



**Lab Testing Detailed Report  
DR100412D**

**Detailed Competitive Testing of the Websense Web Security Gateway 7.5**



**For Essential Information Protection™**  
Web Security | Data Security | Email Security

*May 2010*

## Contents

Executive Summary .....	3
Key Findings .....	4
Figure 1: Averages of Percentage Blocked Values for Malware Threat Types.....	4
Figure 2: Averages of Dynamically Classified Content Blocked on Web 2.0 Sites ...	5
Methodology .....	6
Systems Under Test.....	6
Test Bed Diagram.....	6
How We Did It.....	6
Malware .....	7
Figure 3: Malware - Exploits .....	8
Figure 4: Malware – Redirection.....	8
Figure 5: Malware – Drive by Installers .....	9
Figure 6: Malware – Blended Threats.....	9
Dynamic Content URL Categorization .....	10
Figure 7: Web 2.0 – Sex.....	11
Figure 8: Web 2.0 – Gambling.....	11
Figure 9: Web 2.0 – Hacking .....	12
Figure 10: Web 2.0 – Proxy Avoidance .....	12
Data Loss Prevention.....	13
DLP Detection Techniques .....	13
Figure 11: Data Loss Prevention Test Cases .....	15
Manageability.....	17
The Bottom Line.....	20

# Executive Summary

Miercom conducted an independent third-party validation of the Websense Web Security Gateway version 7.5, as compared to McAfee's Web Gateway (WebWasher), version 6.8.6, Blue Coat's Proxy SG 810-20, version SGOS 5.4.1.12 Proxy Edition, and Cisco's IronPort S650, version 6.3.1-025. (Note: Currently, the IronPort S650 is no longer available. It has been replaced by model S660 which was not part of this review.) Testing was performed at the Websense lab facility in Los Gatos, CA.

Standard security tests were performed for the detection and blocking for multiple categories of real-world malware threats, and included attacks designed to exploit Rich Internet Applications (RIT) and the recently discovered and complex "Aurora" blended threat. The ability of the appliances to correctly categorize and block objectionable content contained within Web 2.0 sites, such as blogs and social networking, was also tested. To evaluate the ability to meet current compliance requirements for medical records and financial information, each appliance's ability to implement Data Loss Prevention (DLP) policy, as well as the policy's effectiveness, was tested. We also looked at each product's ease of management by performing a time and motion study for typical management tasks, and noted whether any additional elements were required to perform these tasks.

We were pleased with the overall performance of Websense Web Security Gateway, particularly its malware blocking and dynamic content categorization effectiveness, as well as the comprehensive and practical nature of its DLP policy implementation. While the competitive products did block objectionable content based on reputation and antivirus strength, the Websense appliance was able to accurately categorize the content, providing more granularity, and better blocking. The management interface also includes customizable reporting features as part of the standard license, a nice touch.

Detailed test results follow and demonstrate a clear advantage for the Websense Web Security Gateway in virtually every metric measured. The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measuring equipment. Contact [reviews@miercom.com](mailto:reviews@miercom.com) for additional details on the configurations applied to the system under test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study, and test specifically for the expected environment for product deployment before making a selection.

The Websense Web Security Gateway 7.5 performed as advertised, and demonstrated several advantages over the other competitive products evaluated in this review.

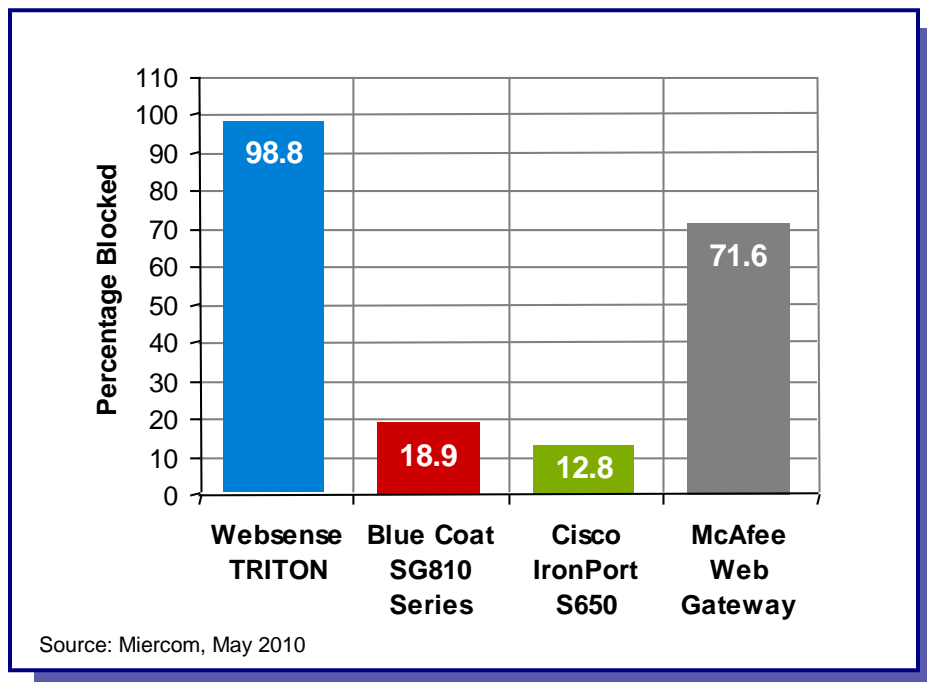
Rob Smithers  
CEO  
Miercom

## Key Findings

Websense Web Security Gateway 7.5 provides proxy-based content analysis of Web and SSL traffic in real time, ensuring safe use of Web 2.0 sites and tools. The appliance can instantly categorize new sites and dynamic content, while proactively discovering security risks and blocking unsafe malware. Its Advanced Content Engine detects, blocks or strips malicious code before it enters the network, and the Content Gateway module classifies new content as it applies decryption and scanning of SSL traffic. The Gateway's dashboard offers feedback on network security, threat detection, traffic loads and user activity.

The Web Security Gateway blocked 98.8% of the advanced modern malware threat types tested, including complex "Aurora" type blended threats, more than 27.2% better than the nearest competitor.

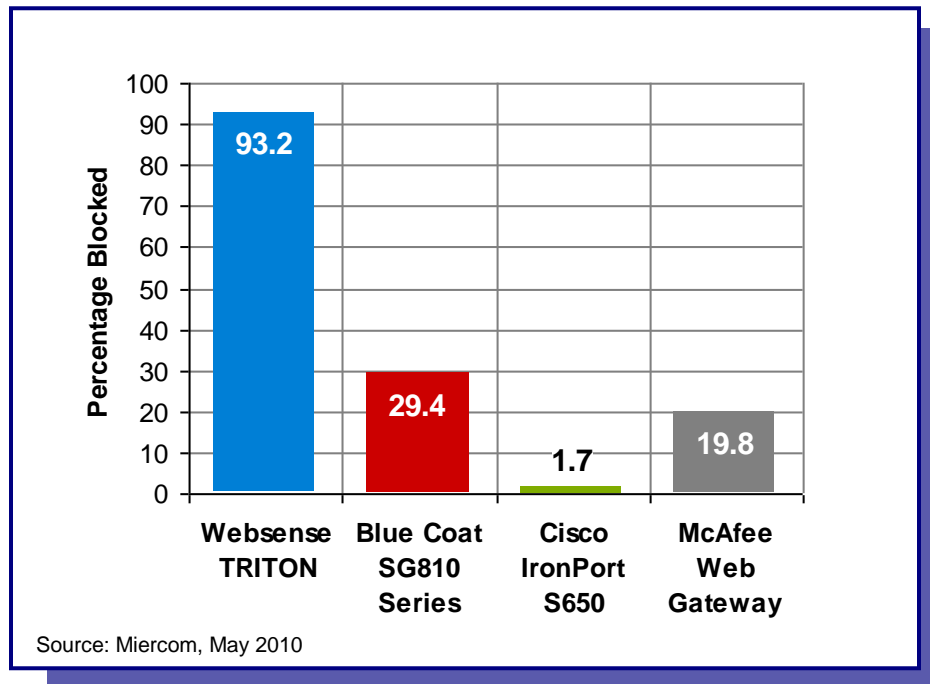
**Figure 1: Averages of Percentage Blocked Values for Malware Threat Types**



*This is the average of the percentage blocked values found in the four charts on pages 8 through 9 on malware types.*

The Websense Gateway provided dynamic content categorization not matched by the other appliances in this test, and was able to block over 93.2% of dynamic, objectionable content, including that contained on Web 2.0 sites, more than 3X the results of the nearest competitor.

**Figure 2: Averages of Dynamically Classified Content Blocked on Web 2.0 Sites**



*This is the average of the percentage blocked values found in the four charts on pages 11 through 12 on blocked URL content.*

Management of the appliance was clear and concise, requiring less time and fewer clicks to create/apply policies and to create reports than the competition. The ability to create customized reports is built in and does not require the purchase of additional products.

The Web Security Gateway provided the most comprehensive, practical, and effective Data Loss Prevention policy, which includes multiple fingerprinting of sensitive documents such as business plans, and compliance policies tailored for medical, financial, education, and business environments.

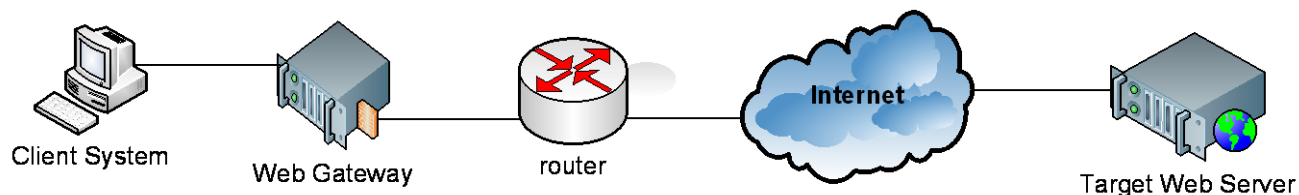
# Methodology

## Systems Under Test

Testing was performed on the following systems:

- Websense TRITON – Web Security Gateway  
Version: 7.5  
Build: 20100129\_1058
- Blue Coat SG810 Series  
Model: 810-20  
Version: SGOS 5.4.1.12 Proxy Edition
- Cisco IronPort S650  
Version: 6.3.1-025
- McAfee Web Gateway  
Version: 6.8.6  
Build: 6257 on wwapp

### Test Bed Diagram



### How We Did It

Test scripts were run on the client system, sending HTTP “GET” requests to the target Web server through the Web gateway. The client system then waited for a response code to be returned. The response code determined whether the URL was blocked or not. The client system was configured to wait up to twenty seconds for a response and retry the URL one time, in order to ameliorate any temporary network issues which might skew the results.

Management of the appliance was also done through the client system.

# Test Results

## Malware

Script, exploit and other advanced forms of web attacks were used to determine inbound threat detection and blocking accuracy of each appliance. A selection of real-world malicious URLs containing several categories of malware was used. We measured the ability of each system to detect and block web sites that contain these threats:

- Malicious Exploit sites – Sites that can take advantage of vulnerability in software, typically targeted at the web browser, plug in or other Rich Internet Application components (RIA) and executed via Java, ActiveX or other scripts to launch an attack.
- Malicious Redirection – Sites injected with code that redirects users without their permission for malicious purposes.
- Malicious Installers – Sites that contain code that installs code on end user systems without consent for the purpose of causing harm. These threats are also known as “drive by” installers and pose one of the more insidious threats as a user merely has to visit a site to become a victim.
- Blended Threats – Attacks that use multiple vectors, such as email and web, to execute an attack targeted at stealing sensitive or confidential data.

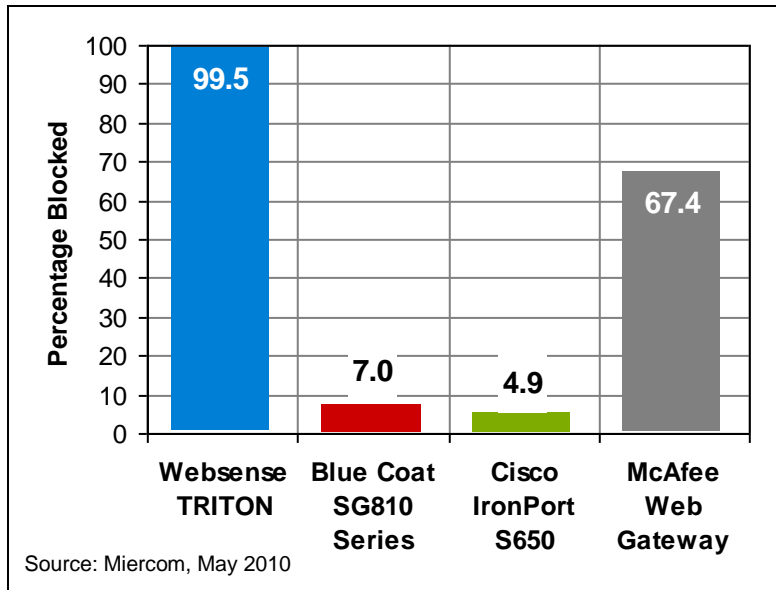
The last category of security risks, blended threats, was intended to test the effectiveness of the web gateway in defending against the sophisticated “Aurora” type attacks such as those experienced recently by Google and other U.S. companies.

The appliances we tested were configured with the default security policies provided by the manufacturer. If these were not provided, we configured the security filtering features to settings found in a typical customer configuration.

The quantity of URLs in each sample set was selected to be statistically relevant. A custom tool that uses a list of URLs as a source to initiate a connection and issue an HTTP “get” command was used to access the URLs. The tool lists the result of the “get” command and logs if the page can be successfully retrieved, or if a block page was issued by the proxy gateway, and under what category was the request blocked. The test was configured with one retry attempt and a 20-second timeout if the target server failed to respond.

**Note:** The Aurora sites included in the Blended Threats test (see [Figure 6](#) on page 9) were brought online after the Metasploit release of the Aurora exploit as part of its penetration toolkit. Updated signatures developed by Antivirus vendors in response to the threat also contributed to higher blocking results by all the products here.

**Figure 3: Malware - Exploits**



**Description:**

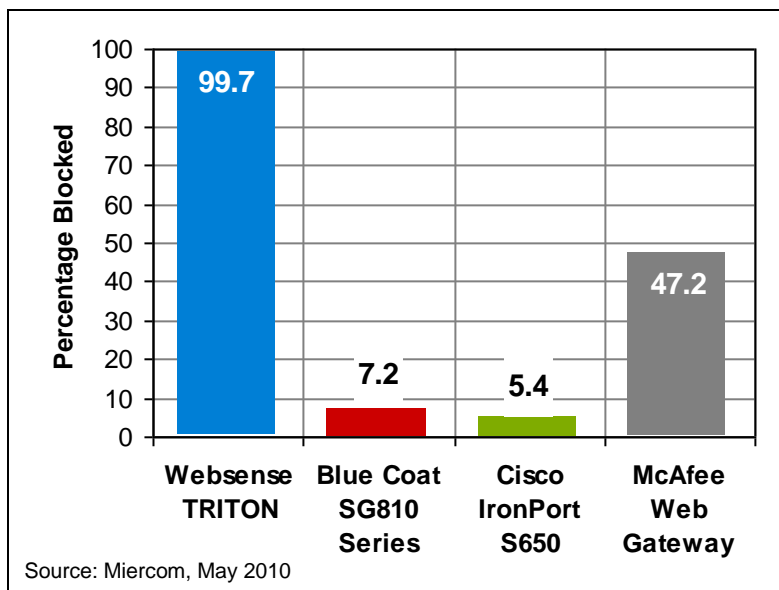
A sample set of 874 URLs containing browser exploits was tested. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

Note: The Cisco S650 that was reviewed has been replaced with model S660 that was not evaluated in this report.

**Results:**

The Websense Web Security Gateway successfully blocked 99.5% of these threats. The next system was McAfee Web Gateway, which blocked 67.4% of the URLs. Blue Coat Systems Proxy SG –Proxy AV SG810-20 and the Cisco IronPort S650 rounded out the bottom of the field, with 7% and 4.9% blocking effectiveness, respectively.

**Figure 4: Malware – Redirection**



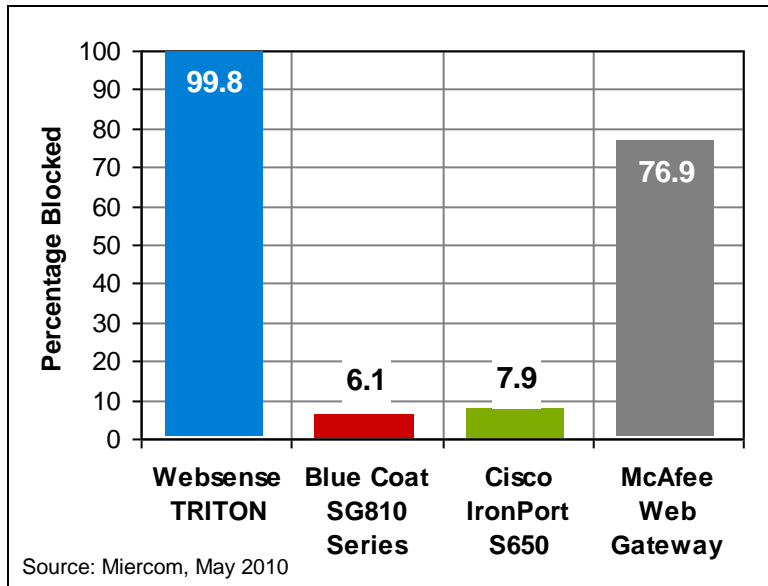
**Description:**

A sample set of 800 URLs containing malicious redirection attacks was tested. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were made.

**Results:**

The Websense Web Security Gateway successfully blocked 99.7% of these threats. Again, the closest competitor was McAfee with 47.2% blocking effectiveness. Blue Coat blocked 7.2% of the attack sites, while Cisco IronPort blocked 5.4%.

**Figure 5: Malware – Drive by Installers**



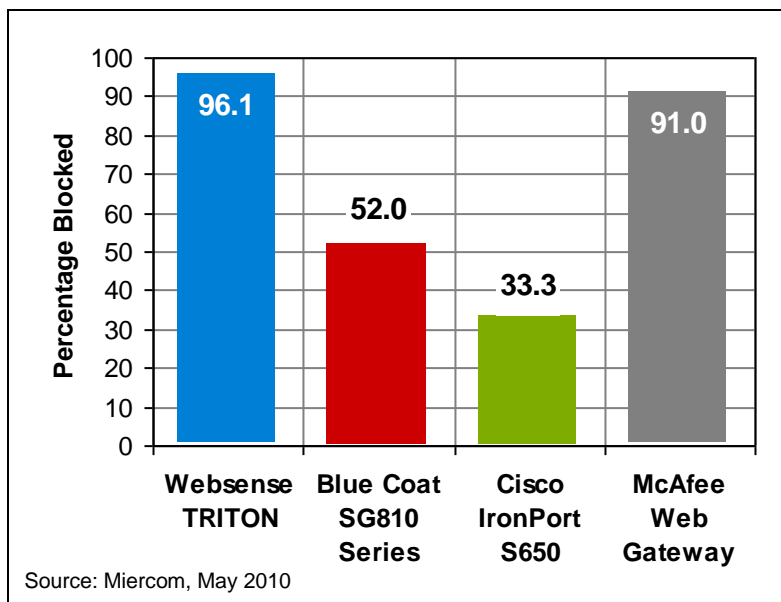
**Description:**

A sample set of 986 URLs representing drive-by installers was tested. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

**Results:**

The Websense Web Security Gateway successfully blocked 99.8% of these sites. McAfee’s Web Gateway blocked 76.9%, while Blue Coat blocked 6% and Cisco IronPort blocked 7.9%.

**Figure 6: Malware – Blended Threats**



**Description:**

A sample set of 80 URLs containing blended threats representative of the “Aurora” type hacking attack was tested. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were made.

**Results:**

Websense Web Security Gateway blocked 96% of these threats. McAfee was second and blocked 91%. Blue Coat ranked third with 52% of the sites blocked. Cisco IronPort successfully blocked 33%.

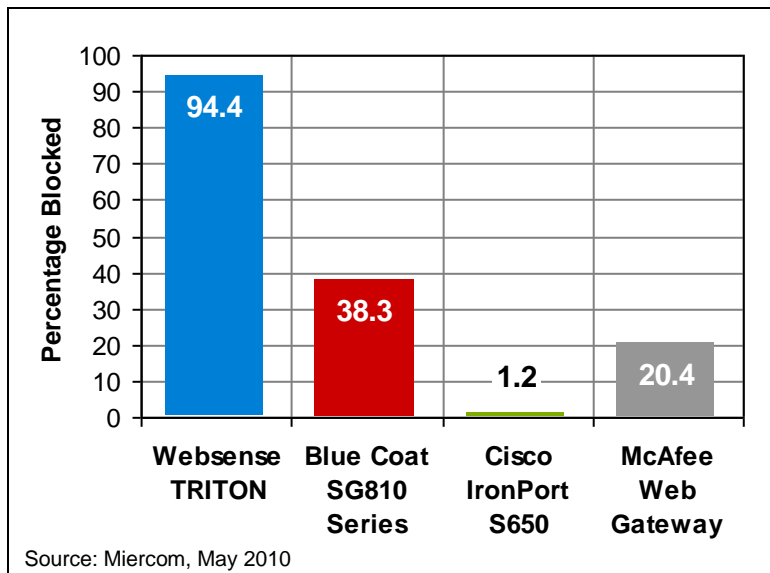
## Dynamic Content URL Categorization

We measured the ability of the systems to identify dynamic content located on social networking and other Web 2.0 sites, such as social networking and blogs, and whether they could create and enforce usage policies. A number of URLs for each test category that was deemed to be statistically relevant was selected as the sample set. Tested categories included sex, gambling, hacking and proxy avoidance.

For testing, we configured the systems under test to block the required category. Connections to URLs on Web 2.0 sites were initiated from a client using the Websense URL evaluation client tool.

The test script was configured with one retry attempt and a 20-second timeout if the target server failed to respond. Results were reported for the number of samples tested, number of sites correctly categorized and blocked, number of sites incorrectly categorized and blocked (false positives) and number of sites incorrectly categorized and not blocked.

**Figure 7: Web 2.0 – Sex**



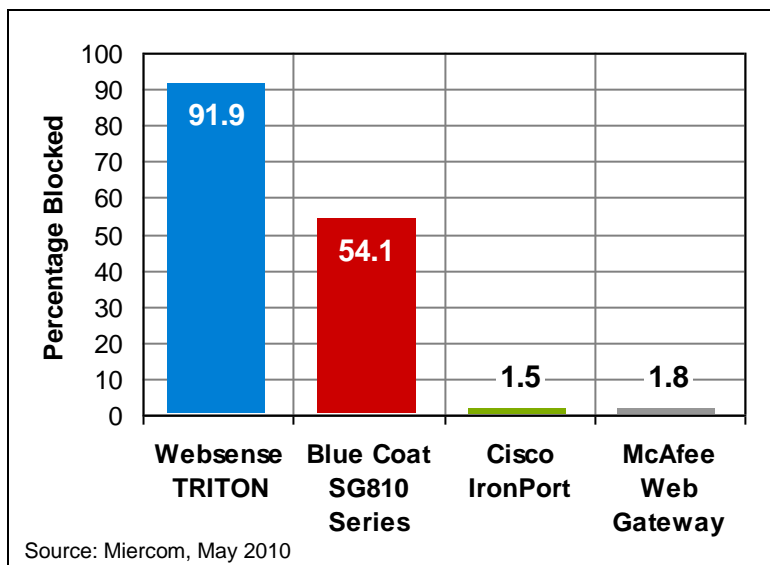
**Description:**

A sample set of 1001 URLs was tested. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

**Results:**

Websense Web Security Gateway correctly blocked 94.4% of the sites. Blue Coat was the second most effective, blocking 38.3%. McAfee only blocked 20.4%, while Cisco delivered only single-digit effectiveness, with 1.2% of the URLs blocked. Blocking for the competitive products appeared largely based on reputation.

**Figure 8: Web 2.0 – Gambling**



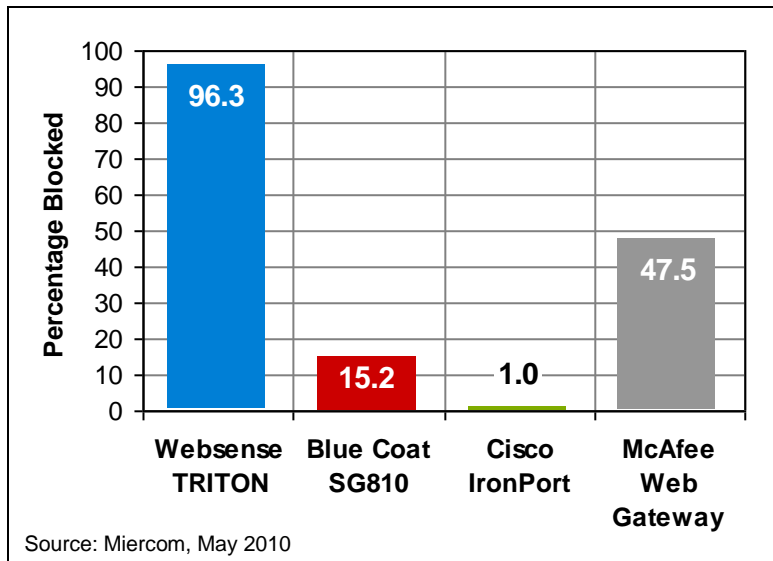
**Description:**

A sample set of 455 URLs was selected to test. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were made.

**Results:**

Websense Web Security Gateway scored 91.9% effectiveness in blocking access to these sites. Blue Coat was somewhat effective, with 54.1% success. Both Cisco and McAfee delivered single-digit blocking, with 1.5% and 1.8%, respectively. Blocking for competitive products appeared largely based on reputation.

**Figure 9: Web 2.0 – Hacking**



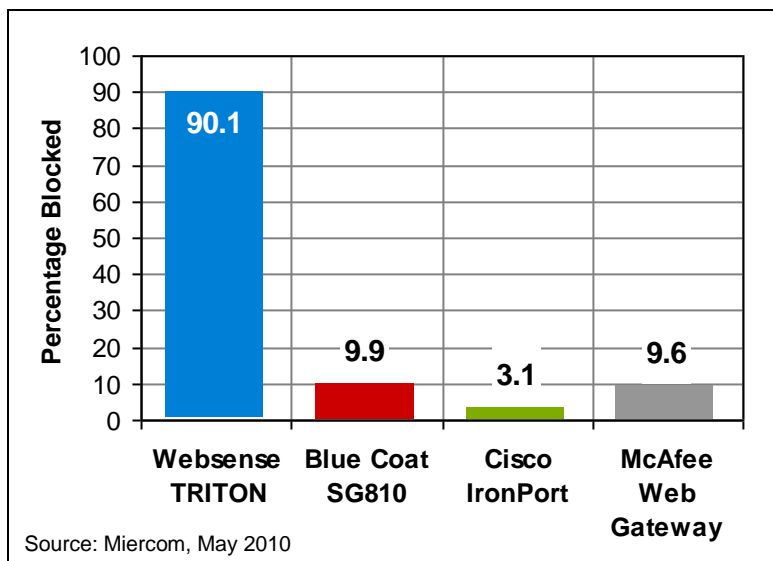
**Description:**

A sample set of 486 URLs was selected including hacking threats. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

**Results:**

Websense correctly blocked 96.3% of these sites. The McAfee Web Gateway A/V technology contributed to a 47.5% effectiveness in blocking, Blue Coat achieved 15.2%, and Cisco IronPort blocked 1%.

**Figure 10: Web 2.0 – Proxy Avoidance**



**Description:**

A sample set of 669 URLs was tested which exhibited the behavior of proxy avoidance. The number of URLs blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

**Results:**

The Websense Web Security Gateway correctly categorized 90.1% of these types of threats. Blue Coat and McAfee performed on par with each other, with 9.9% and 9.6% of the URLs blocked. Cisco IronPort blocked 3.1% of threats.

# Data Loss Prevention

The appliances were reviewed for their creation and enforcement of outbound DLP policies and their reporting of false positive and false negative information. We determined the accuracy of the systems to correctly identify sensitive information such as social security and credit card numbers being transferred outbound via the web channel. Sensitive information samples included names and social security numbers, business plans, customer lists, and medical information such as patient names and diseases.

Three samples of sensitive information were used with formatting variations. The same information was presented in a table format, a letter format, and a mixed format containing both table and letter formats. Multiple sample types were needed to test for both false negatives - samples not identifying sensitive information - and false positives - samples identifying non-sensitive information as sensitive.

Several scenarios of web transmission methods were tested:

- Manually composing a web mail with sensitive information
- Sending a web mail with an attachment containing sensitive information
- Posting sensitive information to a public blog
- Posting information to a social networking page
- Backing up sensitive information to a web-based backup service

Specific data was included in the test cases:

- Customer names and emails
- Customer names and phone numbers
- Customer name and address
- Single patient name and sensitive medical information in the body of webmail
- Employee records with SSN
- Employee records without SSN
- Email body with name and one non-delimited SSN
- Email body with multiple names and SSNs
- Email with attached customer list with SSNs
- Email body – Business Plan
- Email Attachment – Business Plan
- Executive Summary of Business Plan

## DLP Detection Techniques

Solutions that can only identify data by file properties (e.g. name, size, type) are prone to a high rate of false positives. To block the lists of personally identifiable information used in testing, for example, the Cisco IronPort appliance would have to be configured to block all the most common office file types (Microsoft Office files, text files, PDFs, etc). Such coarse blocking techniques would likely interfere with authorized and necessary business processes and are unlikely to be used in production.

Solutions that can only identify data based on full file fingerprints are prone to a high rate of false negatives. A full file fingerprint generated will only match the exact file but will not detect the transmission of data derived from that original document. Information cut-and-pasted into a web-based email, for example, would not be detected. Deployments relying on this kind of

full-file fingerprinting will be able to stop some leaks, such as an attempt to upload that original fingerprinted document to an external web-based file sharing service, but would not detect other versions of that same document. This approach does offer some limited DLP protection but would fail to detect many incidents.

The use of described data and partial fingerprints offers both more granularity and greater accuracy. A solution that describes protected data using regular expressions and statistical pattern matching can detect discrete pieces of confidential data (e.g. Social Security numbers, credit card numbers) without the need to fingerprint specific files. When fingerprinting, the ability to identify partial documents (e.g. the executive summary from a business plan) or data pulled from a database (e.g. a specific customer record) can be critical to preventing data loss without imposing wholesale restrictions on the transmission of the most commonly used file types.

The following table lists the DLP detection mechanisms used by each gateway.

	<b>Websense TRITON</b>	<b>Cisco IronPort</b>	<b>McAfee Web Gateway</b>	<b>Blue Coat SG810</b>
<b>Available Detection Methods</b>	Regular Expressions	Block by file size	Block by file type	No coverage without 3rd Party DLP integration
	Key Phrases	Block by file type	Block by file hash**	
	Dictionaries	Block by file name*	Block by file tag	
	File Properties			
	Statistical Pattern Matching***			
	File Fingerprinting			
	Database Fingerprinting			

**Notes:**

\* Can include wildcards

\*\* Full file fingerprints - no support for detecting modified documents or data that has been copied to a new file.

\*\*\* Referred to as "PreciseID Natural Language Processing"

The tests cases described in the following table (see *Figure 11* on “Data Loss Prevention Test Cases” on page 15) represent common data leakage concerns. Confidential customer information, employee information, and intellectual property can be sent over the Web, either by including that information in the body of a post (for example, a Web-based email or a blog post) or by directly uploading the content as an attachment. When enforcing policies, administrators must be careful not to block legitimate and business critical communications.

**Figure 11: Data Loss Prevention Test Cases**

Test Case Description	Websense TRITON	Cisco IronPort	McAfee Web Gateway	Blue Coat SG810
Web Upload: Customer names and emails in file	● <sup>1</sup>	▲ <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web Upload: Customer names and phone numbers in file	● <sup>1</sup>	▲ <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web Upload: Customer name and address in file	● <sup>1</sup>	▲ <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Single patient name and sensitive disease in body of webmail	● <sup>1</sup>	● <sup>3</sup>	● <sup>5</sup>	● <sup>4</sup>
Web Upload: Employee records with SSN in file	● <sup>1</sup>	▲ <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web Upload: Employee records without SSN in file	● <sup>1</sup>	▲ <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web-based email body with name and one non-delimited SSN	● <sup>1</sup>	● <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web-based email body with multiple names and SSNs	● <sup>1</sup>	● <sup>3</sup>	● <sup>5</sup>	● <sup>4</sup>
Web-based email including attached Customer List with SSNs	● <sup>1</sup>	● <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web-based email body including business plan	● <sup>2</sup>	● <sup>3</sup>	● <sup>5</sup>	● <sup>4</sup>
Web-based email with business plan as attachment	● <sup>2</sup>	▲ <sup>3</sup>	▲ <sup>5</sup>	● <sup>4</sup>
Web-based email including executive summary of business plan in body	● <sup>6</sup>	● <sup>3</sup>	● <sup>5</sup>	● <sup>4</sup>

**Scoring Key:**

● = Full coverage

▲ = Some utility or capabilities not meaningful in real world deployment; or flawed.

● = No coverage

**Footnotes:**

<sup>1</sup> Blocked all samples.

<sup>2</sup> Blocked using PrecisID fingerprint policy.

<sup>3</sup> DLP policy is limited to blocking by file size, file type and file name.

<sup>4</sup> No DLP coverage without 3rd party DLP integration.

<sup>5</sup> Whole file fingerprint;\* if file changes, policy is circumvented.

<sup>6</sup> Block upload to SharePoint. Blocked cut and paste into email.

Websense TRITON includes full-featured enterprise DLP content-aware capabilities with Web Security Gateway Anywhere (WSGA), providing the full range of policy tools including pattern matching and partial fingerprint matching. See the Available Detection Methods table on page 14.

Because Cisco IronPort can natively block only by file size, file type, and file name, administrators who want to block the kinds of information in the tests must configure the system to block all files that match specific criteria. In real-world deployments, blocking all uploads of Microsoft Excel or PDF files will result in the blocking of a large number of innocent and potentially business-critical transactions. See the Available Detection Methods table.

McAfee Web Gateway can fingerprint specific files and look for those exact files being uploaded over the Web, but will only block if the exact file is sent. Even the minor alteration will change the fingerprint/hash of the file. McAfee also supports blocking by file type and file tag. See the Available Detection Methods table on page 14.

No claims about native Web DLP capabilities without integration with a full 3rd party enterprise DLP product can be made on the Blue Coat SG810 product.

## Results:

Websense Web Security Gateway was the only appliance with a DLP scheme which included multiple fingerprints of sensitive data (via the PreciseID Fingerprint Policy) to protect against cut and paste of sensitive information, such as confidential business plans.

**Note:** In the Executive Summary of Business Plan test, we tried to upload samples of a paragraph or a page of sensitive business information that was removed from a business plan directly to Microsoft SharePoint. We also copied the executive summary information from the business plan document and pasted it into an email. The Websense Web Security Gateway passed this test by blocking both scenarios.

The NLP Policy was enabled to protect customer lists, HIPAA information and SSNs. It successfully blocked release of sensitive information for those test cases.

McAfee's Web Gateway was the only other product under test which featured a DLP scheme that also utilizes document fingerprinting. In this test, we observed that the McAfee appliance appeared to fingerprint only the entire file as an MD5 hash, meaning that the prevention policy can be circumvented if changes are made to the file after fingerprinting, such as copy/paste into other applications. The McAfee appliance did not block this outbound transfer of information once we had altered the file. We also saw that McAfee could block by file type, although in practical use this would most likely not be a granular enough DLP strategy.

**Note:** A whole file fingerprint uniquely identifies a data file and is used for discovering any tampering of electronically transmitted information. If a file changes by one character, its new fingerprint will not match the fingerprint of the original file. A file's digital fingerprint is used for preventing sensitive or proprietary information from leaving an organization by way of outbound communications.

Blue Coat Systems Proxy SG – Proxy AV SG810-20 requires 3rd party DLP integration to provide protection. We did not test using any 3rd party product.

The Cisco IronPort S650 DLP policy is limited to blocking by file size, file type, and file name. File name restrictions can also include wildcards. This method of DLP is not granular enough to be effective, and might cause undue problems by blocking non-sensitive files.

## Manageability

Measurements were recorded for the amount of time and number of steps required to perform common management tasks with the goal of providing comparative ratings on the amount of management time required by each system. The amount of time is how long it took to complete a specific task. The number of steps is the total number of clicks, plus the number of different screens or pages accessed, plus the number of sub-menus or individual elements within a screen that are used to complete the task. Tasks to be measured included the following:

- Access dashboard graphs on blocked inbound threats and outbound risks and drill down to a level that includes individual user or incident information
- Create and apply a policy to block top objectionable sites, adult/porn, gambling, illegal activities, hacking, proxy avoidance and all inbound malware
- Create and apply a policy to block outbound transmission of sensitive documents or information
- Create an ad hoc report that lists top security risks by user
- Create an ad hoc report on top data loss incidents by severity

The amount of time and number of clicks were recorded for a selection of tasks listed in the following tables.

Manageability Feature Summary Table				
	Websense TRITON	Cisco IronPort	McAfee Web Gateway	Blue Coat SG810
Actionable Dashboard	●	▲	●	●
Unified Policy Management	●	●	●	●
Outbound DLP Policy Management	●	▲	▲	●
Custom Security Report Generation	●	●	●	●
DLP Incident Report Generation	●	●	●	●

Manageability Time Requirements in Minutes				
	Websense TRITON	Cisco IronPort	McAfee Web Gateway	Blue Coat SG810
Actionable Information Retrieval	1/2	1/2	NA	NA
Policy Creation	5	10	20	30
Outbound DLP Policy Creation	5	5	15	NA
Custom Security Report Generation	2	NA	NA	NA
DLP Incident Report Generation	2	NA	NA	NA

### Scoring Key:

● = Full coverage

▲ = Some utility or capabilities not meaningful in real world deployment; or flawed.

● = No coverage

**Management Task:** Access dashboard graphs on blocked inbound threats and outbound risks and drill down to a level that includes individual user or incident information.

Product	Number of Screens	Number of Sub Screens	Number of Clicks	Average Time to Complete	Comments
Websense	3	0	5	30 seconds	
Cisco	2	0	2	30 seconds	
Blue Coat	N/A	N/A	N/A		Requires external reporting engine
McAfee	N/A	N/A	N/A		Requires external reporting engine to provide user level reports or details

**Management Task:** Create and apply a policy to block objectionable sites, adult/porn, gambling, illegal activities, hacking, proxy avoidance and all inbound malware.

Product	Number of Screens	Number of Sub Screens	Number of Clicks	Average Time to Complete	Comments
Websense	3	0	10	5 minutes	Proxy-based user interface
Cisco	5	0	20	10 minutes	
Blue Coat	15	0	52	30 minutes	Rules-based user interface
McAfee	5	6	23	20 minutes	

**Management Task:** Create and apply a policy to block outbound transmission of sensitive documents or information.

Product	Number of Screens	Number of Sub Screens	Number of Clicks	Average Time to Complete	Comments
Websense	5	0	10	5 minutes	
Cisco	4	0	10	5 minutes	
Blue Coat	N/A	N/A	N/A	N/A	Requires 3rd party DLP product
McAfee	2	3	27	15 minutes	

**Management Task:** Create an ad hoc report listing top security risks by user.

Product	No. of Screens	No. of Sub Screens	No. of Clicks	Average Time to Complete	Notes
Websense	3	0	5	2 minutes	
Cisco	N/A	N/A	N/A	N/A	Needs a separate reporting product
Blue Coat	N/A	N/A	N/A	N/A	Needs a separate reporting product
McAfee	N/A	N/A	N/A	N/A	Needs a separate reporting product

**Management Task:** Create an ad hoc report on top data loss incidents by severity.

Product	No. of Screens	No. of Sub Screens	No. of Clicks	Average Time to Complete	Notes
Websense	4	2	5	2 minutes	
Cisco	N/A	N/A	N/A	N/A	Needs a separate reporting product
Blue Coat	N/A	N/A	N/A	N/A	Requires 3rd party DLP product
McAfee	N/A	N/A	N/A	N/A	Needs a separate reporting product

## Results:

The Websense Web Security Gateway policy-based user interface required less time, fewer screens and fewer clicks to drill down from dashboard views, to create policies and generate customizable reports. To produce customized reports, optional add-on reporting products are required for the Blue Coat, Cisco, and McAfee appliances.

The task of creating and applying a policy to block objectionable sites required 52 clicks and half an hour to perform on the Blue Coat appliance, compared to just 10 clicks and 5 minutes for the Websense Web Security Gateway. The McAfee user interface was feature rich and granular, though not always intuitive. Cisco's global policy has a predefined list of URLs which are selectable by checkbox and can be scheduled. The Blue Coat interface appeared to be a graphic implementation of a previous command line management interface. Its appearance lacked a user friendly GUI in comparison to other vendors.

Websense was able to provide reports on individual threat by individual user by drilling down screens. Cisco IronPort has standard reports for tracking policy and security violations, and provides historical information on trends. It lacks native customized reports but third party applications can be used. The McAfee Web Gateway and Blue Coat SG810 products need separate reporting products to state threat information.

## The Bottom Line

Websense Web Security Gateway achieves the highest scores in security tests for:

- **Detecting and blocking of multiple categories of malware threats**  
The Gateway discovers and blocks network threats and malware attacks with its Advanced Content Engine. It prevents over 98% of advanced malware attacks, including the “Aurora” type blended threats, from entering a network.
- **Categorizing and blocking unacceptable content contained within Web 2.0 sites**  
The Content Gateway module categorizes new content and blocks over 93% of dynamic, objectionable content.
- **Implementing Data Loss Prevention (DLP) policy to attain compliance requirements for medical and financial information**  
The Websense Web Security Gateway presents the most effective DLP policy that includes multiple fingerprinting of sensitive documents, such as business plans, and compliance policies created for medical, education, financial and business settings.

Against competitive products, the Web Security Gateway ranks high in manageability measurements, as in the amount of time, the number of drill-down screens, and the number of steps to complete a standard task. All in all, we find that the Websense Web Security Gateway is a superior web security appliance, able to protect your network from malicious attacks and guard business-critical information from leaving your company.

## Other Notes and Comments

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report. Consult with professional services such as Miercom Consulting for specific customer needs analysis.