BLUE COAT®

Security Empowers Business

SOLUTION BRIEF

TOP FIVE REASONS TO CHOOSE BLUE COAT

Find out what's missing from your current solution

Cybercriminals are constantly devising new ways to steal valuable information from companies like yours. 2015 continues to see malware delivery networks (malnets) as a dominant force in the threat landscape. These infrastructures enable cybercriminals to quickly exploit new security vulnerabilities and repeatedly launch attacks. By targeting popular web destinations such as search engines, social networking sites and email, attacks originating from malnets have become very adept at infecting many users with little added investment. Cyber criminals are also taking advantage of encryption, originally devised to increase security, to further hide malicious activity from detection.

To defend against these types of attacks, your security solution must understand how these attacks work and provide an equally innovative and agile defense system. Your solution must also be effective for all end-users, on all their devices, regardless of how they connect to the internet. It only takes one big security breach to inflict lasting damage to your company's reputation, confidential data or end-user productivity.

Here are the top five ways Blue Coat's web security solutions help prevent malware from harming your business. Can your current vendor do the same?

1 Advanced Security Architecture

The choice is yours to include the state-of-the art security solutions

Blue Coat's secure web gateway offers the most flexible and advanced architecture when it comes to combining and integrating the latest security technologies in your secure web gateway solution. By offering a flexible architecture that includes the Content Analysis System, Blue Coat lets administrators pick and choose the technologies they need and want, and allows them to integrate best-of-breed technologies into their existing infrastructure using ICAP and sandbox brokering.

The Content Analysis System already offers leading edge security solutions including whitelisting, static code analysis, and dual anti-malware engines (selectable by the administrator). It also offers the ability to broker files that have successfully passed through the detection engines to multiple sandboxes, including FireEye and Blue Coat's own sandbox appliance, the Malware Analysis Appliance.

Blue Coat is also the only vendor to give organizations a choice in anti-malware engines. While many recognize that no single anti-malware engine can provide 100% coverage, selecting the appropriate anti-malware solution(s) is a critical decision for every enterprise. Factors such as anti-malware/anti-virus on desktops, frequency of updates, and vendor relationships all impact the ideal anti-malware solution for your enterprise.

Blue Coat delivers the flexibility to choose among multiple industry-leading anti-virus engines, including Kaspersky, McAfee and Sophos, and can run two engines at the same time. As a result, organizations are able to deploy the solution that best addresses their specific requirements and preferences, without compromising the need for best-of-breed technologies.

Websense offers limited options to integrate with the AV engine of choice, and other best-of-breed security solutions, and hence does not offer the same level of coverage or flexibility needed by today's enterprises.

2 Negative day defense

Stop malware at the source

Blue Coat Labs has found that nearly two-thirds of all new attacks originate from known malware delivery networks (malnets). However, the entrenched nature of these malnets and, in some cases, their geographic diversity, makes it nearly impossible to shut them down. What's worse, traditional network security is simply not designed to

Security Empowers Business

protect businesses against sudden attacks from established malnet infrastructures.

The best protection against attacks originating from malnets is Blue Coat's negative day defense – a unique and robust approach to security that can locate and block the source of malicious attacks before they launch.

Because malnets rely on a sustained infrastructure, Blue Coat can identify the source of the attack regardless of the attack payload. By mapping the relationships between malnet components, Blue Coat can quickly identify and block new subnets, IP addresses and host names when they come online. Once the malnet infrastructure has been identified it can be blocked at the source, even before attacks are launched.

❸ Speed and visibility without compromise

Get outstanding performance and security

The growing sophistication of web content and modern malware, and the increased use of encryption by websites require significant computing power to analyze and decrypt traffic in real time. But most security solutions are limited by the speed of their appliances and typically lack any support in hardware for decryption. As a result, legacy web security solutions force enterprises to choose between real-time web traffic analysis and acceptable network throughput.

Blue Coat changes all that with WebPulse, a part of the Blue Coat Global Intelligence Network, combined with our Encrypted Traffic Management solutions. As the backbone of all Blue Coat web security solutions, WebPulse analyzes more than one billion URLs a day and can scale indefinitely with network demand. Blue Coat's secure web gateway will in most cases provide URL ratings in less than 8 msec., but if a user encounters an unrated site, WebPulse will conduct a completely new analysis in approximately 200 msec.

By utilizing hardware assist for encryption and decryption, and also offering a dedicated SSL Visibility Appliance, Blue Coat offers the best performance and visibility for encrypted traffic. Without SSL Inspection, a secure web gateway is blind to an average 40% of internet traffic.

By contrast, competitive solutions like Websense rely on selective scanning of URL content or risk complete appliance failure. The shortcomings of these solutions are due to architecture limitations of their on-premise appliances and their reliance solely on slower software-based encryption and decryption. This requires the appliances to be configured to selectively scan URLs, which can result in malware slipping into your network.

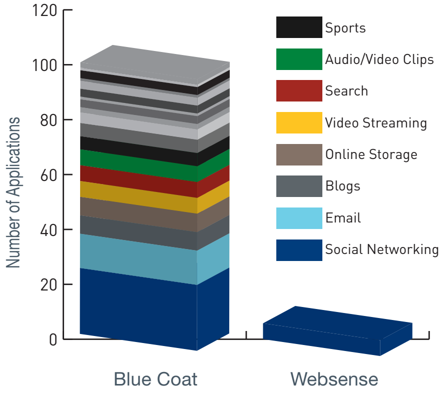
❹ Web, mobile web, and native application controls

Manage how applications are used

Granular web, mobile web, and native application controls make it easier to manage specific Internet activities without blocking entire websites or applications. Blue Coat's web policy engine allows IT to create granular policies to help prevent misuse of various capabilities available on these applications. For example, IT can enable Facebook use for business communications while disabling comment posting, media uploads, messaging, and games within the site.

Blue Coat provides over 200 web, mobile web, and native application controls for more than 100 applications and websites including Facebook, YouTube, Gmail, LinkedIn, Box, Dropbox and more. On the other hand, solutions such as Websense provide no mobile application controls and only a handful of social networking applications. Only Blue Coat has the comprehensive application controls needed to help businesses maximize bandwidth, minimize security risks and extend corporate and regulatory policies for network access and use.

These applications can be used and are accessed on any network, in any location, by any user in the organization. In addition to providing controls, for web, mobile, and native applications, Blue Coat offers the ability to implement these controls by deploying a hybrid solution (on-premise, virtual, and in the cloud) for any device (Mac, Windows, iOS, Android), and protecting the device on any network. Administrators get reporting and management for all users, in a single view across the entire hybrid solution.



Blue Coat supports a wide range of web application controls spanning multiple categories

BLUE COAT®

Security Empowers Business

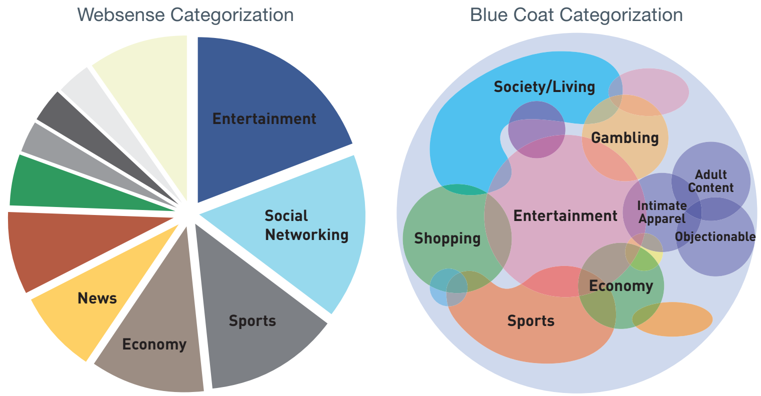
SOLUTION BRIEF

❺ Multi-dimensional categories

Get the most accurate URL ratings

Traditional URL filtering assumes that a URL can be described with a single category, such as Sports, Entertainment or Social Networking. As a result, IT must apply a blanket “allow or deny” policy to sites that fall within these categories. While this approach might work for some explicit URLs, it’s less effective for sites such as Facebook, which cannot be easily characterized by a single category.

To provide more accurate URL ratings, Blue Coat supports multi-dimensional categories – a modern approach to URL filtering that assigns up to four categories to the various types of content on a page. Not only do multiple categories provide a more accurate description of page content, IT administrators can easily set policies based on any or all of the available categories. This approach provides the highest level of policy accuracy to protect users from malicious content.



Rather than discrete categories, Blue Coat applies multi-dimensional rating to enable the highest level of security and productivity

Learn more:

To learn more about our solutions please visit us here www.bluecoat.com/protect-the-web or contact us at www.bluecoat.com/contactus.

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

© 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-TOP5-BLUECOAT-ADVANTAGES-EN-v4a-0615