lastline

TRIPWIRE AND LASTLINE

LEADING-EDGE PROTECTION FOR ADVANCED AND EVASIVE THREATS

HIGHLIGHTS

- Protect critical data through an enterprise-class hardened solution
- Receive a reliable, objective view of overall security posture across all endpoint systems
- Leverage real-time global threat intelligence to automatically block known advanced threats
- Analyze zero-day evasive malware with full-system emulation sandbox technology
- Highlight anomalies that indicate a breach by unknown malware
- Quickly determine endpoint risk priority and take action

OVERVIEW

In order for security operations teams to keep up with the constantly changing threat landscape they need tools capable of quickly collecting, analyzing and correlating a diverse set of data. To prevent infections from becoming data breaches, they must be able to quickly respond to the results those tools provide.

Tripwire® Enterprise provides real-time endpoint and server monitoring and detection, with protection from advanced, evasive, and zero-day exploits through integration with the Lastline Breach Detection Platform. The integration provides a comprehensive end-to-end solution with unprecedented protection of both known and unknown threats.

HOW THE JOINT SOLUTION WORKS

Tripwire Enterprise continuously captures, monitors and records system and file change data on a broad range of enterprise servers and end-point platforms. When a Tripwire Enterprise agent discovers a suspicious, unknown threat, it sends the data to Lastline for further analysis.

The Lastline Breach Detection Platform identifies advanced and previously unknown threats specifically designed to evade first-generation sandboxes and traditional security systems. Lastline's technology performs full-system emulation of the hardware (CPU and physical memory) to execute malware inside of a real operating system, allowing visibility into attempts by malware authors to fingerprint the runtime environment.

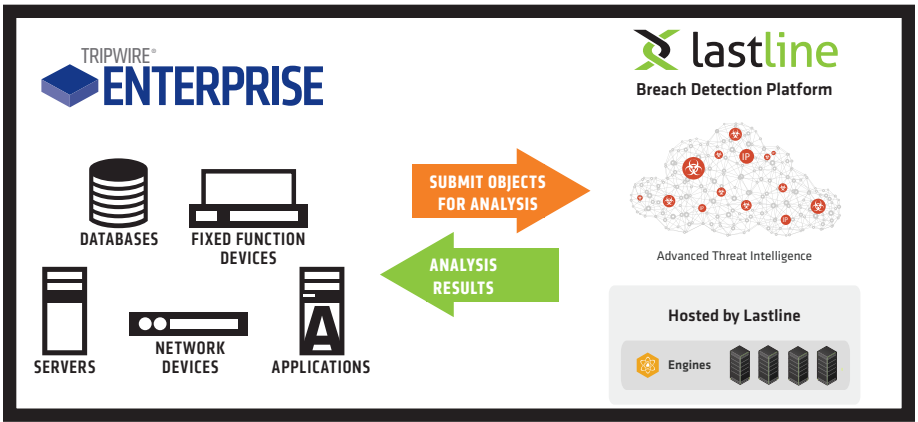

FIG. 1 *Working together, Tripwire and Lastline greatly reduce the time needed to accurately detect and protect against advanced and evasive threats from the network edge to endpoint systems.*

Lastline automatically updates its threat intelligence database, creating protections for all newly discovered threats and sharing them with Lastline subscribers worldwide in minutes. Malicious binaries detected by Tripwire Enterprise are tagged as malicious, enabling prioritization of actions for changes on endpoint systems as well as blocking these binaries within minutes at the network level, preventing further infection.

ABOUT LASTLINE

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.

Lastline's technology correlates network and object analysis to achieve 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.

tripwire®

◆ Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

©2014 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc.
All other product and company names are property of their respective owners. All rights reserved.

TAPLL1a 201501