Solution Brief

Symantec Technology Integration Partner: LogRhythm

Business Challenge

Encryption has become ubiquitous for certain internet communications and cloud-based services. While encryption helps address organizational requirements to operate securely over the Internet, it also creates blind spots for an organization's security team. Encryption not only protects legitimate traffic, it can also mask the activity of threat actors. This makes it difficult to distinguish between normal network activity and malicious network activity, such as data exfiltration, botnet communication, zero-day attacks, phishing attempts and network policy violations. By 2017 Gartner predicts that more than half of network attacks targeting enterprises will use encrypted traffic to bypass traditional security controls.

Solution Overview

As the use of SSL and TLS to encrypt e-mail, mobile and cloud applications continues to grow, organizations increasingly need visibility into the encrypted traffic traversing their networks in order to detect and respond to threats hidden in these channels. Symantec's encrypted traffic management solutions and LogRhythm's Network Monitor solution together eliminate the encrypted traffic blind spot by uncloaking security threats hidden in encrypted traffic. Delivered in part by the market-leading Symantec SSL Visibility, Symantec's decryption capabilities enhance existing security solutions such as Network Monitor by providing visibility into previously hidden traffic and advanced threats, without requiring significant upgrades or re-architecting the network security infrastructure. As a key product in Symantec's encrypted traffic management solution set, SSL Visibility is a high-performance, purpose-built solution that utilizes comprehensive policy enforcement to inspect, decrypt and manage SSL traffic in real-time, while ensuring data privacy and regulatory compliance. SSL Visibility's unique "decrypt once, feed many" design enables a single appliance to simultaneously provide decrypted feeds to multiple network and security tools, including LogRhythm's Network Monitor.

LogRhythm's Network Monitor receives decrypted network traffic from SSL Visibility and then uses advanced analytics to expose critical activities and threats such as advanced attacks, data exfiltration and network usage policy violations. Network Monitor performs deep packet inspection of traffic decrypted by Symantec to identify applications and extract a rich set of Layer 7 metadata at line-rate. Users can perform unstructured searches across this data to run investigations and access highly valuable forensic evidence. Users can also enable Network Monitor's Continuous Search-Based Alerting to perform automated analysis of saved searches to detect when specific conditions are met. In addition, Network Monitor features the automated packet-level analytics engine, Deep Packet Analytics, which leverages Lua-based scripting to automatically detect a variety of network anomalies and user-defined conditions, including network intrusions, protocol mismatches, or the traversal of sensitive information, such as social security numbers or credit card account numbers.

LogRhythm

Partner: LogRhythm

Partner Product: LogRhythm Network Monitor, Security Intelligence Platform

Symantec Product: SSL Visibility

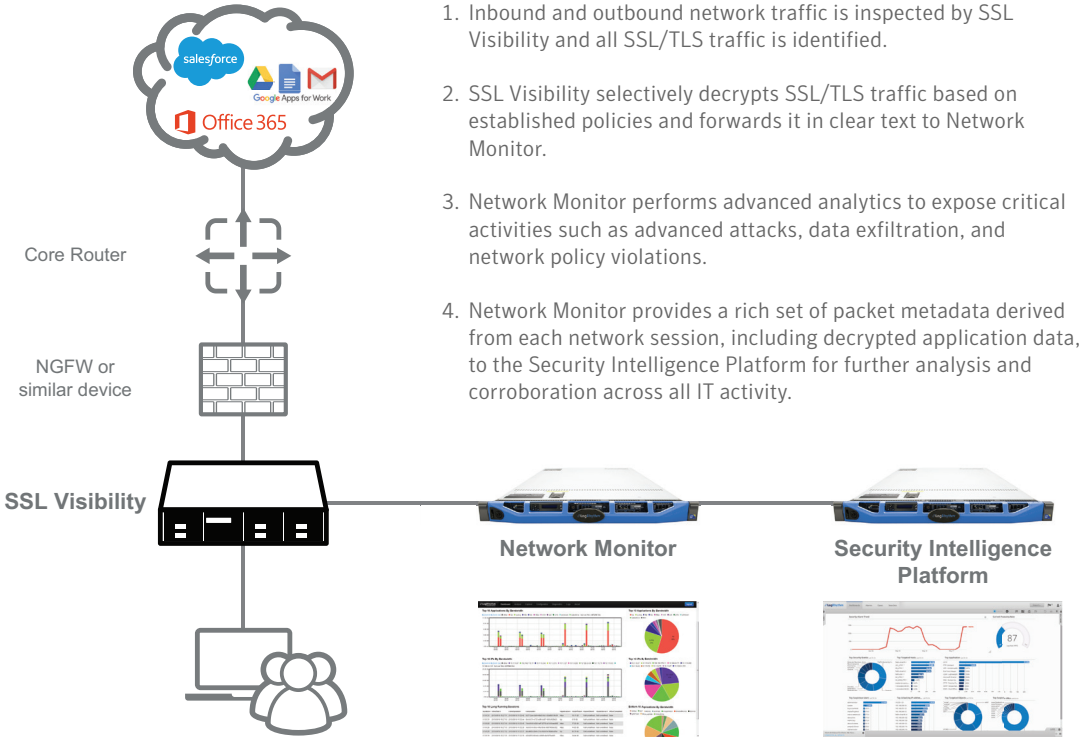
Symantec

In response to network anomalies, Network Monitor can perform selective packet capture on sessions that contain specific types of packet data based on user-defined criteria.

Network Monitor can be configured to forward extracted metadata to LogRhythm's Security Intelligence Platform for automated machine analytics and centralized search-based forensic analytics leveraging the broader context provided by event and machine data collected from other systems and devices across the distributed environment. Together, the Network Monitor and SSL Visibility provide deep visibility and analytics for encrypted SSL network traffic to enable rapid detection and response to threats hidden in network traffic, while preserving user privacy and ensuring regulatory compliance.

How it Works

The following diagram demonstrates how SSL Visibility and Network Monitor can be deployed together to quickly and simply provide best-in-class encrypted traffic management and analysis for real-time threat detection and response. Tested and certified to work together, the joint solution analyzes traffic and provides comprehensive network visibility through an intuitive web-based UI to solve critical security concerns, and expose network anomalies and inappropriate user activity.



1. Inbound and outbound network traffic is inspected by SSL Visibility and all SSL/TLS traffic is identified.
2. SSL Visibility selectively decrypts SSL/TLS traffic based on established policies and forwards it in clear text to Network Monitor.
3. Network Monitor performs advanced analytics to expose critical activities such as advanced attacks, data exfiltration, and network policy violations.
4. Network Monitor provides a rich set of packet metadata derived from each network session, including decrypted application data, to the Security Intelligence Platform for further analysis and corroboration across all IT activity.

Key Features and Benefits

Data Theft

Many organizations allow employees to access cloud sharing sites such as Box and Egnyte for business purposes, but they need to be able to monitor encrypted SSL traffic to ensure that sensitive files are not inappropriately sent outside of the organization.

1. SSL Visibility intercepts and decrypts SSL traffic based on established policies and sends an unencrypted copy of this traffic to the Network Monitor.
2. The Network Monitor can alert administrators when files of a certain size or type, such as Excel, are moved off internal systems, including to cloud applications via encrypted communications. Network Monitor can also automatically alert administrators when specific data, such as social security numbers or credit card numbers traverse the network.
3. Administrators can then drill down to see the file name, extract the file contents and identify the application being used, giving them complete visibility into the activity on cloud sharing sites.

BotNet Detection

Botnet callbacks often use standard ports and sometimes legitimate applications to disguise their traffic in order to avoid detection.

1. SSL Visibility intercepts and decrypts traffic based on established policies and provides a copy of decrypted network traffic to Network Monitor.

2. The Network Monitor analyzes the traffic to detect non-HTTP traffic on port 80 and identify the true application.

3. Full packet capture of the decrypted session discloses additional content not identified via traditional security tools, allowing further analysis and verification of security incidents.

About LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. Learn more about www.logrhythm.com/products/network-monitoring.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_sb_TechPartner_SSLVisibility_LogRhythm_EN_v1a