Technology Partner

Partner Product:
Security Analytics Platform

Guidance Software Product:
EnCase Endpoint Security

GUIDANCE SOFTWARE AND BLUE COAT PARTNERSHIP:

WHERE NETWORK ANALYTICS MEETS ENDPOINT SECURITY

SOLUTION OVERVIEW

The Blue Coat and Guidance Software partnership allows an enterprise to achieve comprehensive protection against advanced malware and zero-day attacks across the network and through all of its endpoints.

Using a fully-indexed and classified record of all network traffic captured by the Blue Coat Security Analytics Platform, security analysts are able to see potential threats over the network, with EnCase Endpoint Security answering critical questions regarding potentially infected endpoints.

With complete visibility into the enterprise via the Blue Coat and Guidance partnership, security professionals may quickly answer pertinent questions about the source and scope of the threat, including:

- Are there undetected threats actively operating within my enterprise?
- Which threats pose the greatest risk?
- Is sensitive data or regulated data involved in the attack?
- How did it happen?
- What actions are necessary to remediate the problem?

The Security Analytics Platform extracts and reconstructs all attributes associated with advanced malware and threats – including every packet, flow, file, application and detailed server information as well as source and destination IPs. Combining Security Analytics with the Blue Coat Malware Analysis Appliance, you have details of previously unknown malware that has been thoroughly analyzed by next-generation sandboxing and malware detonation.

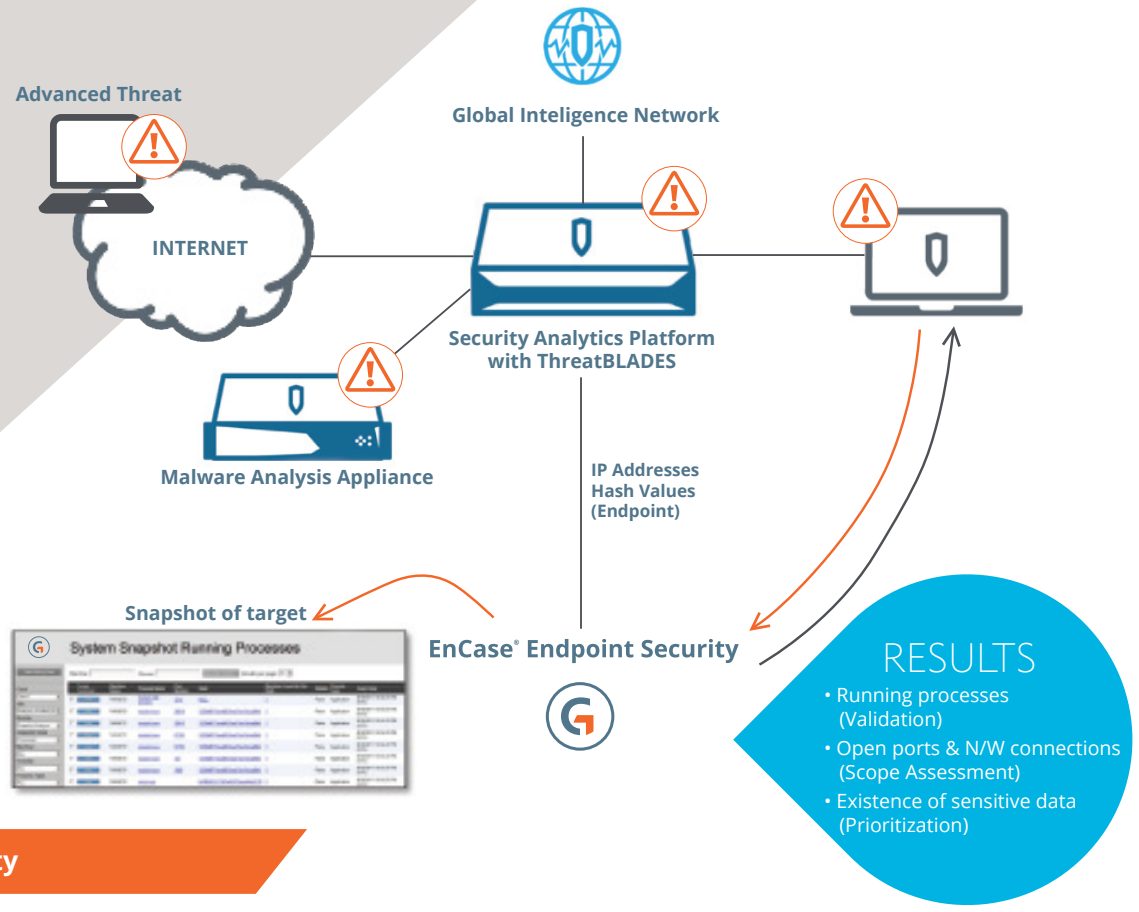
The Security Analytics technology also leverages the Blue Coat Global Intelligence Network – aggregated threat intelligence from 15,000 customers and 75 million users – and Blue Coat ThreatBLADES providing instant, actionable intelligence about web, email, or file-based threats.

This critical threat data can be automatically passed to EnCase Endpoint Security where it can immediately validate all of the infected endpoints. It provides details about whether the malware actually executed and reports on all activity at the exact endpoint. After validation and scope assessment, EnCase Endpoint Security can launch remediation commands, allowing security analysts to completely eradicate it and quickly return the network to a trusted state. Comprehensive attack details captured from both network traffic and endpoints empower security teams to fortify networks and endpoints against any subsequent attacks.

HOW IT WORKS

Integrated Workflows

Blue Coat Security Analytics Platforms acts as a security camera on the wire, uncovering actionable intelligence about security threats to applications, files, and web content. With this retrospective look, you can quickly identify the targeted attacks that slip past traditional prevention-based security tools. The integrated workflow between the two solutions enables Security Analytics Platforms to automatically initiate incident response related queries to potentially effected endpoint via EnCase Endpoint Security. EnCase Endpoint Security validates whether the threat successfully installed and/or executed on indicated endpoints, queries for the existence of sensitive data, captures details related to the attack that exist only on its target computers.



Rapid Triage 360° Visibility

The combined Blue Coat Security Analytics and EnCase Endpoint Security capabilities are delivered on platforms drawing upon the most comprehensive visibility into network and endpoint threat information.

The Security Analytics Platform integrates directly with Blue Coat ThreatBLADES. Leveraging the Blue Coat Global Intelligence Network and the "network effect" from more than 15,000 customers and 75 million users, ThreatBLADES provide instant, actionable intelligence about web, email, or file-based threats. The real-time file extraction capability automatically extracts and inspects files to enable immediate, identification of known threats and optimizes malware sandboxing by eliminating known threats.

The Blue Coat Malware Analysis Appliance bridges the gap between blocking known malware, and detecting and analyzing unknown and advanced malware. Integrated with the Security Analytics Platform, the appliance simulates a customer's actual production systems to detect malware and uses custom virtual environments for faster anomaly detection. The Malware Analysis appliance provides a map of the damage a threat would cause if allowed to run in any network, enabling containment of zero-day threats and unknown malware, intelligence on new threats is then shared with the Security Analytics Platform for eradication.

EnCase Endpoint Security is built on EnCase technology, the gold standard for digital investigations. EnCase Endpoint Security is driven by forensics processes and technologies configured to automatically deliver a complete, unobstructed view of the endpoint the moment an alert is received. A non-resource intensive agent on each system performs all needed activities and can be disguised to prevent deletion by malware or notice by malicious insiders. The entire operation is transparent to users to avoid disruption or tipping off potential suspects, and works on a wide variety of operating systems for laptops, desktops, file servers, email servers, print servers and even POS systems. This ensures that as attackers adopt new techniques or new vulnerabilities are exploited, your security technology can adapt to meet the challenges associated with detecting zero-day and unknown threats.

Comprehensive

Once assessed, the combined solution allows you to block the spread of infection, as well as eliminate the threat from compromised endpoints, recovering your operations with no disruption to business. Additionally, information and results throughout the entire process are recorded for forensic analysis to assist federal law enforcement in identifying and prosecuting state-sponsored and criminal groups.

KEY FEATURES & BENEFITS

With Blue Coat Security Analytics Platform and EnCase Endpoint Security you can:

- Control the risks and costs associated with a network breach
- Proactively identify and validate zero-day and undetected threats across network and endpoints
- Prioritize response to the most critical threats
- Reconstruct the evidence and associated files
- Quickly remediate and recover from unknown threats across the network and endpoints

1055 East Colorado Blvd
Pasadena, CA 91106-2375

T. (626) 229-9191

guidancesoftware.com

experts@guid.com

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

ABOUT BLUE COAT

Blue Coat is a leading provider of advanced web security solutions for global enterprises and governments. Our mission is to protect enterprises and their users from cyber threats – whether they are on the network, on the web, in the cloud or mobile.

Blue Coat protects and serves over 15,000 organizations every day, including over 70% of the Fortune Global 500. We partner with Chief Security Officers and network and security operations teams to address fundamental shifts in their computing landscape – with equally vital network, security and cloud implications. The Blue Coat Security Platform unites network, security and cloud technologies to maximize security protection, minimize network impact and fully embrace cloud applications and services. The platform was forged by Blue Coat's 20+ years of front-line security experience, fortified by deep engineering and research prowess.