



Security  
Empowers  
Business



# BLUE COAT TECHNOLOGY PARTNER: CYPHORT

SSL encrypted traffic is pervasive in organizations around the world, representing 35% of all enterprise network traffic today.<sup>1</sup> With a 20% annual growth rate, SSL encrypted traffic increasingly presents a blind spot in organizations; most current security solutions cannot see or manage this traffic or the threats that hide within. Advanced Persistent Threats (APTs) are increasingly using SSL-based attacks, with Gartner predicting that 50% of all network attacks will be encrypted by 2017.<sup>2</sup> Security tools such as Next Generation Firewall (NGFW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Data Leak Prevention (DLP), security analytics and malware analysis devices are typically blind to SSL traffic or experience significant performance degradation if SSL inspection is enabled. A new approach is clearly needed.

## Solution: Blue Coat SSL Visibility Appliance and Cyphort Advanced Threat Defense Platform

Blue Coat's encrypted traffic management (ETM) solution eliminates the encrypted traffic blind spot and combats the security threats hidden in encrypted traffic while preserving privacy, policy and regulatory compliance. Comprised of the market-leading Blue Coat SSL Visibility Appliance, it enhances existing security solutions by providing visibility into previously hidden traffic and advanced threats without requiring significant upgrades or re-architecting the network security infrastructure.

The SSL Visibility Appliance is a high-performance purpose-built solution that utilizes comprehensive policy enforcement to inspect, decrypt and manage SSL traffic in real time while ensuring data privacy and regulatory compliance. The SSL Visibility Appliance's unique "decrypt once, feed many" design empowers multiple security tools, such as the Cyphort Advanced Threat Defense Platform, with new-found visibility into encrypted traffic to effectively detect and eliminate advanced threats without hindering device or network performance. The combination of the SSL Visibility Appliance and the Cyphort Advanced

Threat Defense Platform delivers best-in-class ETM to decrypt SSL traffic to uncover hidden threats and eliminate these SSL blind spots.

The Cyphort Advanced Threat Defense Platform accurately detects and analyzes next generation malware, providing actionable, contextual intelligence that enables security teams to respond to attacks faster, more effectively, and in as surgical a manner as their attackers. The ability to detect and automatically prioritize threats based on business risk empowers Cyphort customers to remediate the most damaging attacks with velocity. Built-in integration with third party enforcement devices allows customers to contain threats as they are discovered.

The Blue Coat SSL Visibility Appliance is an integral component to an organization's encrypted management strategy, and provides visibility into SSL encrypted traffic without requiring the re-architecting of the network infrastructure. The SSL Visibility Appliance gives the Cyphort Advanced Threat Defense Platform visibility into all SSL traffic and applications to close the security visibility loophole created by encrypted traffic. In addition, it has the ability to selectively decrypt and inspect suspicious or unknown encrypted traffic while not inspecting other SSL traffic due to mandates such as HIPAA, SOX, PCI, Sarbanes-Oxley, and so on.



**Partner:** Cyphort Inc.

**Partner Product:** Cyphort Advanced Threat Defense Platform

**Blue Coat Product:** SSL Visibility Appliance

<sup>1</sup> NSS Labs, "SSL Performance Problems," <https://nsslabs.com/reports/ssl-performance-problems> June 2013.

<sup>2</sup> Gartner "Security Leaders Must Address Threats From Rising SSL Traffic". Published: 9 December 2013

### How it Works:

The diagram below demonstrates how the Blue Coat and Cyphort solutions work together to provide best-in-class ETM.

The Blue Coat SSL Visibility Appliance provides decrypted content from SSL flows to the Cyphort platform. Based on its unique “decrypt once - feed many” design, the SSL Visibility Appliance can also simultaneously share its decrypted data with other existing security appliances that support next generation firewall, malware analysis, forensics, compliance and DLP if present. The joint solution allows enterprises to easily add SSL visibility and inspection capabilities, along with category-based inspection policies into their existing network security architectures.

The Cyphort Advanced Threat Detection solution is delivered as software that can be distributed as Cyphort Collectors and Cyphort Cores with updates from the Cyphort Threat Network. Collectors are software-based sensors deployed at strategic network locations, such as Internet egress points, data centers and branch offices. Collectors monitor traffic across web and email applications, ‘collecting’ files to be inspected for the presence of malware. Cyphort Core software contains the advanced threat detection and mitigation logic. Collectors forward the collected network objects, including objects hidden in SSL and associated metadata to the Cyphort Core for analysis. The Cyphort Core also includes an analytics engine for accurate threat classification, which correlates the aggregated data for verification and mitigation of attacks. The Cyphort solution leverages the Threat Network, a cloud service that feeds global threat intelligence to the Cyphort Core for enhanced detection of current threats. Cyphort requires no configuration changes to inspect decrypted traffic from the SSL Visibility Appliance.

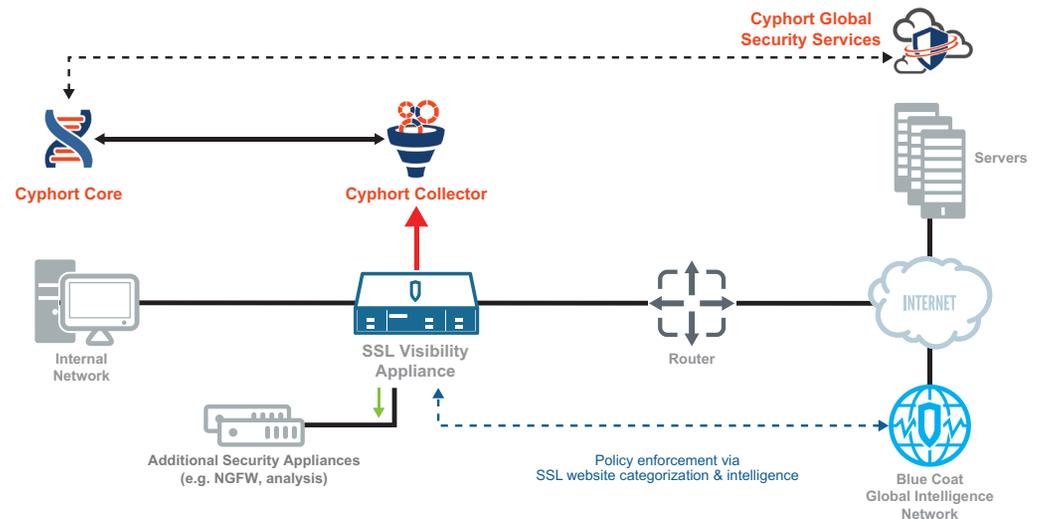
### Benefits

The combined SSL Visibility Appliance and Cyphort Advanced Threat Defense Platform:

- Provides best-in-class ETM to detect and eliminate the SSL encrypted traffic blind spots
- Preserves privacy, policy and regulatory compliance
- Provides visibility into advanced malware traffic
- Integrates seamlessly with existing infrastructure

### About Cyphort

Founded in 2011 by a team of security experts, Cyphort offers an advanced threat defense that goes beyond malware detection to reveal the true intent of an attack and the risk it poses to your organization while offering prioritized and expedited remediation. Our software-based approach combines best-in-class malware detection with knowledge of threat capabilities and your organizational context to cut through the avalanche of security data to get at the threats that matter so you can respond with velocity, in hours not days. To learn more about Cyphort visit [www.cyphort.com](http://www.cyphort.com).



© 2015 Blue Coat Systems, Inc. All rights reserved. Blue Coat, the Blue Coat logos, ProxySG, PacketShaper, CacheFlow, IntelligenceCenter, CacheOS, CachePulse, Crossbeam, K9, the K9 logo, DRTR, MACH5, PacketWise, Policycenter, ProxyAV, ProxyClient, SGOS, WebPulse, Solera Networks, the Solera Networks logos, DeepSee, “See Everything. Know Everything.”, “Security Empowers Business”, and BlueTouch are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only. Blue Coat makes no warranties, express, implied, or statutory, as to the information in this document. Blue Coat products, technical services, and any other technical data referenced in this document are subject to U.S. export control and sanctions laws, regulations and requirements, and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws, regulations and requirements, and acknowledge that you have the responsibility to obtain any licenses, permits or other approvals that may be required in order to export, re-export, transfer in country or import after delivery to you. v.SB-TECHPARTNER-SSL-CYPHORT-EN-v1b-0215