BLUE COAT®

Security Empowers Business

BLUE COAT TECHNOLOGY PARTNER: GUIDANCE SOFTWARE

SOLUTION BRIEF

Problem

Advanced. Stealthy. Low and slow. Zero-day and unknown. Many attacks are designed to evade your perimeter security – or are so new that a solid defense strategy has yet to be created. This malware can go completely undetected or hide among the countless alerts received each day, exploiting your network and endpoints, customer data and trade secrets behind your back. Preventative measures offer no defense against these advanced attacks. What's needed is an integrated and holistic approach to detection and response across network and endpoints. You need the ability to answer key questions quickly in order to effectively detect, validate, prioritize, respond to, remediate, and recover from the most critical of these threats – before irrecoverable damage is done.

As an information security professional tasked with information threat defense, you need complete visibility into the enterprise to quickly answer critical 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 or regulated data involved?
- How did it happen?
- How do I get rid of the threat?

Solution Overview

The Blue Coat and Guidance Software partnership enables an enterprise to gain comprehensive protection against advanced malware and zero-day attacks across the network and the endpoint.

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 CyberSecurity answering critical questions regarding potentially infected endpoints.

The Security Analytics Platform extracts and reconstructs all attributes associated with advanced malware and threats – including source and destination IPs, every packet, flow, file, application and server information. 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.

Guidance® SOFTWARE

Partner: Guidance Software

Partner Product: EnCase Cybersecurity

Blue Coat Products: Security Analytics Platform

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, which provide instant, actionable intelligence about web, email, or file-based threats. With this critical information automatically passed to EnCase Cybersecurity, the solution immediately validates any/all infected endpoints and provides details about whether malware actually executed, while reporting on the exact endpoint activity itself. Following validation and scope assessment, EnCase Cybersecurity can launch remediation commands, allowing security analysts to completely eradicate zero-day malware from all endpoint systems and quickly recover from any affect or impact. Additionally, comprehensive attack details captured from both network traffic and endpoints enable the security team to fortify the network and endpoints against any subsequent attacks.

How it Works

Integrated, Automated Workflows across Network Traffic and Endpoints

Security Analytics acts as a security camera on the wire, uncovering actionable intelligence about security threats to applications, files, and

BLUE COAT®

Security Empowers Business

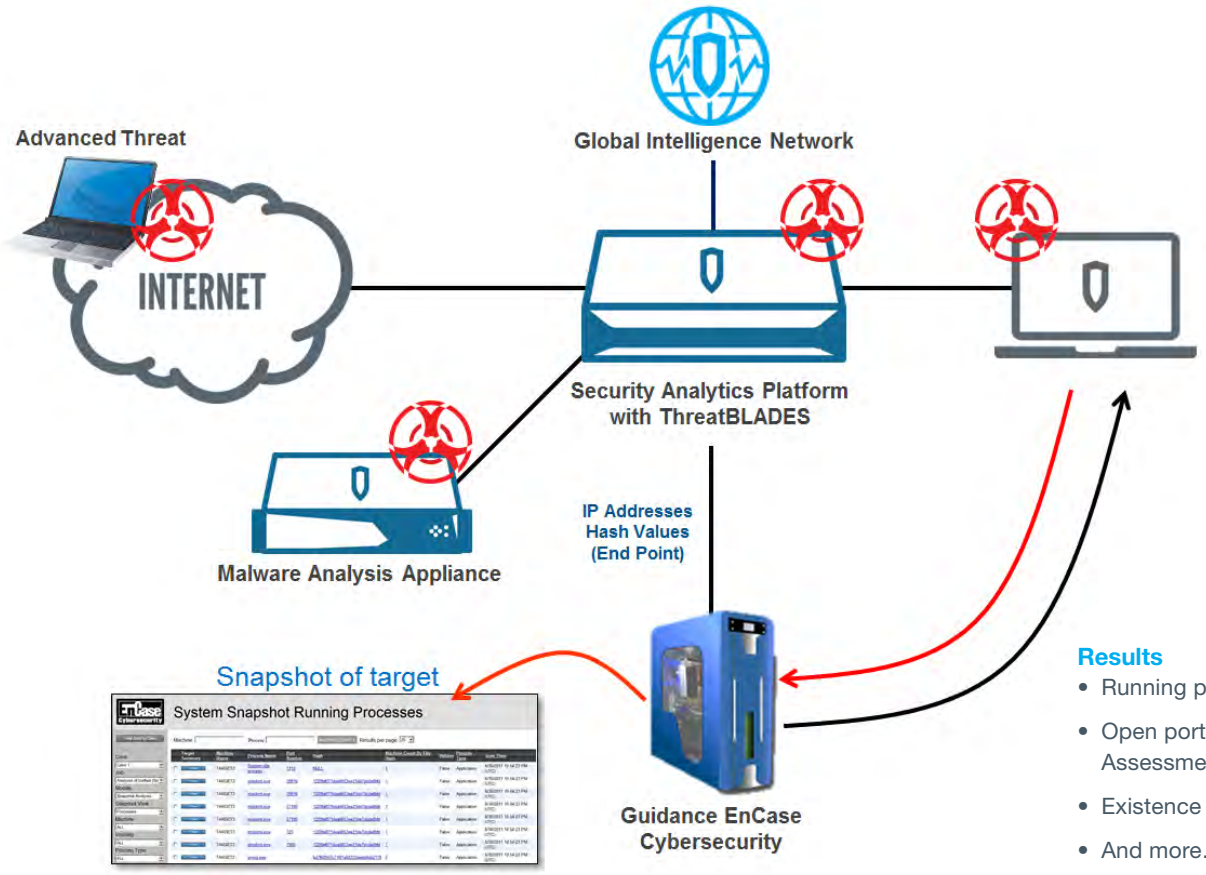
SOLUTION BRIEF

web content. With this retrospective look at traffic on the network, you can quickly identify the stealthy and targeted attacks that slip past traditional prevention-based security tools. The integrated workflow between the two solutions enables Security Analytics to automatically initiate incident response related queries to potentially effected endpoint via EnCase Cybersecurity. EnCase Cybersecurity 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, looks for lateral spread, and more.

Rapid Triage with 360° Visibility

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

The Security Analytics Platform integrates directly with Blue Coat ThreatBLADES to deliver a real security game changer. Leveraging the Blue Coat Global Intelligence Network and the “network effect” from more than 15,000 customers and 75 million users, the ThreatBLADES provide instant, actionable intelligence about web, email, or file-based



Results

- Running processes (Validation)
- Open ports & N/W connections (Scope Assessment)
- Existence of sensitive data (Prioritization)
- And more…

SOLUTION BRIEF

BLUE COAT®

Security Empowers Business

threats. The real-time file extraction capability automatically extracts and inspects files to enable immediate, automatic identification of known threats and optimizes malware sandboxing by eliminating known threats from unnecessary detonation.

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 evasive malware and uses custom virtual environments for faster anomaly detection. Without ever putting actual systems or applications at risk, 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. After detection and analysis, intelligence on new threats is shared with the Security Analytics Platform for eradication of the full scope of the attack.

EnCase Cybersecurity is built on EnCase technology, the global standard for forensic and digital investigations of all kinds. EnCase Cybersecurity 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 tiny, passive service 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 Remediation

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 who are targeting your business.

Key Features and Benefits

With Blue Coat Security Analytics Platform and EnCase Cybersecurity 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

Redefining Cyber-Defense

The combined Security Analytics Platform and EnCase Cybersecurity solution equips your team with the means to achieve 360-degree view and control of all endpoint data and network traffic, enterprise-wide — enabling a dramatic reduction in the time needed to detect and remediate both known and unknown threats.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® Enterprise platform is used by numerous government agencies, more than 70 percent of the Fortune 100, and more than 40 percent of the Fortune 500, to conduct digital investigations of servers, laptops, desktops and mobile devices. Built on the EnCase Enterprise platform are market-leading electronic discovery and cyber security solutions, EnCase eDiscovery, EnCase Cybersecurity, and EnCase Analytics, which empower organizations to respond to litigation discovery requests, perform sensitive data discovery for compliance purposes, conduct speedy and thorough security incident response, and reveal previously hidden advanced persistent threats or malicious insider activity. For more information about Guidance Software, visit www.encase.com.

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