follow-up investigation.

Automated Response

Low-fidelity alerts prevent automated response workflows due to lack of confidence in the accuracy of the alerts. Lastline's high-fidelity alerts enable Lastline Sensors, when deployed in-line, to automatically block malicious activity. You can also integrate Lastline Defender with products already in your security stack to automate response workflows, such as:

- Block malicious content entering the network via email or web traffic
- Send TCP resets to block communication between devices
- Update Access Control Logs
- Blacklist communication with domains and IP addresses
- Block malicious content in mail or web

Secure Cloud Workloads

Bad actors target your workloads in infrastructure-as-a-service (IaaS) environments like AWS. They employ a range of techniques to penetrate your cloud infrastructure, launch new instances, and move laterally to launch attacks on other workloads, ultimately harvesting and exporting data. These techniques include:

- Targeting your servers in public subnets in your virtual public cloud (VPC) on AWS
- Exploiting a misconfigured server with open ports to gain a foothold in your internet-facing assets
- 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)
- Compromising servers running in your AWS instances and downloads data

Lastline Defender protects against advanced threats in both your internal and external public cloud traffic in AWS:

- Block inbound exploits of vulnerable applications and services to protect your cloud workloads
- Detect malicious lateral traffic and prevents discovery of other workloads and lateral movement
- Block anomalous data access before a bad actor can exfiltrate the data

Regulatory Compliance

Lastline Defender helps you satisfy IDPS-specific compliance requirements and best practices frameworks. These include PCI DSS 11.4, HIPAA (NIST SP 800-66), FISMA (NIST SP 800-53), NIST DE.AE (Detect – Anomalies and Events) and DE.CM (Detect – Security Continuous Monitoring), and Center for Internet Security Control 12.7.

Deployment Flexibility and Significantly Lower TCO

Pricing and deployment models for legacy IDPS are based on limited distribution of hardware appliances at critical locations. Unfortunately, your network infrastructure has evolved far beyond a well-defined perimeter with limited access points to include a diverse mix of BYOD, IoT, and public cloud data centers.

With Lastline Defender, you have complete deployment flexibility. Lastline Defender's user-based pricing enables you to deploy Lastline Sensors wherever you need visibility without incurring additional licensing costs. Defender's agentless, cloud-based architecture gives you the freedom to deploy the components where you want.

Lastline Defender: Proven Protection

You need more advanced protection for your network than your stand-alone IDPS can provide. Lastline's NDR platform delivers the accuracy, visibility, detection and response that your IDPS lacks to stop threats entering or operating in your network. **Learn why** over 20 million users trust Lastline.

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

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