lastline

White Paper

Network Security in an Encrypted World

Security professionals use the network to collect data, detect malicious activity, implement security controls, and protect against threats. However, analyzing encrypted network traffic presents challenges. This white paper discusses the advantages as well as the challenges of security products that monitor network traffic, and outlines how Lastline addresses these challenges.

Why the Network Should Be the Focus for Encryption

Security products that protect organizations against advanced threats generally fall into two categories:

- Endpoint-based products require the installation of software components (agents) on individual devices, and monitor the activity of users, applications, and the operating system.
- Network-based products require the installation of software components on physical or virtual devices that monitor network traffic as it is transmitted from one device to another.

A comprehensive security strategy requires the deployment of both product categories. Although endpoint agents provide local visibility into individual devices, they do not provide complete protection against advanced threats. Network-based products provide broader detection and response, which is why CISOs, SOC analysts, and incident responders rely heavily on this category.

The Need for Complete Coverage

Modern IT systems are complex and heterogeneous. They include a wide range of devices such as desktops, notebooks, printers, BYOD and IoT (such as security cameras and the company fridge). These devices are expanding an organization's attack surface and bad actors use them as a stepping stone to execute a data breach.

Network security products provide visibility into the behavior of these devices, and they can see every communication that targets any of them. This visibility is much more complete than what endpoint products can achieve for two important reasons:

- First, it is almost impossible to install an agent on every single device in a heterogeneous network. In many cases, agent software is not available for all platforms and OS versions deployed in an organization. In the case of IoT, there is typically no way to install security software.
- Second, when new devices (including BYOD) appear on the network, it is often impossible to identify them quickly and add endpoint protection without network visibility.

Network Traffic as Ground Truth

Network packets provide raw evidence that is often an essential ingredient for investigations and forensic analysis. In particular, network traffic provides ground truth that attackers cannot tamper with. However, this is not the case for endpoint products. When attackers compromise a machine, they run malicious code side-by-side with the endpoint agent. Hence, it is possible for attackers to tamper with (or even disable) an endpoint agent, or to interrupt the communication between the agent and a central server that collects and reacts to alerts.

Endpoint vendors attempt to harden their systems against these attacks, but it's still a cat-and-mouse game where defenders have to catch up with adversaries' latest tricks. Network visibility, on the other hand, provides certainty. When you see that your data has left the network, you know the breach has happened. If there is no data exfiltration, you have full confidence that an intrusion was not successful.

Connecting the Dots

In many security incidents, intrusions affect multiple machines across the network. For example, an attacker might obtain initial access by compromising a low-level asset, such as the machine of a user who clicked on a malicious link that installed malware. The attacker can then attempt to elevate their privileges, perform reconnaissance to identify higher-value targets, and move laterally.

While moving along the stages of the attack chain, an intruder will leave breadcrumbs in multiple places. While it is possible to aggregate and correlate these pieces of information from multiple endpoint agents and reconstruct some stages of the attack, endpoint products tend to take a more isolated and localized view of threats. A network-based solution is the logical place to see more activity related to the attack.

The Challenge of Encrypted Network Traffic

Encryption protects the confidentiality and privacy of sensitive data in motion. However, encryption also poses a challenge to network security products. If these products cannot inspect the payload of connections, they lose their ability to detect and respond to threats.

The Rise of Encrypted Data

The use of encryption on the Internet has risen dramatically. For example, the **Google Transparency Report** shows that the fraction of encrypted web traffic on the Internet has steadily increased, from around 50% five years ago to between 80% and 90% today.

Although the percentage of encrypted traffic on "the inside" -- within the networks and data centers of organizations -- is lower, initiatives such as the **zero trust network architecture** will likely increase the number of organizations embracing encryption to secure internal data. Thus, it is important to understand how network security products can deliver visibility and protection in the presence of ubiquitous encrypted traffic.

Encrypting traffic prevents network security products from inspecting the payload. This means that they can neither leverage signatures to detect known threats nor extract objects (e.g., files or documents) before submitting them to a sandbox for deeper analysis. While this affects the effectiveness of network-based products, it does not mean that network security is obsolete. Users still need the complete coverage, the context, and the certainty that only the network can provide. However, users need the proper solution to obtain these resources.

Overcoming the Challenge: Lastline Defender

Lastline Defender is a Network Detection and Response (NDR) platform that detects and contains sophisticated threats. It does this by applying unsupervised Machine Learning (ML) to network traffic in order to detect anomalies, using supervised ML to create classifiers of malicious network activity and leveraging its Global Threat Intelligence Network to scan traffic for known malware payloads.

Lastline Defender employs two methodologies to deal successfully with encrypted communication: decrypting network traffic and analyzing encrypted traffic.

Decrypting Network Traffic

Organizations have many reasons to inspect network traffic content, ranging from compliance to policy enforcement and security. For example, organizations may monitor outgoing data to detect the presence of sensitive information, ensure that employees only visit acceptable websites from their work computers, and understand if a compromised host connects to command and control (C&C) sites. To meet these objectives, many organizations have deployed instrumentation points that break open encrypted connections and allow security products to analyze payloads. These instrumentation points include:

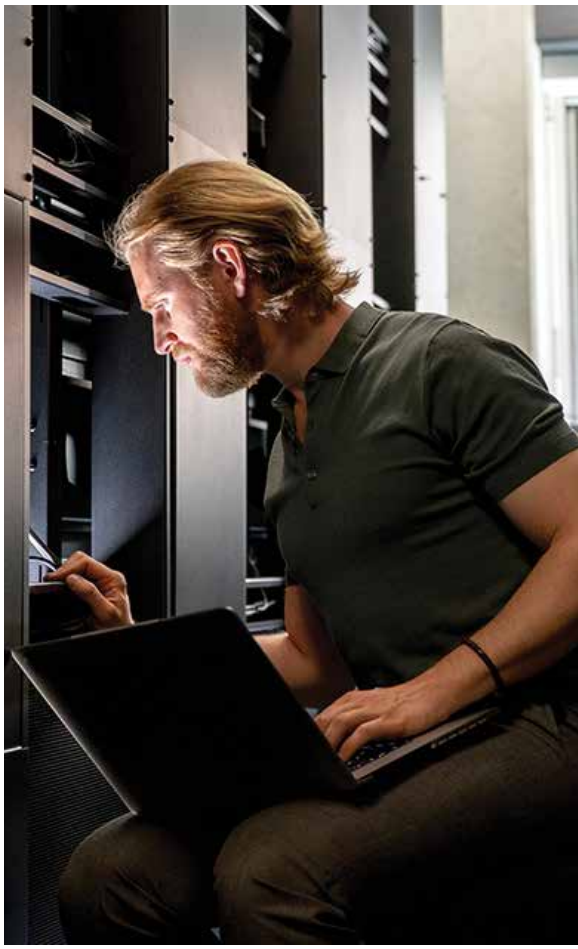
A. **Web Proxy:** Web proxies inspect web traffic between clients in their network and the Internet. Most web proxy products allow for breaking open HTTPS connections, and using the Internet Content Adaptation Protocol (ICAP) interface to offer third-party products (such as data loss prevention and antivirus) access to cleartext traffic. Lastline supports the ICAP interface and can connect to a proxy to scan unencrypted web traffic for threats.

B. **TLS Termination Proxy:** TLS termination proxies (also called reverse proxies) sit in front of servers that offer content to clients on the Internet. The proxy will decrypt inbound traffic before forwarding it to a server. The purpose of a TLS termination proxy is to reduce the load from the web servers by performing costly computations necessary for decrypting traffic. TLS forwarding proxy deployments are natively supported by AWS through their Elastic Load Balancing (ELB) service, which includes SSL/TLS decryption capabilities. Reverse proxy deployments enable the Lastline Sensor to monitor cleartext traffic that the proxy and a web server exchange.

C. **Mail Transfer Agent:** The Lastline Sensor can act as a mail transfer agent (MTA), inserted into the email delivery chain. In this configuration, the Lastline Sensor receives emails from an upstream email server and can inspect the full content (headers and body) in cleartext. After inspecting an email, the Sensor forwards it to a downstream email server for delivery. In addition to inspecting email traffic and raising alerts, the Lastline Sensor can remove malicious URLs and attachments from emails or block malicious emails.

D. **Active TLS Interception:** The Lastline Sensor can work with any active middlebox that intercepts and breaks open encrypted connections that can forward the plaintext traffic to the monitoring (sniffing) interface of the Sensor.

Decrypting network traffic with TLS Version 1.3



The Internet Engineering Task Force (IETF) published a new TLS standard (in **RFC 8446**) in August 2018. A key question is the expected impact of TLS 1.3 on the ability of network products to break open and inspect encrypted traffic. The IETF Network Working Group published a **use case document** that describes the full impact of the proposed protocol changes. In this section, we summarize the most important changes and their implications.

The most notable change introduced by TLS 1.3 is that it mandates Perfect Forward Secrecy (PFS), an objective which provides the assurance that a session key will not be compromised even if the private key of the server is leaked. This is achieved by generating a unique session key for every connection.

Before TLS 1.3 and PFS, all data transmitted between a client and a server could be decrypted if the server's private key was known. Network security products could leverage this to decrypt and monitor inbound network traffic. Specifically, a security tool could get the secret key of a server and then passively capture network traffic to the server and decrypt it without being an active element in the connection (a bump-in-the-wire). This will no longer be possible, however.

It is important to understand that TLS 1.3 and PFS have little impact on active products that terminate TLS connections such as proxies, MTA deployments, and active interception devices. That is, it remains possible to intercept and inspect outbound connections from clients within the network to servers on the outside. However, TLS 1.3 does introduce a change whereby the server certificate, which the server presents to prove its identity to a client, is now encrypted in the initial handshake (the server certificate was in the clear before).

As a result of certificate encryption, a web proxy is no longer able to use the certificate to determine that a particular connection is sensitive and should not be inspected. For example, a proxy might be configured to allow and pass through connections without inspection to trusted destinations, such as online banking or health care sites. Without access to the server certificate, the proxy has to break open (terminate) and relay traffic for all connections. Despite this change, the impact of TLS 1.3 on Lastline's ability to access and analyze decrypted network traffic is minimal.

Analyzing Encrypted Traffic

Even when a Sensor has no access to decrypted traffic and payloads, Lastline provides significant protection against malicious activity. To achieve this, our solution inspects and uses traffic (connection) metadata and leverages the following three detection techniques:

A. **Anomaly Detection:** Lastline uses ML to build a baseline of expected traffic. The system creates models that capture host profiles and patterns of normal traffic. These models leverage connection metadata that is not encrypted (even when the application payload is encrypted). This metadata includes the source and destination IP addresses and ports, the number and size of packets that are exchanged, and timing information.

   When a Sensor identifies a connection that violates the baseline and appears as an outlier (an anomaly), the system can generate an alert. For example, Lastline Defender might identify connections between two endpoints that have never communicated, an unexpected volume of traffic to a remote host on the Internet (possibly indicating data exfiltration), and a connection to an unexpected port, using an unusual protocol. Of course, not every outlier is an attack, and making this naive assumption leads to high volumes of false positives. Thus, Lastline cross-references anomalies with models of malicious behaviors to identify those instances that actually matter

B. **Threat Intelligence and Indicators of Compromise:** Lastline analyzes millions of threats every day collected by Lastline's global customer and partner base, and sends results to the Lastline Global Threat Intelligence Network. This is the industry's largest curated repository of malicious artifacts, malicious behaviors, and indicators of compromise (IoCs). The threat indicators include IP addresses, DNS names, certificate information, and TLS fingerprints (using JA3). This data is present in all network connections, including encrypted traffic, and we check every connection against these IoCs.

C. **Encrypted Traffic Analysis:** Encrypted traffic analysis: Lastline pioneered an innovative approach of building models that operate directly on encrypted traffic to identify malicious communication without the need to inspect any payload. These models leverage traffic features such as:

   - The length of individual packets
   - The number of packets exchanged in each round between a client and a server
   - The duration of a connection
   - The timing between packets.

Lastline Defender uses ML to train models on the large volume of (malicious) network traffic produced by millions of samples that we detonate in our sandbox every day. For more details, an academic paper that describes the ideas of an early version of encrypted traffic analysis is available **here**.

Conclusion

The use of encrypted traffic inside the network continues to increase as more organizations use it to secure data. Its use, however, can decrease the effectiveness of many network-based security products to detect malicious content and activity, leaving organizations unprotected. The Lastline Defender NDR platform is designed to detect and respond to threats in encrypted traffic by decrypting network traffic as well as analyzing encrypted traffic.

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

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