Solution Brief

Symantec Technology Integration Partner: Lastline

Business Challenge

Attorney General Eric Holder once said, “There are two types of American companies, those that have been hacked and those that don’t know that they have been hacked.” Is it okay to just accept that your network defenses have been breached? Is there a way to find out for sure whether your layers of information security have been compromised, whether your employees have been victims of drive-by downloads, and whether Advanced Persistent Threats (APTs), zero-day attacks, and advanced malware still target your enterprise?

Solution Overview

Like a security camera for your network, Symantec Security Analytics records, indexes and classifies everything that crosses your network. It extracts and reconstructs every detail associated with advanced malware and unknown threats, including source and destination IPs, every packet, flow, file, application, and detailed server information. Security Analytics leverages analysis capabilities of the Lastline Breach Detection Platform to identify evasive and zero-day threats with a next-generation, full-system emulation sandbox. Security Analytics also leverages the Symantec Global Intelligence Network – aggregated threat intelligence from 15,000 customers and 75 million users to provide instant, actionable intelligence on web, email, and file-based threats. Armed with this analysis, incident response teams can assess damage, contain malware, mitigate data loss, and prevent subsequent attacks by fortifying the network.

lastline

Partner: Lastline, Inc.

Partner Product:
Lastline Breach Detection Platform

Symantec Product: Security Analytics

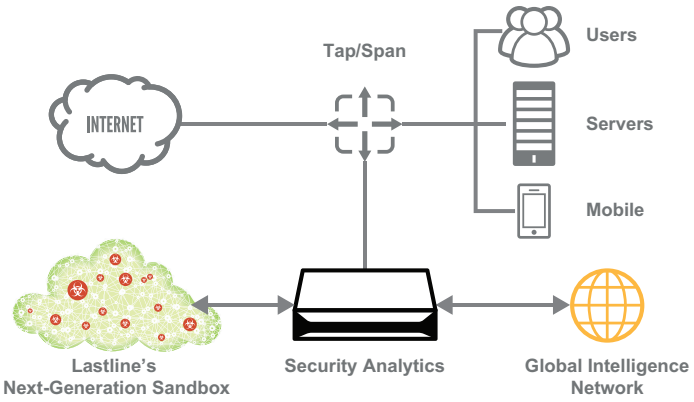
How it Works

Security Analytics records and indexes full packet captures of all activity and can reconstruct objects (files, email and Instant Messaging messages, PHP, Ajax, JavaScript and more). The data captured by Security Analytics along with unknown files are passed to the Lastline Breach Detection Platform to expose Command and Control communication to and from APTs, drive-by downloads of malware from known malicious sites, and zero-day advanced malware.

Objects reconstructed in Security Analytics are inspected to determine if they are known malicious files. The open web services REST API in Security Analytics allows suspicious files to be passed to a cluster of Lastline Engines hosted in the cloud for further analysis. These Engines use a unique full-system emulation sandbox to provide the deepest level of visibility into unknown malware behavior and identify advanced attacks and malware attempting to evade detection.

Objects identified to contain APTs or other forms of advanced malware are reported back to Security Analytics, which can trigger pre-configured policy-based alerts and incident responses.

Symantec



Key Benefits

Advanced malware detection

By integrating Lastline's Breach Detection Platform with Symantec's Security Analytics, security professionals can detect previously-identified malware, and also uncover unknown threats like APTs, zero-day attacks, and advanced malware.

Security incident response and resolution

When the Lastline Breach Detection Platform detects a threat it reports back to Security Analytics. Security Analytics can initiate automated policy-based incident response and resolution procedures.

Situational awareness and continuous monitoring

The full and continuous capture of network traffic in the Security Analytics Platform makes it possible to examine any part of the enterprise network in multiple ways. The Lastline Breach Detection Platform analyzes suspicious objects reconstructed by Security Analytics and can provide evidence of APTs that have previously gone undetected.

About Lastline, Inc.

Lastline is innovating the way companies detect active breaches caused by advanced persistent threats, targeted attacks, and evasive malware with its software-based Breach Detection Platform. Lastline's open architecture integrates advanced threat defenses and intelligence into existing operational workflows and security systems. Inspection of suspicious objects occurs at scale in real time using a full-system emulation approach to sandboxing that is superior to virtual machine-based and OS emulation techniques. Network and object analysis correlate for timely breach confirmation and incident response. Lastline was built by Anubis and Wepawet researchers and industry veterans with decades of experience focused specifically on advanced breach weaponry and tactics. Headquartered in Redwood City, California with offices throughout North America, Europe and Asia, Lastline's platform is used by global managed security service providers, Global 2000 enterprises and leading security vendors worldwide. To learn more, visit www.lastline.com.

For More Information

Learn more about Symantec Technology Integration Partners on our website.

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