BLUE COAT

Security Empowers Business

Solution Brief

Advanced Threat Protection

A Complete Lifecycle Approach to Advanced Threat Protection

More than 100,000 new malware samples alone are discovered every day, and exploits are evolving and diversifying quickly. Meanwhile, today's unknown malware and zero-day threats continue to evade even the best traditional security defenses. According to the 2013 Verizon Data Breach Report, 84 percent of attacks took only seconds, minutes, or hours to compromise their targets, while 78 percent of breaches took weeks, months, or years to discover.

Consequently, there is a shift toward a new approach that integrates real-time protection, dynamic analysis and post-breach investigation and remediation. This approach closes the gap that exists between ongoing security operations and incident discovery, containment and resolution. The net result: your business can move beyond fear and start focusing on possibilities.

Blue Coat: Uniquely Capable of Addressing the Requirements

The Blue Coat Advanced Threat Protection solution integrates technologies from the Blue Coat Security and Policy Enforcement Center and the Resolution Center. It delivers a comprehensive, integrated and modern approach to advanced persistent threats, advanced targeted attacks, advanced malware, unknown malware and zero-day threats through its Advanced Threat Protection Lifecycle Defense.

This defense is the first to integrate a business process view that aligns with how your security team operationalizes new intelligence and technologies to fortify your security infrastructure against future attacks. The Blue Coat Advanced Threat Protection Lifecycle Defense operates in three stages:

- **Detect and Protect for Ongoing Security Operations**: The Blue Coat Secure Web Gateway and Blue Coat Content Analysis System with malware scanning engines, protect in real-time against known threats, malicious sources, and malware delivery networks. Contextual information about new threats is shared locally and globally via the Blue Coat global intelligence network in a continuous feedback loop that extends threat knowledge and protection effectiveness.
- **Analyze and Mitigate for Incident Containment**: Unknown threats are escalated for incident containment using the Blue Coat Content Analysis System and Security Analytics Platform, which both use the Blue Coat Malware Analysis Appliance. As the behaviors and characteristics of unknown or advanced malware and zero-day threats are learned through automated analysis, that intelligence is shared across the security infrastructure, shifting protection to the gateway for a more scalable defense.
- **Investigate and Remediate for Incident Resolution**: The Security Analytics Platform allows security incident escalation for retrospective analysis to enable threat profiling and incident resolution. Intelligence of the now-known threat is used to investigate and remediate the full scope of the attack, including other instances of the threat already on the network. The intelligence on the full scope of the attack is shared locally across the security infrastructure as well as globally across Blue Coat's 15,000 customers and 75 million users to operationalize the new knowledge and fortify the security infrastructure.

BLUE COAT

Security Empowers Business

Blue Coat Global Intelligence Network

STAGE 1: ONGOING OPERATIONS

- Blue Coat Secure Web Gateway
- Blue Coat Content Analysis System with malware scanning and whitelisting
- Blue Coat SSL Visibility Appliance

STAGE 2: INCIDENT CONTAINMENT

- Blue Coat Content Analysis System with malware analysis
- Security Analytics Platform by Solera, a Blue Coat company, with Blue Coat ThreatBLADES and Malware Analysis Appliance

STAGE 3: INCIDENT RESOLUTION

- Security Analytics Platform

Figure 1: Blue Coat Advanced Threat Protection Solution seamlessly combines local and global threat intelligence to turn unknown threats into known threats – increasing the overall effectiveness of the security infrastructure against today's advanced threats.

Shared Threat Intelligence: Fortifying the Security Infrastructure

The Blue Coat Advanced Threat Protection solution relies on local and global intelligence-sharing at each stage of the incident lifecycle defense to fortify the security infrastructure. New threat intelligence is shared across your security infrastructure, as well as globally with 15,000 Blue Coat customers and their 75 million users.

This powerful network effect drives an increase in defense scalability and effectiveness by turning unknown threats into known threats that can then be blocked at the gateway in the future. This delivery of new threat intelligence back to the gateway assures faster inoculation against dynamic and emerging threats.

Best-of-Breed: Optimize Your Existing Security Investments

The Blue Coat Advanced Threat Protection solution is designed to integrate into your existing security infrastructure, including your IPS, NGFW, SIEM and malware sandbox solutions, allowing you to deploy a defense-in-depth approach that shares information to increase protection.

For example, the solution is designed to act as a neutral and open broker for sandboxing solutions by passing unknown or suspicious files to both the Blue Coat Malware Analysis Appliance and/or other third-party sandboxing tools. With this integrated capability to serve files for analysis across multiple systems, you have the flexibility and freedom of choice to build a comprehensive defense against targeted attacks and unknown threats.

BLUE COAT

Security Empowers Business

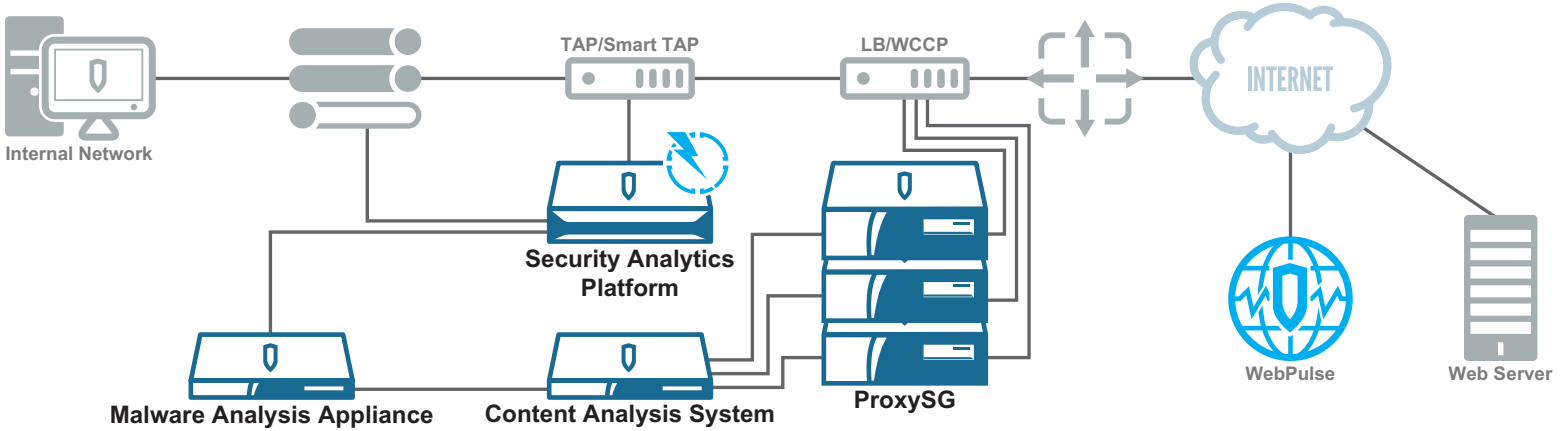

Figure 2: Blue Coat Advanced Threat Protection Reference Architecture.

Summary: Benefits and Advantages

Blue Coat is the only company that provides a business-process oriented approach that integrates ongoing operations with threat detection, incident containment and resolution. The table below summarizes the business advantages of the Blue Coat Advanced Threat Protection Solution.

BUSINESS-PROCESS ORIENTED DEFENSE	The lifecycle approach aligns defenses to the business process for operationalizing new threat intelligence to fortify the security infrastructure.
SCALABLE, EFFECTIVE DEFENSE AGAINST ZERO-DAY THREATS AND UNKNOWN MALWARE	Through the Advanced Threat Protection Lifecycle Defense, unknown threats become known threats so protection against future attacks can be shifted to the gateway.
GLOBAL AND LOCAL SHARING OF THREAT INTELLIGENCE	At each stage of the lifecycle defense, new threat intelligence is shared both locally across the security infrastructure and globally across 15,000 customers and their 75 million users to create a network effect.
OPTIMIZED SECURITY INFRASTRUCTURE INVESTMENTS	The Blue Coat Advanced Threat Protection solution integrates into your existing security infrastructure to provide a stronger defense in-depth strategy against advanced attacks and malware.

Learn More

Get the details about the Blue Coat Advanced Threat Protection solution by scheduling an appointment with your Blue Coat representative today. For contact information visit www.bluecoat.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