BLUE COAT®

Network
+ Security
+ Cloud

BLUE COAT TECHNOLOGY PARTNER: TRIPWIRE

SOLUTION BRIEF

Business Challenge

Endpoint security has evolved over the last several years moving beyond simple AV protection to encompass new technologies such as application protection and privilege management, whitelisting, execution isolation and comprehensive visibility and controls. While the network and, in particular, the security proxy remain the primary control point in effective data security, the intelligence and actionable data that can now be gathered from endpoint devices such as Windows PCs and Linux machines is extremely useful for both the security operations and incident response teams.

As enterprise network administrators deal with BYOD, shadow IT, and the Internet of Things, the need for endpoint detection and response is crucial. Blue Coat's portfolio of products integrates with Endpoint Detection and Response (EDR) technologies, allowing security professionals to see what is happening at the endpoint and on the network in real time, or through historical network traffic recordings. This "anywhere, anytime" visibility is vital to identifying critical attack indicators and for performing impact analysis as attackers move within an organization's network.

Protect Against Known and Zero Day Threats

The escalating cyber threat challenge facing most businesses and government organizations seems insurmountable. Enterprises are dealing with the reality that "it's not a matter of if, but when you will be breached." Operating in a continuous state of compromise has become the new normal. In this type of environment, it is critical to be able to detect and remediate malware and zero-day threats as quickly as possible, and provide complete and accurate evidence – while also fortifying the network against any repeat attacks.

tripwire®

Partner: Tripwire, Inc.
Partner Product: Tripwire Enterprise, Tripwire Log Center

Blue Coat Product: Content Analysis, Malware Analysis and Security Analytics

Solution: Tripwire and Blue Coat

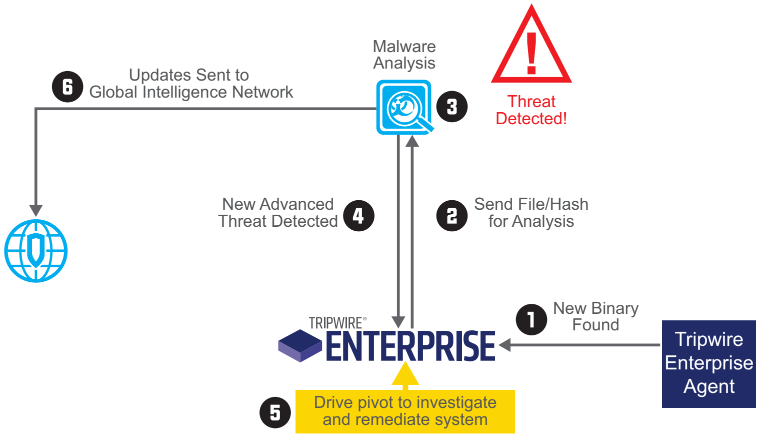
Tripwire Enterprise together with Blue Coat Security Analytics and Malware Analysis enables a rich unified network to endpoint visibility, providing the ability to detect advanced malware through to swift remediation. For any infected asset, incident response teams can seamlessly pivot between Blue Coat Security Analytics, Tripwire Enterprise and Tripwire Log Center to determine the scope of the breach and then take action to isolate, block and remediate any infected devices. Together, Tripwire and Blue Coat reduce the time required to accurately detect and respond to advanced threats.

How it Works

Protecting Critical Systems from Unknown Threats

When a file is not identified at the endpoint, Tripwire Enterprise automatically sends the complete file to Blue Coat Malware Analysis. Blue Coat performs a powerful dual-detection that combines virtualization and emulation to capture more malicious behavior across

a wider range of custom environments. Full results of the analysis are passed back to Tripwire Enterprise, which can be used to tag the file assets as malicious. This sequence dramatically speeds up the process to validate and prioritize actions for the incident response team, thereby reducing the time to remediate threats. The diagram below demonstrates how this process works.


Malware Analysis
Threat Detected!
6 Updates Sent to Global Intelligence Network
3
New Advanced Threat Detected 4
2 Send File/Hash for Analysis
1 New Binary Found
TRIPWIRE® ENTERPRISE
Tripwire Enterprise Agent
5 Drive pivot to investigate and remediate system

Determining the scope of the breach

Tripwire and Blue Coat have created two pivots between Security Analytics and Tripwire Enterprise and Tripwire Log Center.

Tripwire Enterprise and Security Analytics: Upon an alert of a suspicious event that has been captured by Blue Coat Security Analytics, the Incident responder can quickly review all the recorded data, perform root cause analysis and then pivot into Tripwire Enterprise to correlate and verify for the existence of malicious behavior at the suspected endpoint(s). Security Analytics allows rapid contextual pivots using IP Address, domain name or file hash.

Tripwire Log Center and Security Analytics: If the incident response team is alerted to unusual behavior from Tripwire Log Center, the team can quickly pivot directly into Security Analytics using a series of search parameters, such as IP Source and Destination, Port Source and Destination as well as start and end time/date. The investigating team can quickly pivot between the endpoint data and a rich set of recording network data to look for anomalies and quickly ascertain if they need to take action.

Benefits

Together, Tripwire Enterprise and the Blue Coat Security Portfolio:

- Dramatically reduces time-to-discovery and time-to-response
- Provides complete visibility network to endpoint
- Allows security analysts to prioritize alerts
- Provides rapid investigation and pivot to remediation

About 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 cyber security 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.

Tripwire solutions also deliver actionable reports and alerts and enable the integration of valuable endpoint intelligence into operational systems like change management databases, ticketing systems, patch management and security solutions including SIEMS, malware detection and risk and analytics. These integrations are part of our Technology Alliance Program and they ensure our customers have robust, accurate information to make their organizations more cyber-secure. To learn more, please visit: www.tripwire.com.

For More Information

Learn more about Blue Coat technology partners on our website.

BLUE COAT®

Network
+ Security
+ Cloud

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000