

**Blue Coat WebPulse™ >**

Technical Overview of the WebPulse Collaborative Defense

## Table of Contents

<b>INTRODUCTION</b>	<b>1</b>
<b>BLUE COAT'S WEB SECURITY ARCHITECTURE</b>	<b>2</b>
PROACTIVE DEFENSES	2
BLUE COAT WEBFILTER / WEBPULSE – HIGH LEVEL OVERVIEW	3
How it works	3
RECOMMENDED FEATURES FOR MALWARE PROTECTION	4
URL filtering	4
Authentication	5
Controlling data types	5
Protocol compliance	5
SSL interception	5
Malware scanning	5
Log file analysis / reporting	5
<b>WEBPULSE TECHNICAL OVERVIEW</b>	<b>6</b>
CLASSIFICATION ACCURACY	6
Multiple ratings per URL	6
Prevent users from bypassing the content filter policy	6
Quality checks	7
PERFORMANCE	7
DYNAMIC REAL-TIME RATING (DRTR) AND DYNAMIC LINK ANALYSIS	7
Real-time malware detection modules	8
URL background checker	8
BACKGROUND ANALYSIS TECHNIQUES	8
MALWARE DETECTION	9
Detection and analysis of malicious traffic	9
Malicious site and content identification & analysis	9
Malicious site fingerprinting	9
Web reputation	9
Malicious PDF detection	9
Malicious JavaScript detection	10
Malware content analyzers	10
Malware signature scanners	10
Malware behavioral scanners	10
Phishing detection	10
Detection of Illegal or questionable sites (scam sites)	10
Third-party intelligence	10
Active user community	11
Immediate availability of malicious content identification to WebPulse users	11
MALWARE DELIVERY NETWORKS ANALYSIS	11
WEB APPLICATION AND WEB APPLICATION OPERATION CONTROLS	12
Managing web application and web application operation changes	12
<b>CONCLUSION</b>	<b>13</b>

## Introduction

The web has become an integral part of every business. At the same time, social media has transformed the web into a dynamic and complex environment – ideal for the proliferation of malware in increasingly covert and sophisticated ways.

This evolving environment makes it more difficult to manage web access and bandwidth use. It also introduces security challenges that web filtering may be uniquely suited to address. With over 20 million web sites created in 2010 alone, it is critical that web security solutions provide accurate site ratings, global diverse coverage, and real-time rating of new URLs.

The Blue Coat WebPulse™ is a cloud-based infrastructure specifically designed to harness the power of user-driven behavior and to translate user input into global web and web threat intelligence. Launched in 2004, WebPulse is the most advanced and most relevant web security technology in the industry. WebPulse is a collaborative defense that powers Blue Coat web security solutions by integrating input from over 75 million diverse global users. WebPulse uses multiple technologies to analyze this input to deliver the fastest and most accurate web ratings of any vendor. Within the WebPulse framework, each incoming URL request is processed by many different threat analysis methods, both automated and manual.

WebPulse uses its cloud infrastructure to deliver web intelligence to Blue Coat Web Security solutions, both appliance and cloud-based. WebPulse seamlessly delivers frequent database updates as well as new defense types such as analytical methods and additional language support. Users benefit instantly from these new defenses and updates without having to administer updates to their appliances or SaaS service.

The intent of this document is to provide insight into the WebPulse collaborative defense, which is an integral part of Blue Coat's proactive security defenses.

## Blue Coat's Web Security Architecture

### Proactive, layered web defenses

It is no longer effective to simply detect and block threats. With the sophistication of malware techniques and the advent of mass-market malware – attacks that require little investment but achieve high penetration – web security solutions need to be proactive in anticipating and blocking malware before a business is infected.

A proactive, layered web defense requires five key components:

#### -> A global collaborative Cloud intelligence infrastructure is essential. It requires:

- An integrated, community-watch-based ecosystem that can leverage the real-time experience of users who visit millions of Web pages each day.
- A hosted, or cloud-based, infrastructure that can use multiple threat-detection engines, machine analysis and human raters to aggregate and analyze data from the user community.

#### -> Real-time content filtering

Backed by a global collaborative intelligence system, real-time content filtering combines dynamic protection with the granular category control that businesses need to implement for acceptable Internet use policies. Comprehensive category coverage and the ability to assign multiple categories to a given URL provide the multi-dimensional control that it takes to manage today's complex web environment.

#### -> Inline threat detection

Inline threat analysis is an integral component of a proactive web security solution. It can inspect SSL-encrypted traffic, as well as user-authenticated software downloads from the web, attachments sent through Webmail, and other content.

#### -> Web application and content controls

This layer consists of web content and web application controls that prevent downloads from unknown web sites, detect masquerading files, and allow or deny web applications or web application operations (for example, post message or upload attachment) based on users, groups, or other policy variables.

#### -> Protection for remote and mobile users

Remote and mobile users are steadily increasing, and they require the same level of protection as users at the corporate office. Extending the protection of WebPulse through a web-filtering client or SaaS gives these users proactive defenses and reduces their risk of bringing malware into the business network.

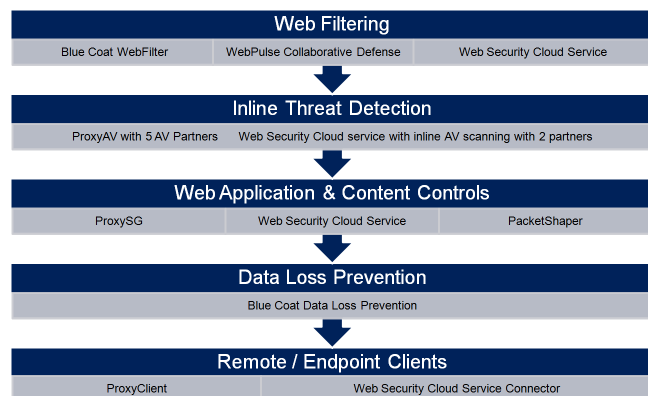


Figure 1: Blue Coat's Proactive, Layered Defenses

### Blue Coat WebFilter / WebPulse: A high-level overview

Blue Coat WebFilter™, in conjunction with the WebPulse collaborative defense, plays several key roles in this multi-layered defense. They include responding proactively against zero-day attacks, preventing 'phone home' attempts from spyware and even botnet-infected systems, and detecting phishing and malvertising threats. By preventing malware from being downloaded from the Internet, combined with in-line malware scanning by ProxyAV appliances or the web security SaaS, the defense achieves maximum effectiveness.

WebFilter and WebPulse are designed to deliver a highly responsive, proactive, front-line defense for the in-line malware scanner – not to be its replacement.

WebPulse can simply be described as a basic input-output system. The massive input is generated by more than 75 million users, including Blue Coat ProxySG and PacketShaper appliances, the Web Security Module SaaS and K9 consumer users. WebPulse – as a black box – performs real-time analysis and outputs a URL rating. The output is fast (milliseconds). Users get feedback in real time. There is no need for update cycles or patches, and nothing time-consuming or periodic to compromise protection.

This section provides a high-level look at how WebFilter and WebPulse work. The next section will reveal technical details about WebPulse – the black box.

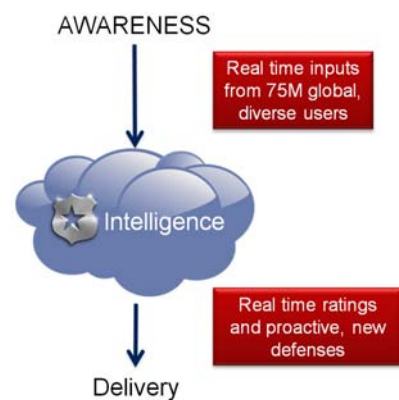
#### How it works

Requests to URLs are first checked against the local BCWF database or the local ratings cache on other Blue Coat products. If the URL can be categorized locally, the category information can be used to allow or block the request.

Typically, the percentage of locally unrated content is about five percent. If the URL is not in the local WebFilter database or ratings cache, the URL is dynamically sent to WebPulse. In the cloud the URL will first be checked against the central master database. This is comparable to the local lookup; if the URL is in the master database, the URL category will be sent back to the requesting WebPulse client and can be used to allow or block the request. The new result is automatically cached locally.

If the URL is also not in the central master database in the cloud, Dynamic Real-Time Rating (DRTR) will be used to analyze and categorize it in real time. The URL category will be sent back to the requesting WebPulse client and can be used to allow or block the request.

**Note:** It is very important to understand the principle behind the WebFilter (BCWF) philosophy. In many cases, web-based attacks start by injecting scripts into trusted web pages. These scripts typically generate a dynamic link to a malware host over a dynamic and powerful malware delivery network. The primary goal of BCWF is to analyze and block links to the malware itself. Users should never be prevented from viewing a trusted web page. The script itself does not harm the users' PC. This is fundamentally different from the approach of many vendors in the web security space, and raises these questions: Do they know where the actual malware is? If yes, why are they blocking the innocent page that hosts the link? If not, why not, since they have found the link?



Independent of the real-time rating result, the URLs will be sent to several background processes in parallel. Some of the background processes are focused on providing new content ratings for the database. Others are focused on hunting for evidence of malware activity. DRTR is primarily a content categorizer, but it is also used to log a large amount of metadata about each URL it analyzes, and it is this metadata that feeds many of the background processes. Many URLs are not web pages and are not suitable for DRTR categorizing, but WebPulse still gathers as much information about the URL as possible to feed the background processes.

WebPulse uses several methods, including sandbox techniques, to analyze scripts and detect malicious payloads and referenced domains.

When a user accesses a binary file through a URL that WebPulse has not seen before, WebPulse will also download that file and run it through a bank of up to ten different AV scanners with full heuristics, script analyzers (for example, malicious java scripts with heap sprays), sandboxes, and other malware-detection mechanisms. New threats are identified within ten minutes and automatically added to the master URL database to protect other customers.



This is one way in which WebPulse cloud users work together to provide broad real-time protection and receive a strong zero-day response to new web threats – when only a few anti-virus vendors have even been able to detect them.

In addition to Blue Coat's own analysis, several third-party URL feeds covering malware and phishing sites are reviewed for inclusion in the database. Further, when used with Blue Coat ProxyAV, ProxySG can send any URLs that ProxyAV identifies as malware sources to the WebPulse service for verification.

It's important to know that malware feeds are quality-checked before being integrated into the Blue Coat WebFilter database. This prevents false positives.

For security-related categories, incremental BCWF database updates occur every five minutes. This enables the local defense to maintain performance by responding to as many requests as possible.

### **Recommended features for malware protection**

Blue Coat's web security solutions have a broad feature set. The following section provides a brief overview about features that are useful – and recommended – for malware protection.

#### **URL Filtering**

This is the first point at which requests to known malware sources can be blocked. For URLs that are not known or not included in the local database, the ProxySG or Web Security Module connects to WebPulse collaborative defense. Unrated URLs are then analyzed in real time.

### **Authentication**

The most secure way to authenticate users is to authenticate each single new session. If the desktop is infected with malware and is authenticated, it cannot communicate with systems on the Internet (for example, to download additional malware or send out confidential information) that are the malware sources. Without this authentication, the user is vulnerable to malware attacks.

### **Controlling data types**

If users have no right to install software on their desktops, why should they be able to download executable files from the Internet? Blocking executable files is another step in protecting against malware. Often malware tries to download software to add additional malicious content on the infected desktop.

Another reason for blocking executable files is that malicious dynamic links could point to an executable malware file that would be installed on the desktop. Blocking executable files prevents this threat.

File-type blocking can be done based on true file-type detection. Blue Coat best practice recommends blocking executable files in general for regular Internet users. If this is not acceptable, they should at least be blocked for sites that are unrated. Blue Coat also maintains a Best Practices document, with additional recommendations for blocking content from certain categories.

### **Protocol compliance**

ProxySG and the Web Security Module use application proxies for several protocols. Because there are two connections – one between client and proxy and one between proxy and server – threats like buffer overflow attacks on the protocol level can be filtered out. The proxy changes protocol behavior (from server to proxy) to RFC-conforming behavior (from proxy to client).

### **SSL Interception**

SSL-encrypted traffic tunnels require a secure web gateway solution. Terminating SSL at the proxy enables detection of malicious content and tunneled applications. Certificate management can be used to verify X.509 certificates and allow only trusted client or server certificates. Non-SSL traffic attempting to exit via port 443 – which may be an indication of a malware infection – can also be blocked by the proxy.

### **Malware scanning**

The last step in malware protection is inline malware scanning. Both inbound and outbound data can be malware-scanned using ProxySG's co-processor ProxyAV or the built-in AV scanning of the Web Security Module. By default, all traffic, including large files, are scanned by ProxyAV appliances or inline with the Web Security Web Security Module. The SaaS implementation of Web Security Module is limited to scanning the initial 10Mb of attachments.

Inline AV scanning by dedicated ProxyAV appliances is a valuable differentiator from most other secure web gateway solutions, many of whom use a selective scanning approach.

### **Log file analysis / reporting**

Checking access log files on a regular basis is recommended. This means checking often enough to recognize normal traffic, so that new, unusual, or abnormal traffic can be spotted and investigated. Blue Coat Reporter is a superb tool for analyzing access log files.

## WebPulse Technical Overview

### Classification accuracy

Accuracy refers to the ability of a filtering product to categorize URLs precisely and consistently. The accuracy level answers the question, "Of the 100 URLs the filter categorized as X (Pornography, Spyware and Gambling, for example), what percentage were actually X?"; the higher the percentage, the greater the filter's accuracy. False negatives provide another accuracy indicator. The question in this case would be, "How many of type X did you miss?" Blue Coat technology delivers the most accurate categorization of any web security vendor.

WebPulse is able to rate URLs based on multiple levels:

- > Domain: all hosts of bluecoat.com could have the same rating
- > Host: host1.bluecoat.com and host2.bluecoat.com could have different ratings
- > Directory: host1.bluecoat.com/directory1 and host1.bluecoat.com/directory2 could have different ratings
- > File name: host1.bluecoat.com/directory1/good\_file.jpg and host1.bluecoat.com/directory1/malicious\_file.jpg could have different ratings
- > Query string: www.facebook.com/?sk=inbox and www.facebook.com/?sk=ff could have different ratings
- > IP address: for performance reasons (to prevent reverse DNS lookups) it is possible to add IP address-based ratings to the BCWF database
- > Protocol and header analysis is an additional rating option

**Note:** usually we talk about unrated content being sent to WebPulse by ProxySG. Technically this is not 100 percent correct. URLs categorized as "web hosting" will also be sent to WebPulse for real-time analysis to apply a more accurate rating – if necessary.

### Multiple ratings per URL

Web pages do not always fit easily into a single category. An example of this is www.facebook.com/?sk=inbox, which is both a social networking site and an email application within Facebook. An accurate web filter recognizes this and classifies the site into both of these categories, giving enterprises the flexibility to control which parts of any site can be accessed by their users. WebFilter can provide up to four categories per web page, which reflects web page content much more accurately and makes possible thousands of granular sub-category combinations for flexible and powerful policy enforcement.

### Preventing users from bypassing the content filter policy

To achieve high accuracy, WebPulse is able to prevent users from bypassing the content filter policy by accurately analyzing and classifying tools such as:

- > **Translation sites** that provide online translation of languages.
- > **Archive sites** that cache selectable content from the past.
- > **Image searches** that are delivered by a search engine.
- > **Proxy anonymizers** that relay requests via intermediary sites that are often obscure.

Early-generation filtering technology often provides only superficial ratings (examples: translation site, image search or archive site), but this is not helpful for implementing a policy. Customers do not want to block all image searches or all translation and archive requests. In contrast, Blue Coat is able to see the destination webpage embedded in the intermediary page to make an accurate and useful rating. For example, Blue Coat WebFilter accurately categorizes an archive of cnn.com as News/Media.

**Note:** *On policy-enforcing systems like ProxySG or the Web Security Module, a search engine safe-search policy can be enforced – which also helps to prevent users from bypassing the content filter policy.*

### Quality checks

The WebPulse infrastructure is supported by a set of stringent quality checks designed to reduce false positives and over blocking. All rating changes and malware identifications must pass Blue Coat's proprietary quality checks before they are released to the customer base.

### Performance

When talking about WebPulse, it's important to talk about performance. WebFilter and WebPulse provide a highly scalable high-performance solution. Only a small percentage of the overall web traffic has to be analyzed by WebPulse in real time.

WebFilter is optimized to run on-proxy (onbox). Rating requests are processed in RAM, usually an order of magnitude faster than when they are run offbox. WebFilter typically rates around 95 percent of the web pages requested by a corporate or educational user on-proxy in less than eight milliseconds. For the other 5 percent, a rating can be instantly and transparently requested from WebPulse's master database (typically in less than 70ms) or from WebPulse's Dynamic Real Time Rating (typically in about 200ms, although there are some dependencies on the performance of the site in question). Processing rating requests on-proxy is the fastest possible architecture for high performance and scalability. That's why Blue Coat provides incremental database updates every five minutes for security-related categories and every six hours for non-security-related categories.

The onbox database also includes IP addresses for the most common web sites so that DNS reverse lookups don't add delay to the processing of URLs.

Other WebPulse clients such as ProxyClient, K9 or PacketShaper use a temporary local cache of ratings from WebPulse to increase performance.

### Dynamic Real-Time Rating (DRTR) and dynamic link analysis

Over 300 libraries are available in WebPulse to rate new content in real time. Real-time rating supports about twenty languages, including Pornovian, a generic module that detects pornography-related content. This and various threat-detection features, are key components of WebPulse. Together they present another unique differentiator.

It's important to note that the real-time rating modules also provide feedback to the requesting system (ProxySG, Web Security Module, ProxyClient or K9) in real time.

Real-time threat detection includes dynamic link analysis (DLA). Cybercriminals place a script on a trusted web page that forces the browser to download malicious content from a typically unrated and quickly changing malware host. The offending URL will be sent to WebPulse in real time.

Real-time rating disassembles a web page and analyzes its components. Here is an extract of the kinds of information that is used to assign categories:

- >Language (example: English)
- >Source code language (example: JavaScript)
- >Document type (example: HTML)
- >Character set (example: UTF-8)
- >External link categories
- >Content words
- >Scripts
- >Iframes

#### **Real-time malware detection modules**

Most of the real-time malware detection modules are looking for characteristics of the content (data or traffic) that may indicate danger. At the same time, they also assess the source for indications of danger – using more than nine years of WebFilter experience in mapping the shady parts of the Internet. If the combination of characteristics is sufficiently suspicious, they trigger. The modules ask, how does the bad content differ from legitimate content? How are they serving their content? Where are they serving it from? Access to suspicious content, which triggers a response from the real-time malware detection modules, can be blocked immediately.

#### **URL background checker**

The background checker system has two modules: a foreground (real-time) module and a background (off-line research) module that checks the background of a URL or site. The research module gathers data on malware delivery networks (MDN) so the real-time module can ask, does this URL belong to one of those networks? Access to URLs pointing to MDNs can be blocked immediately.

#### **Background analysis techniques**

Not all analysis can be done in real time. When there isn't enough information for a real-time decision, or when the content is not applicable to real-time rating, the boundary between real-time and background rating is being crossed. For the small volume of content that cannot be rated in real time – typically less than two percent – a Deep Background Rating Analysis (DBRA) service uses sophisticated, proprietary techniques and feeds the analysis back into the master WebPulse ratings database. As a final step, human raters continuously train the DRTR and the DBRA and perform focused investigation and rating of rare sites.

It's worth mention that DBRA processes also run on URLs that were rated in real time, to decide if a rating should be added to the database. This indicates that not all the URLs that have been rated in real time will be added to the database. One criterion for adding a URL to the database is its number of requests per unit time.

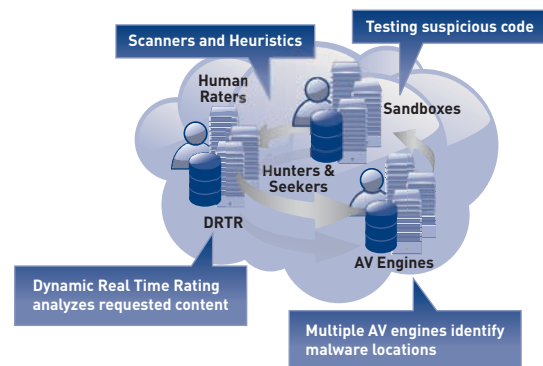
DBRA is looking for additional evidence to supplement what was collected in real time. Once identified, this information can be used to fine-tune and update real-time rating modules. An example is an HTTP referrer header: having knowledge about the referrer allows WebPulse to analyze the full path of a web-based attack. In many cases malware hosts present their malicious contents only when the requests contain a certain referrer, such as a search engine result.

### Malware detection

Given the rapidly evolving threat landscape, effective malware protection requires a broad set of detection mechanisms. To that end, WebPulse technology has a unique approach to protection against malware in Internet traffic, combining the following analysis and identification techniques:

#### Detection and analysis of malicious traffic

To identify malware distribution mechanisms, including intermediaries and malware hosts, WebPulse incorporates hundreds of malicious-traffic detection rules that instantly recognize and block traffic to malicious sites. These rules are constantly fine-tuned, expanded and updated to reflect real-time information identified by Blue Coat's malware experts. They eliminate the need for you to spend time trying to become an expert in Web defense. For example: in a recent quarter, more than 100 new traffic analysis rules were added to WebPulse; about 65 percent of these rules were designed to help identify malware and its sources, typically targeting traffic from a specific malware ring or botnet.



#### Malicious site and content identification and analysis

It's important to constantly evaluate risks associated with all sites that users access. Malware that has been embedded in reputable sites is identified, even if it has been obfuscated. Blue Coat conducts this analysis in multiple ways:

##### *Malicious site fingerprinting*

To match the speed with which malicious sites change their domains, WebPulse utilizes advanced fingerprinting modules that quickly recognize similar sites that appear on new servers.

##### *Web reputation*

WebPulse collects many kinds of reputation information about sites. It automatically scores the reputation of web sites and categorizes sites with a heightened security risk as Suspicious.

##### *Malicious PDF detection*

WebPulse includes a module that scans and identifies malicious PDF files in real time. It also flags PDFs that are merely suspicious for additional background research.

### *Malicious JavaScript detection*

WebPulse logs information on JavaScript from the millions of web pages that are requested every day. Blue Coat researchers use this intelligence to identify characteristics that indicate suspicious behavior and create appropriate new defenses for them.

### *Malware content analyzers*

WebPulse has proprietary analyzers that identify malicious sites in real time, using statistical analysis techniques to locate suspicious content on web pages.

### *Malware signature scanners*

WebPulse utilizes several background signature-based scanners to compare executable files and other potentially risky file types against a database of known malware to determine if they're malicious. These scanners make it possible to quickly identify both known and emerging threats that are being hosted in new locations.

### *Malware behavioral scanners*

WebPulse utilizes several background behavioral scanners to run executable files within a sandbox to determine whether the behavior is in fact malicious. One of these scanners uses proprietary Blue Coat algorithms to statistically compare the behavior of the file being analyzed to the behavior of other malicious and non-malicious executables to inform the decision. These scanners make it possible to quickly identify malicious files based on their behavior, regardless of whether they're completely new attacks or variants of existing attacks that aren't yet in signature-based databases.

### *Phishing detection*

WebPulse includes proprietary real-time algorithms that identify phishing sites posing as financial institutions. These algorithms, coupled with the real-time WebPulse processing of customer requests to uncategorized sites, are able to find new phishing threats almost immediately. Blue Coat's unique mechanism often detects sites before they appear on any third-party phishing lists.

### **Detection of illegal or questionable sites (scam sites)**

The background checker (and some of the other modules) can be used to target any large, complex network of web sites, and many scam networks fit this description. Several of the large malware delivery networks also contain sub-networks that deal in this sort of material; the background checker blocks this content in real time (generally with Suspicious as the initial rating).

### **Third-party intelligence**

Third-party intelligence is used to complement Blue Coat's primary research and analysis. In addition to all of the techniques described above, WebPulse gathers information from numerous third-party intelligence sources. These include commercial malware and phishing lists, community-contributed content, and general research and ongoing monitoring of the overall web security threat landscape. Information from third-party sources must meet a very high standard of quality and pass a set of rigorous checks before the source is accepted for inclusion in the WebPulse system.

### Active user community

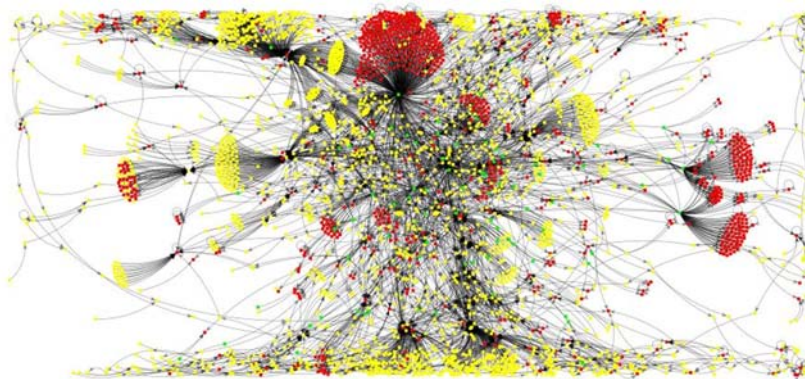
The worldwide WebPulse community comprises more than 75 million diverse users who are extremely active in ensuring the accuracy and effectiveness of the WebPulse service. They send billions of new web requests to WebPulse every week, giving the service a clear, current view of the huge numbers of new and changed web areas and – hiding inside those huge numbers – the locations of the most likely sources of web-borne threats and the hidden paths that lead to them. Blue Coat is committed to investigating and responding to community requests and feedback (submitted via [sitereview.bluecoat.com](http://sitereview.bluecoat.com)) within 24 hours. The WebPulse community provides Blue Coat with a significant sample of all traffic traversing the Internet on a second-by-second basis. WebPulse uses its malicious content detection techniques (described above) to analyze traffic, sites and content and deliver an extremely high rate of malware identification. The usage patterns of the WebPulse community and its real-time analysis provide invaluable insights to users and the highest possible level of web-threat protection for Blue Coat customers.

### Immediate availability of malicious content identification to WebPulse users

WebPulse ensures that you have what you need to protect yourself as soon as you need it. As soon as a rating change or malware identification passes the WebPulse quality checks, all WebPulse users have access to the information. WebPulse clients accessing WebPulse can query the cloud service in real time to receive the new rating.

### Malware delivery networks analysis

Cybercriminals run vast networks of sites and servers to collect victims, relay them to a designated location, infect or entice them, collect payments, serve new or upgraded payloads, or perform other operations. Like any mainstream web architecture, there is provision for redundancy, failover, backup and administration. But these malware delivery networks have an Achilles' heel: their size and complexity presents WebPulse with a large attack surface. Blue Coat has used its long experience in the Cloud, and its high volume of web traffic, to develop systems that identify and track MDNs. Every day, WebPulse automatically identifies thousands of new sites and servers as members of known MDNs, protecting our users from whatever new exploits and payloads the MDNs may be offering, no matter how well they may be hidden or encrypted.



Graphical mapping software makes it easy to see how the large malware delivery network in the center of the image above pulls unsuspecting users into the attack. Color code for the image above: red = threat site; yellow = link site, green = search result/email.

### **Web application and web application operation controls**

In addition to URLs and IP addresses, the WebFilter database contains information about web applications:

- >Application Name (example: Facebook)
- >Application Operations (example: Post Message)
- >Application Category (example: Social Networking)

This information can be used to build very granular policies to control web application usage using Blue Coat's Web Application Policy (WAP) Engine.

New applications and application operations can be implemented and made available to ProxySG or Web Security SaaS customers without the need for SGOS updates. Because this information is part of the BCWF database, all changes are available on ProxySG for both Content Policy Language (CPL) and Visual Policy Manager (VPM), and for the Web Security SaaS as soon as an automated BCWF database update is being installed.

Both Blue Coat Reporter and Cloud Reporting show new applications and application operations as soon as they're available.

### **Managing web application and web application operation changes**

A critical part of web application control is the early detection of application changes so adjustments can be made promptly. Blue Coat has implemented Q&A processes for all supported applications and application operations. Applications and operations are monitored; when a change is detected, Blue Coat takes action immediately, rolling out changes using standard BCWF database updates.

## Conclusion

Blue Coat constantly evolves its web security solutions to proactively prevent and combat fast-changing web threats. They offer powerful advantages to customers because they leverage:

**The Cloud:** WebPulse, as a cloud-service component of WebFilter, has been in continual development for the past nine years – longer than any other cloud security solution. It enables Blue Coat to constantly enhance and upgrade its capabilities with no impact, downloads, or patches for customers to deal with. This gives Blue Coat the greatest agility of any vendor in dealing with changing threats.

**The Community:** With input from the industry's largest user base – 75 million and growing – WebPulse has the greatest possible understanding of what users are encountering on the Internet right now. This provides valuable direction and focus for our security research efforts. We have never needed to use web crawlers to search for content; we can simply focus on what our users are browsing.

**Anti-malware detection technology:** Using a bank of cloud-based AV scanners allows us to add new scanners that have shown recent accuracy improvements or unique capabilities against specific threats, disable scanners that are drifting toward unacceptable levels of false-positive detections, and steadily monitor and modify the configuration of individual systems (and the bank as a whole) for optimum performance and accuracy in identifying malware on the Internet.

**Security industry relationships:** As new research organizations appear and others focus on areas of specialization, it's important to adjust our relationships with them to ensure fast information-sharing, and to evolve collaborative processes for addressing new threats.

**Ongoing expansion plans:** Blue Coat Security Labs continues to invest in people, equipment, and relationships to build and strengthen our internal expertise.

**Expertise in Security:** Blue Coat has deep roots in blending machine learning technology with human researchers in joint feedback loops. This is the only solution that meets the challenge of reliably managing the huge volume of Web traffic every day.



Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direct  
+1.408.220.2250 Fax • [www.bluecoat.com](http://www.bluecoat.com)

Copyright © 2011 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use. Blue Coat, ProxySG, PacketShaper, CacheFlow, IntelligenceCenter and BlueTouch are registered trademarks of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners.

v.WP-WEBPULSE-TECHNICAL-OVERVIEW-V1-0911