Lab Testing Detailed Report
DR130214

Competitive Testing of the
Websense TRITON Web Security Gateway Anywhere v7.7.3

February 2013

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Miercom conducted an independent third-party validation of the Websense TRITON Web Security Gateway Anywhere (WSGA) version 7.7.3, with comparisons to McAfee Web Gateway 5500, Blue Coat ProxySG 900, version SGOS 6.4.1.2 Proxy Edition, Cisco IronPort S370 AsyncOS 7.6.1, Palo Alto Networks PA-2020, version 5.0.1 and FireEye Web MPS 1300, version 6.2.0.

Standard security tests were performed to verify the detection, blocking and operational capabilities on multiple areas of real-time malware threats, modern malware, sandboxing and forensic reporting. The ability of the appliances to correctly identify threats from a large sample of web requests of an unknown nature emulated what the solutions need to provide when users click on web links. This point of click protection testing also focused on specific stages of advanced threats, or the cyber kill chain, such as lures, exploits and dropper files.

We also evaluated the ability to stop sensitive information leakage or theft, such as financial, social security numbers and other sensitive private information. Implementation of the Data Theft Protection policy within Websense TRITON WSGA was thoroughly exercised to ensure the effectiveness of these policies when put in place. Ease of management was tested by performing a time and motion study for typical management tasks. We noted whether any additional elements were required to perform these tasks.

We were pleased with the overall performance of the Websense TRITON WSGA solution, particularly its malware blocking and real-time defense effectiveness, as well as the comprehensive and practical nature of its DLP policy implementation as a defense against data theft and for data loss prevention. Detailed test results follow and demonstrate a clear advantage for the Websense TRITON WSGA solution in virtually every area 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 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 TRITON WSGA solution performed as advertised, and demonstrated several advantages over the other competitive products evaluated in this review.

Rob Smithers
CEO
Miercom

2.0 Key Findings

Websense TRITON Web Security Gateway Anywhere (WSGA), part of the TRITON unified security platform, provides proxy-based content analysis of Web and SSL traffic in real time, ensuring safe use of the internet. The Websense TRITON WSGA solution can analyze new sites and dynamic content in real-time, while proactively discovering security risks and blocking unsafe malware. Its Advanced Content Engine (ACE) detects, blocks or strips malicious code before it enters the network. The WSGA dashboards offer feedback on network security, threat detection, traffic loads and user activity for both in and outbound traffic.

The TRITON Web Security Gateway Anywhere demonstrated superior edge over the other vendors in the testing areas of Web Security Effectiveness, Modern Malware Threat Stages, Data Theft Protection, Malware Sandboxing and Forensic Reporting, plus Manageability and Effectiveness. Each vendor was presented equal opportunity for the various testing that is demonstrated below.

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 Anywhere provided the most comprehensive, practical, and effective data theft and loss prevention policy. Their forensic reporting capabilities were able to report on detected malicious embedded links and block outbound sensitive data such as custom encrypted files, password data files, or slow data leaks.

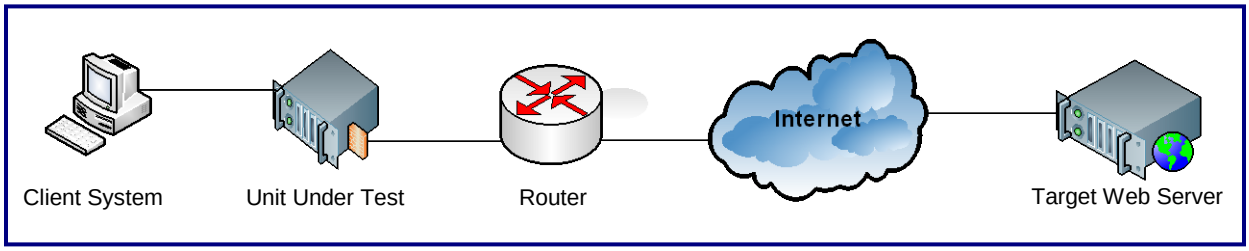
3.0 Methodology

3.1 Systems Under Test

Testing was performed on the following systems:

- Websense TRITON
  Web Security Gateway Anywhere
  Version: 7.7.3
  ThreatScope Malware Analysis Sandbox
- Blue Coat ProxySG and ProxyAV
  ProxySG 900 Series and ProxyAV 1200
  Version: SGOS v6.4.1.2
- Cisco IronPort S-370
  Web Security Appliance
  Version: AsyncOS 7.6.1
- McAfee Web Gateway
  MWG 5500
  Version: 7.2.0.5
- Palo Alto Networks
  Model: PA-2020
  Version: 5.0.1
- FireEye
  Web MPS 1300
  Version: 6.2.0

3.2 Test Bed Diagram



3.3 How We Did It

Test scripts were run on the client system, sending HTTP “GET” requests to the target Web server through the unit under test. The client system then waited for the response from the unit under test and analyzed the http headers and page source code to determine if the requested web request was blocked or not. The client system was configured to wait up to twenty seconds for a response and retry the web request 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.

3.4 Test Cases

Three types of security effectiveness validation tests, one feature verification test, and finally an easy-of-use and manageability test were performed. The following summarizes the five areas of focus for this testing and validation report.

Open Web Requests Testing using a Large Sample of Unknown Nature

A web security effectiveness validation test was performed to validate the ability of each unit under test to detect and block real-world threats, including complex malicious exploits. The test focused exclusively on validating the ability of the units under test to correctly analyze and block malicious content contained within a sample of live web targets of an unknown nature.

This approach would give each individual security solution a fair chance to analyze and proactively block threats from an unbiased sample set of live internet targets. It was the equivalent of placing each security solution on a live network and having each appliance perform security protection to determine their total security coverage against real-world web requests to live web servers on the internet.

A fundamental aspect of the test was to validate proactive security and see how much protection each vendor provided real-time as the web requests happened.

All security appliances tested were carefully configured to block every security related category available within their respective administrative consoles and to use available defenses such as anti-malware engines.

Advanced Threat Stage Testing

For this test, a selection of verified attacks was used in a replay system which allowed for the extraction of the threats and all of their associated code as found on the internet and were then replayed and fed to each security solution in exactly the same form. Advanced forms of web attacks such as malicious lures, exploits and dropper files were used to determine the threat detection and blocking accuracy of each appliance.

Malware Analysis and Forensic Sandboxing System Comparison

Malware analysis sandboxing is a threat analysis mechanism that allows for the safe execution and analysis of potential malware and its associated system modification behavior.

For this test, two malware analysis and forensics sandboxing systems were tested. The first malware analysis and forensics sandboxing system was the Websense ThreatScope system with the advanced threat dashboard within WSGA. The second system was the FireEye Web MPS. Both systems tested provide a sandbox environment of testing potential malware including zero-day threats contained within common files. Both systems were tested and scored on their ability to provide rich forensic detail including:

- The infection process
- Post-infection activities including network communications
- System-level events and processes
- System changes and file modifications

Data Theft Prevention (DTP) and DLP Feature Analysis

While not a comparative test, some of the Websense TRITON WSGA's DTP defenses were analyzed in detail along with new DLP detection techniques, including OCR of text within images and slow data leak detection. These features were not tested on the competing solutions, as either these defenses are not offered or are offered in a very basic form. To evaluate the Websense TRITON WSGA's ability to meet current challenges of data theft and loss prevention, the appliance's feature set was catalogued and it was decided to focus on six key aspects of modern data theft and loss prevention. These six key features were singled out due to the important role they play in current data loss prevention countermeasures.

Custom Encrypted File Detection: Custom encryption is being used to bypass the methods offered by many security solutions. Sensitive data encrypted using custom encryption can render the effectiveness of any data recognition technology useless. However, detecting files using custom encryption provides an alert to security administrators.

Password File Theft Detection: Password file theft prevention was selected, as often these files are used in the first steps to gain unauthorized system access. Stealing of password files, as with any other sensitive data, can also be encrypted using custom encryption.

OCR of Text within an Image: OCR or Object Character Recognition was selected as this is a simple, yet sophisticated method to bypass data loss prevention methods. By converting sensitive data to an image, for example, it can become an easy and quick way to leak data passed security systems.

Slow Data Leak Detection (cumulative): The fourth method outlined in the report is the Slow Data Leak Detection or cumulative DLP, which attempts to stop data from leaking out in a cumulative fashion. The purpose is to bypass data leakage countermeasures by breaking up the data into smaller subsets and 'leaking' them out one-by-one over a period of time.

Geo-location Destination Awareness: This feature plays a critical role in detecting data loss by analyzing the location of the destination of the data being transferred or via policy by blocking data export to specific countries and other policy variables.

Data Capture for Security Incidents: For security incidents, the ability to capture the data exfiltrating on outbound web requests by providing the file to security administrators within the context of forensic reporting details. Knowing what data is being targeted is key to improving defenses and policy controls.

Management Interface Usability

The final focus of the test validated 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.

4.0. Web Security Effectiveness

A web security effectiveness validation test was performed to validate the ability of each unit under test to detect and block real-world threats, including complex malicious exploits. The test focused exclusively on validating the ability of the units under test to correctly analyze and block malicious content contained within a sample of live web targets of an unknown nature. Over 2.25 million web requests were provided to the units under test making this the largest audited web security effectiveness test completed.

This approach would give each individual security solution a fair chance to analyze and proactively block threats from an unbiased sample set of live internet targets. It was the equivalent of placing each security solution on a live network and having each appliance perform security protection to determine their total security coverage against real-world web requests to live web servers on the internet.

A fundamental aspect of the test was to validate proactive security and see how much protection each vendor provided real-time as the web requests happened.

The test script was configured with one retry attempt and a 90-second timeout if the target server failed to respond. Results were reported for the number of samples tested blocked and categorized.

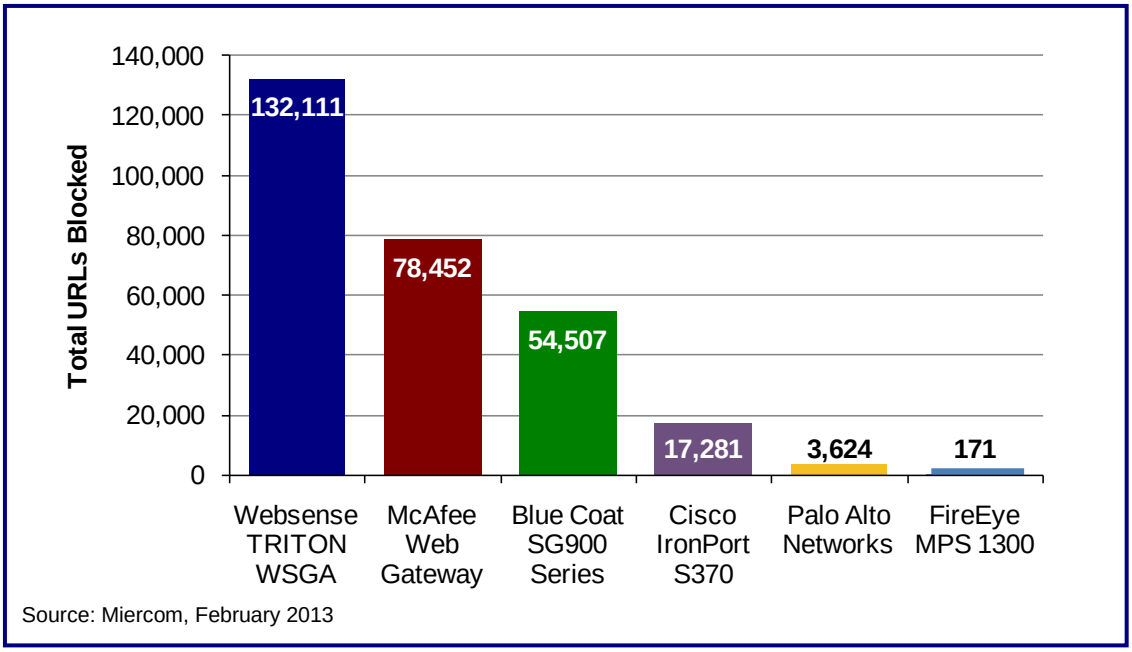
All tested appliances were configured to block every security category available in their respective administrative consoles and to utilize defenses such as anti-malware engines.

Figure 1: Security Effectiveness Totals

Effectiveness Totals for the 2.26 million URLs

System	Total Number Blocked	Total Percentage Blocked
Websense	132,111	5.84%
McAfee	78,452	3.47%
Blue Coat	54,507	2.41%
Cisco	17,281	0.76%
Palo Alto Networks	3,624	0.16%
FireEye	171	0.01%

Figure 2: Security Effectiveness



Source: Miercom, February 2013

Description:

Over 2.25 million web requests were utilized of an unknown nature. The solutions were tested to identify web threats just as they would on a customer network. Solutions that provide real-time defenses when the user clicks on the link, plus broader coverage across the cyber kill chain were likely to score higher. Solutions that require background analysis, sandboxing or threat confirmation lab processes were likely to score lower in this test. This is the difference between predictive or lean-forward defenses and passive or forensic defenses; they each have their own value and purpose in a defense strategy.

Real-time Blocking Effectiveness Results:

Websense TRITON WSGA identified and blocked 132,111 of these web requests as threats. The McAfee Web Gateway solution blocked 78,452 requests. Blue Coat blocked 54,507

requests as threats. Cisco IronPort blocked 17,281 of the web requests as threats. Palo Alto Networks blocked 3,624, and FireEye blocked 171 web requests as threats.

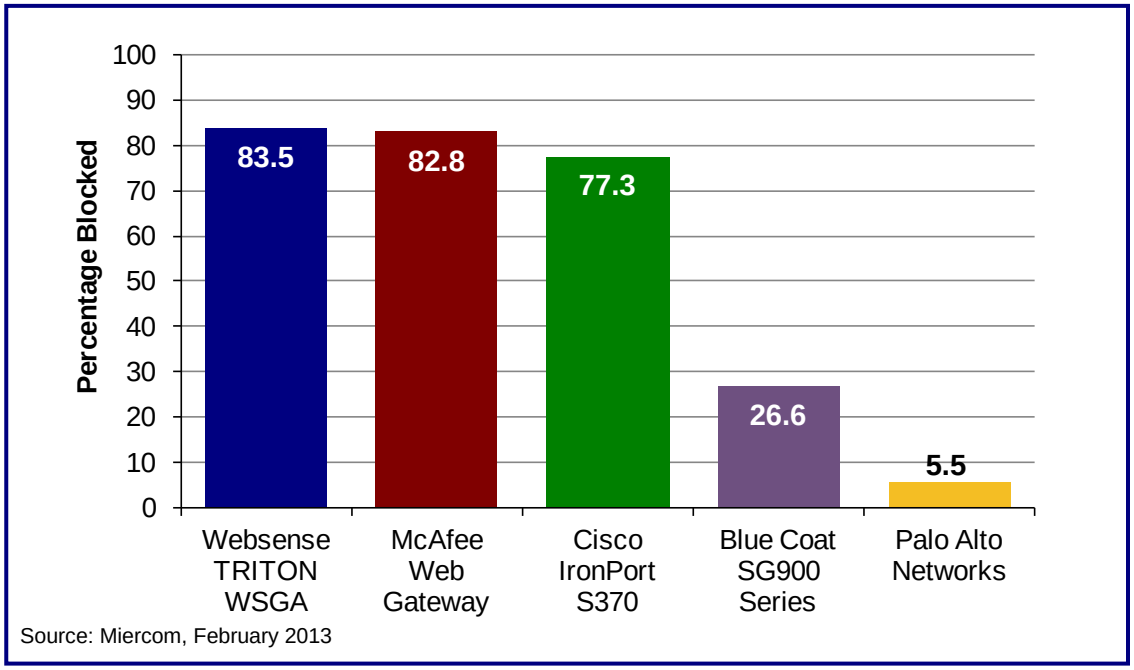
It is recognized that FireEye and other solutions may require background processes and time to confirm threats via sandboxing and forensic analysis, and thus are not suited for a point of click web threat protection test that favors real-time defenses, but the results do provide a measure of the device's ability to proactively block some malicious content in real-time. Malware sandboxing and forensic reporting are analyzed later within this report.

5.0 Modern Malware Threat Stages

Lures, redirects, exploit kits, dropper files and other advanced stages of web attacks from the cyber kill chain were used to determine inbound threat detection and blocking accuracy of each appliance. This test utilized a selection of known real-world malicious web requests containing several methods from the cyber kill chain to specifically call out effectiveness. We measured the ability of each system to detect and block web requests that contain these threats as it relates to the cyber kill chain method tested. FireEye was omitted from this test recognizing its background sandboxing analysis defenses, however the FireEye solution is reviewed later in the report for sandboxing and forensic reporting.

Lures - Users are often lured to malicious sites from web links in social networking, blogs, search engines and email or phishing with embedded web links. The lures can be free software, prize money or trips. The domain/web link appears to be a legitimate business name. However, the embedded web link is directed to a malicious website often containing exploit code. The website may also ask for personal or confidential credentials in a data theft scam.

Figure 3: Malware – Lures



Source: Miercom, February 2013

Description:

A sample set of 545 web requests containing sites that lure users to other malicious sites were tested. The number of web requests blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

Real-time Blocking Effectiveness Results:

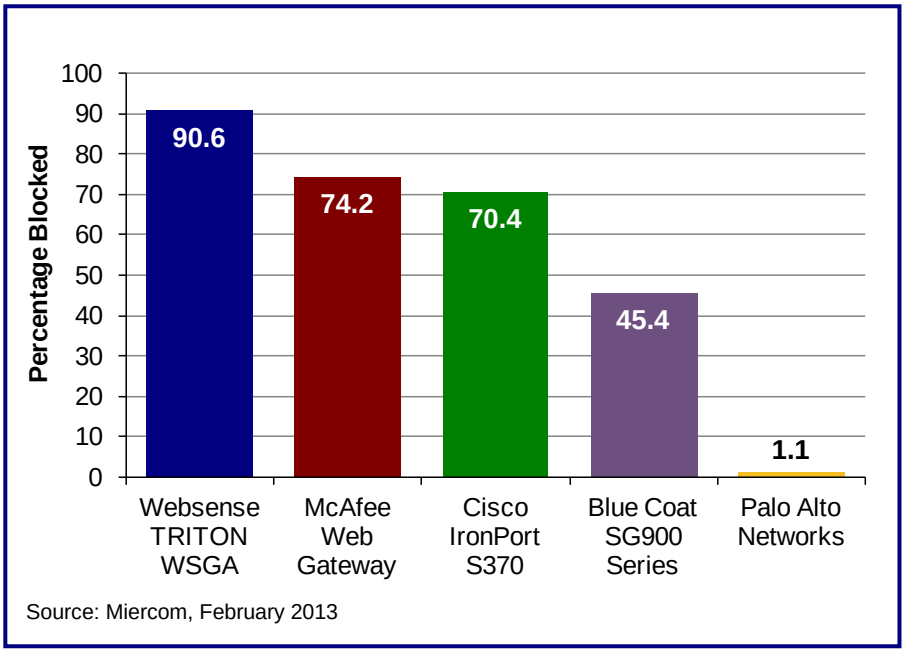
The Websense TRITON WSGA successfully blocked 455 web requests to stop 83.49% of these threats. McAfee blocked 451 for 82.75% of the web requests. Cisco IronPort blocked 421 for 77.25% and Blue Coat blocked 145 for 26.61% of the web requests. Palo Alto Networks achieved 30 blocked web requests for a 5.50% blocking effectiveness, respectively.

Exploit Kit Detection - An exploit can be used to gain control or to deny service to a computer or system. The primary source of this attack is through a compromised web site, or redirecting traffic to a malicious web site. An exploit kit will analyze a target system for vulnerabilities or an open door, and if found, the attack normally delivers a malware dropper file. If no open door or vulnerability is detected, the user advances to their desired web location keeping the exploit kit hidden from detection.

Exploit kit detection was used to test the effectiveness of the appliances in defending against such attacks as the sophisticated "Black Hole" exploit kit which is a prevalent web threat. The appliances tested were configured using the default security policies or to settings found in a typical customer configuration.

The number of web requests in each sample set was selected to be statistically relevant. A custom tool was used to initiate a connection and issue an HTTP "get" command to access the web request. The tool lists the result of the "get" command, and provided details if the page was successfully retrieved, or if a block page was issued by the security gateway and in what security rating was the request blocked. The test was configured with one retry attempt and a 90-second timeout if the target server failed to respond.

Figure 4: Malware – Exploit Kits



Source: Miercom, February 2013

Of the 628 web requests that contained exploits, Websense blocked over 90%.

Description:

A sample set of 628 web requests containing exploits was tested. The number of web requests blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

Real-time Blocking Effectiveness Results:

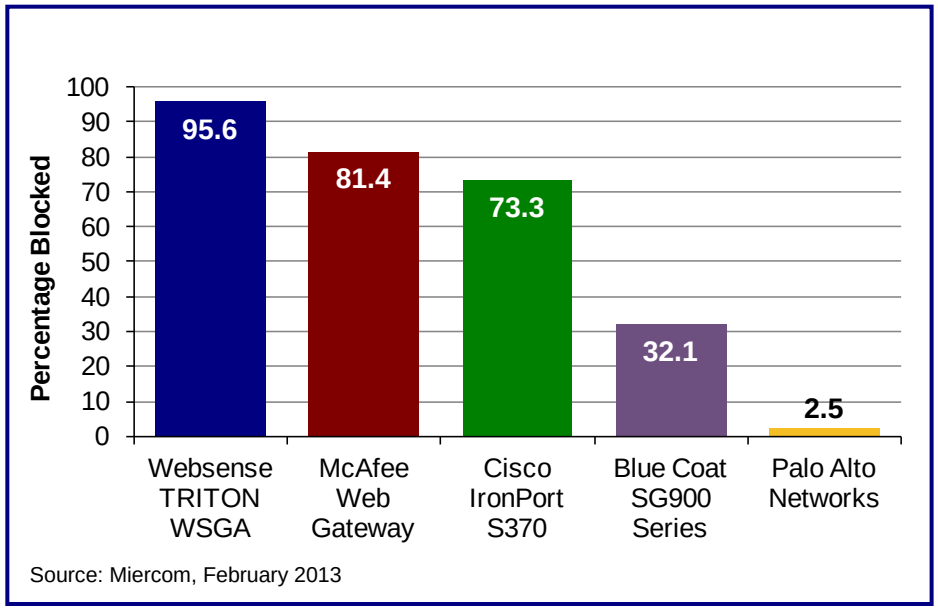
The Websense TRITON WSGA successfully blocked 569 resulting in 90.61% of these threats associated with exploit kits. McAfee blocked 466 for 74.20% of the web requests. Cisco IronPort blocked 442 at 70.38%. Blue Coat blocked 285 threats at 45.38% and Palo Alto Networks blocked 7 for a 1.11% blocking effectiveness, respectively.

Dropper Files - A program that will install malware onto a targeted system, most likely after an exploit kit has detected a vulnerability or open door into the system to evade detection. The dropper file is not malware itself; instead it carries the initial malicious code and is often not detected by anti-malware software because it is not an infected file, but carries the code to "drop" malware into a system. Many dropper files call-home within the first minute; some may delay for five minutes or longer before calling-home to download desired malware for the target system.

Once a dropper is executed, it loads itself into memory, extracts the malware payload and writes it to the file system. It may perform installation procedures and execute the newly dropped malware which often calls-home for additional malware files. The dropper usually ceases to execute at this point as its primary function has been accomplished.

Droppers are used by malware creators to disguise their malware. They create confusion among users by making them look like legitimate applications or well-known and trusted files.

Figure 5: Malware – Dropper Files



Description:

A sample set of 633 web requests representing sites with dropper files was tested. The number of web requests blocked and missed was recorded. Any errors or failures were deducted from the sample total before any calculations were done.

Real-time Blocking Effectiveness Results:

The Websense TRITON WSGA successfully blocked 605 or 95.58% of these sites. McAfee's Web Gateway blocked 515 for 81.36%, while Cisco IronPort blocked 464 for 73.30% and Blue Coat blocked 203 for 32.07%. Palo Alto Networks blocked 16 for a 2.53% total.

6.0 Data Theft and Loss Prevention

Websense TRITON WSGA was reviewed for the creation and enforcement of outbound Data Theft Prevention (DTP) and Data Loss Prevention (DLP) policies. This test solely focused on the Websense TRITON WSGA to validate the DTP and DLP policies for prevention and accuracy. We determined the accuracy of the WSGA appliance 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, and customer lists.

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.

Two scenarios of web transmission methods were tested. A web mail was composed with sensitive information and a web mail was sent with an attachment containing sensitive information.

6.1 DTP and DLP Detection Techniques

In general, 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, an 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 (or hash sums) 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 or its content. This approach does offer some limited 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 theft and loss without imposing wholesale restrictions on the transmission of the most commonly used file types.

Six different data theft and loss scenarios were validated for WSGA and the results are discussed in the following sections:

Data Theft Prevention (DTP) Controls

- Custom Encrypted File Detection
- Password File Data Theft Detection

Data Loss Prevention (DLP) Controls

- OCR of Text within an Image
- Slow Data Leak Detection (cumulative)
- Geo-location Destination Awareness
- Data Capture for Security Incidents

6.2 Custom Encrypted File Detection

To prevent data theft, Websense TRITON WSGA data theft prevention controls can be activated, including detecting custom encrypted files. This feature works by identifying the typical types of data that malicious users target, such as password databases, and the mechanisms used to transport the data over the Web (such as proprietary encryption and known malicious file structures).

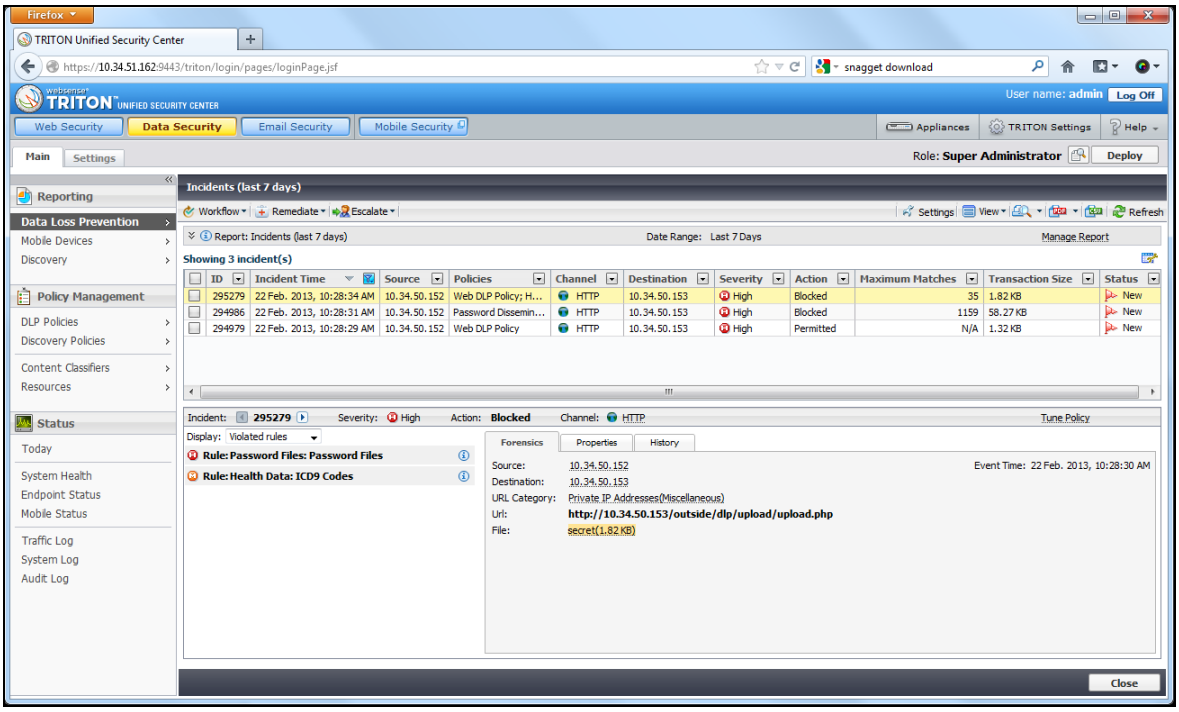
Our testing included sending a custom encrypted file via HTTP. The default for outbound scanning and data theft protection was enabled. A file named secret.tc was sent outbound through the WSGA appliance and was successfully blocked.

6.3 Password File Data Theft Detection

To prevent data theft, Websense TRITON WSGA data theft prevention controls can be activated, included the detection of files containing passwords often from AD or SAM databases. This new feature works by identifying the typical types of data that malicious users target (such as password databases) and the mechanisms they typically use to transport the data over the web (such as proprietary encryption and known malicious file structures).

Our test included sending a password list file via HTTP. The default for outbound scanning and data theft protection was enabled. A password file named secret was sent through the WSGA appliance and was blocked successfully.

Figure 6: Password File Data Theft Detection

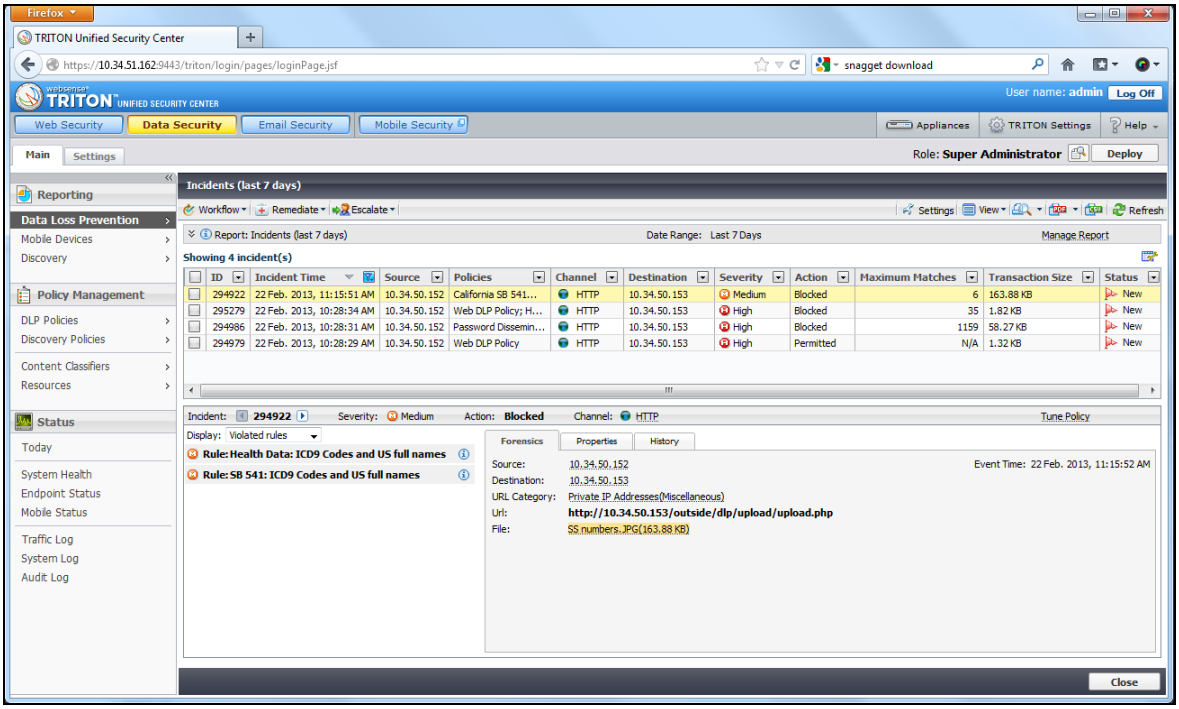


6.4 OCR of Text within Images

Many organizations now archive confidential information with images, including check images for financial institutions and health care images for patients. The advent of smartphones with high resolution cameras also enables the capture of confidential information with images for exfiltration outside an organization. Optical Character Recognition (OCR) provides the ability to detect text within images for analysis of data theft or loss. For example, an account number off a check image, a patient name and number from a health related image, or a smartphone image of intellectual property text can be detected.

This test included sending image files with various extensions containing sensitive data. The OCR capabilities for text extraction from images containing text should be detected and blocked. WSGA includes integrated DLP controls such as OCR of text within images. An image file with text named SS_numbers.jpg was sent through the WSGA appliance and was blocked successfully.

Figure 7: OCR of Text within Images



Activating the OCR DLP feature to detect image files containing confidential information can be accomplished in several easy steps. The test proved that the OCR files sent from within the company were blocked. This is a superior tool to prevent confidential information stored within images from leaving a company or organization.

6.5 Slow Data Leak Detection (Cumulative)

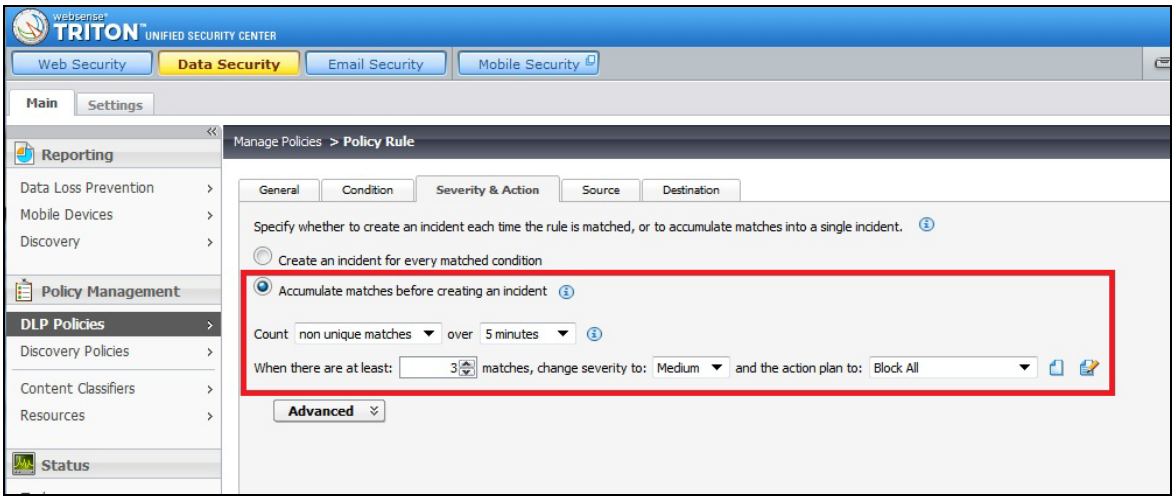
Common data leakage concerns are that confidential customer information, employee information, and intellectual property can be sent over the web, either by including that information in the body of a post or by directly uploading the content as an attachment. When enforcing policies, administrators need to be careful not to block legitimate and business critical communications, often in low volume use cases, that may be legitimate.

For example, a DLP policy is likely to only alert when a significant amount of confidential information within a request is detected, not a single instance. Attackers understand these

detection thresholds and slowly exfiltrate confidential data in small volumes to avoid detection. They also understand the most defenses are not watching the cumulative nature of outbound traffic to detect a slow cumulative data leak. Websense TRITON WSGA provides a DLP control for slow data leak detection where the administrator can define the volume of confidential information incidents and the time period.

This test determined data leaks over time; for example one credit card number from the same source in a 30-day time period. For this test and timeliness, we used credit card numbers within requests using a policy of allowing one or two credit numbers within five minutes, however blocking the use of three or more credit numbers in a five-minute time period from the same source.

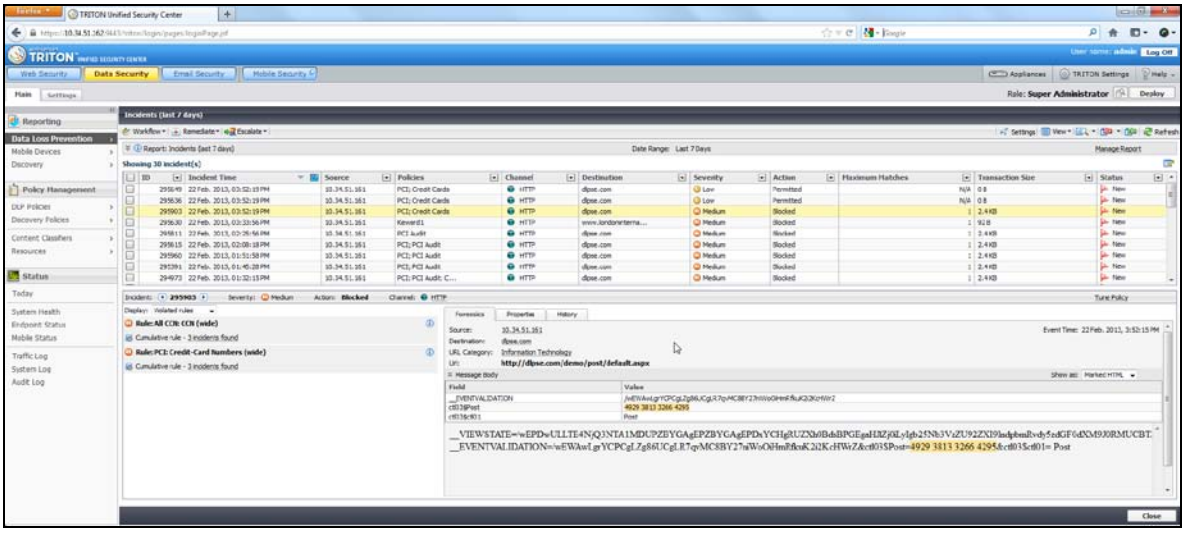
Figure 8: Slow Data Leak Detection



The results for this test proved to detect data loss using the policy of three credit card numbers within a five-minute period from the same source and blocking the data from leaking out.

The results are displayed in the following screen.

Figure 9: Results of Blocked Data Leak

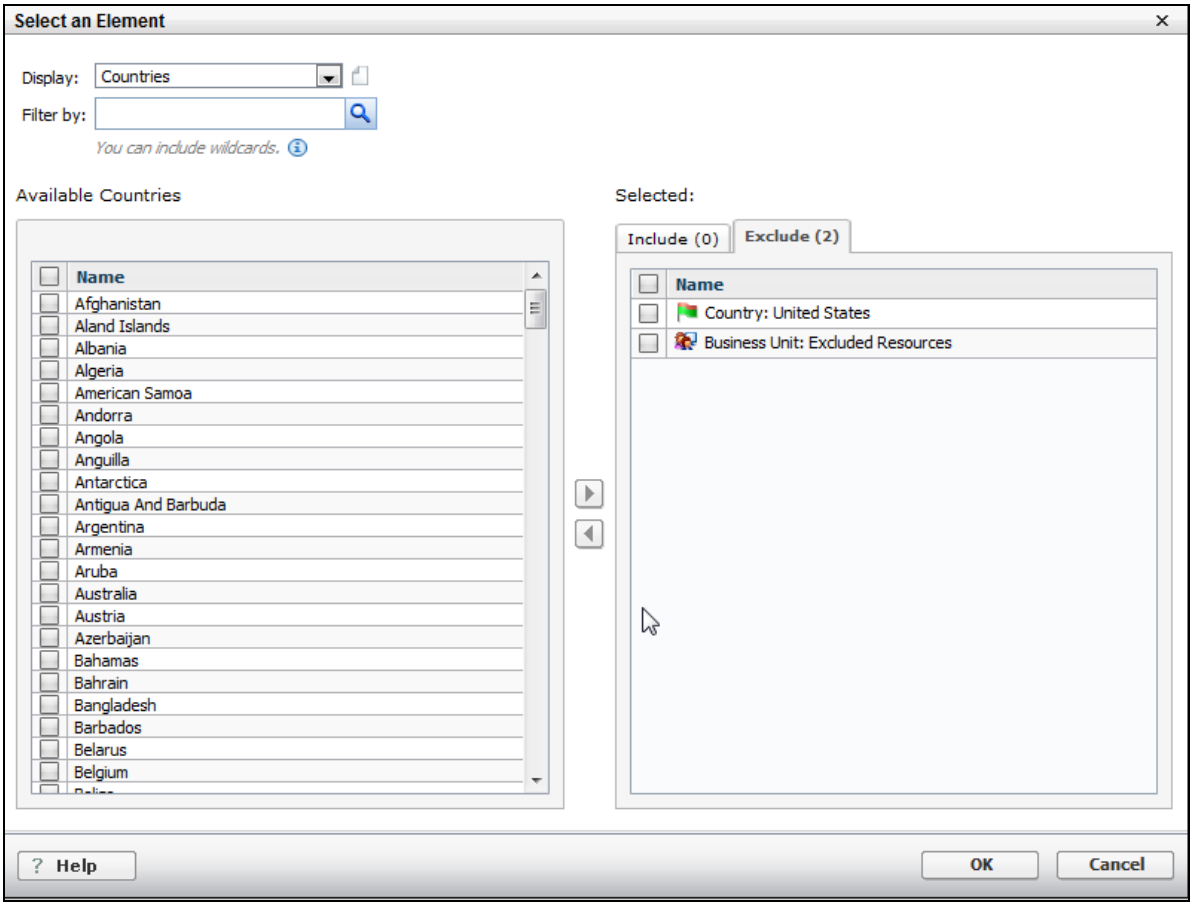


6.6 Geo Location Destination Awareness

Using this feature, one can create and enforce a policy based on the destination country. Countries can be specified as web destinations, and users can be blocked from uploading data to web sites that are hosted in specific countries. Geo destination awareness can also be useful in forensic reporting on security incidents to understand where communications were destined, along with who was attacked, how, and what data was targeted.

This test uses a policy that allows the keyword FTKW to post within the USA but block if it is posted to any other country as shown below:

Figure 10: Destination Configuration with Keyword



After managing policy by key word and selecting a destination, there were six different destination categories in the “Display” field to choose from: Countries, Domains, Networks, Web Categories, Business Units, and Custom Computers. For all six categories, an include and/or exclude option was available.

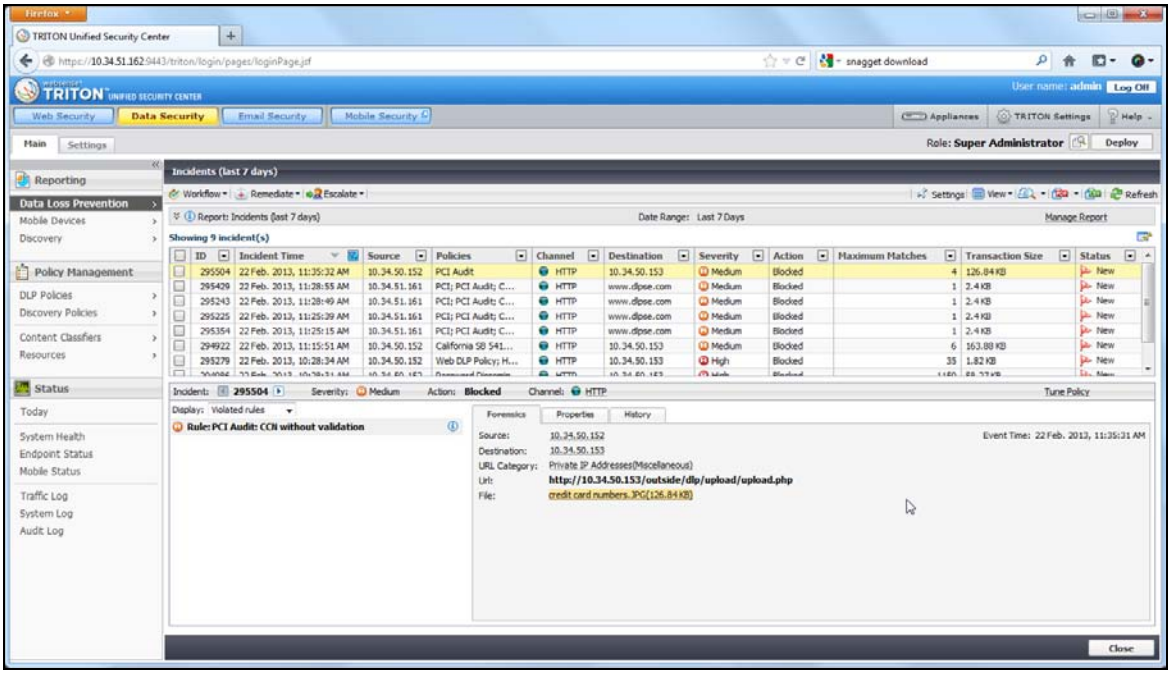
These features enable very granular blocking by destinations. For example, a policy can exclude one country, however, the policy may still need to access a certain set of networks within that country, so the policy can exclude the set of networks that require access and block everything else for that country.

6.7 Data Capture for Security Incidents

For security incidents when possible, one needs to capture the data file or content within the request for forensic analysis. This provides security administrators with a more complete picture of the security incident by knowing the targeted data.

This test uses the image file capture of confidential customer information as shown below to validate the feature. Clicking on the file itself will display the image for forensic analysis, role-based administrative rights to forensic details are included with WSGA. An image file with text named credit card numbers.jpg was sent through the WSGA appliance and was blocked successfully.

Figure 11: Data Capture for Security Incidents



Real-time Blocking Effectiveness Results:

Websense TRITON WSGA includes full-featured enterprise DTP and DLP content-aware capabilities, providing the full range of policy tools including pattern matching, fingerprinting and binary containment of data theft.

Websense proved to detect and block data theft for the six features tested. Configurations to block data theft are a simple to set-up. Successful detection of custom encrypted and non-encrypted files, such as a password file, were blocked, plus slow data leak detection, geo-location destination awareness controls and forensic reporting, OCR of text within images, and data capture for security incidents.

To verify the incident, a complete screen capture is displayed showing the incident, source, rules and policy that triggered it. The screen captures also identify that the tested file was blocked.

7.0 Malware Sandboxing and Forensic Reporting

Understanding malware infection processes, outbound requests and system changes via sandboxing of potentially malicious files provides important insight for remediation efforts and improved defenses. The combination of malware sandboxing with detailed forensic reporting enables security administrators to safely analyze malware and understand its impact and focus.

Sandboxing has been around for years as a background passive analysis within security labs and is now surfacing in customer facing solutions such as the Websense TRITON WSGA with the ThreatScope malware analysis sandbox, plus the FireEye Web MPS and MAS solutions both using sandboxing of suspicious files.

As part of malware sandboxing and forensic reporting testing, Websense TRITON WSGA with ThreatScope and FireEye MPS 1300 appliance were reviewed and compared for malware analysis details and forensic reporting. The testing used a set of five web requests with known malware infected or malicious files. The testing determined the outcome of these web requests and their associated files by the ease of use, malware analysis, drill down mode, and the forensic reporting features available.

Reporting Feature Summary Table		
	Websense TRITON WSGA and ThreatScope	**Fire Eye Web MPS 1300**
Threat Dashboard	●	▲
Customizable Severity Levels	●	■
Malware Forensics	●	▲

Scoring Key:

● = Full coverage

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

■ = No coverage

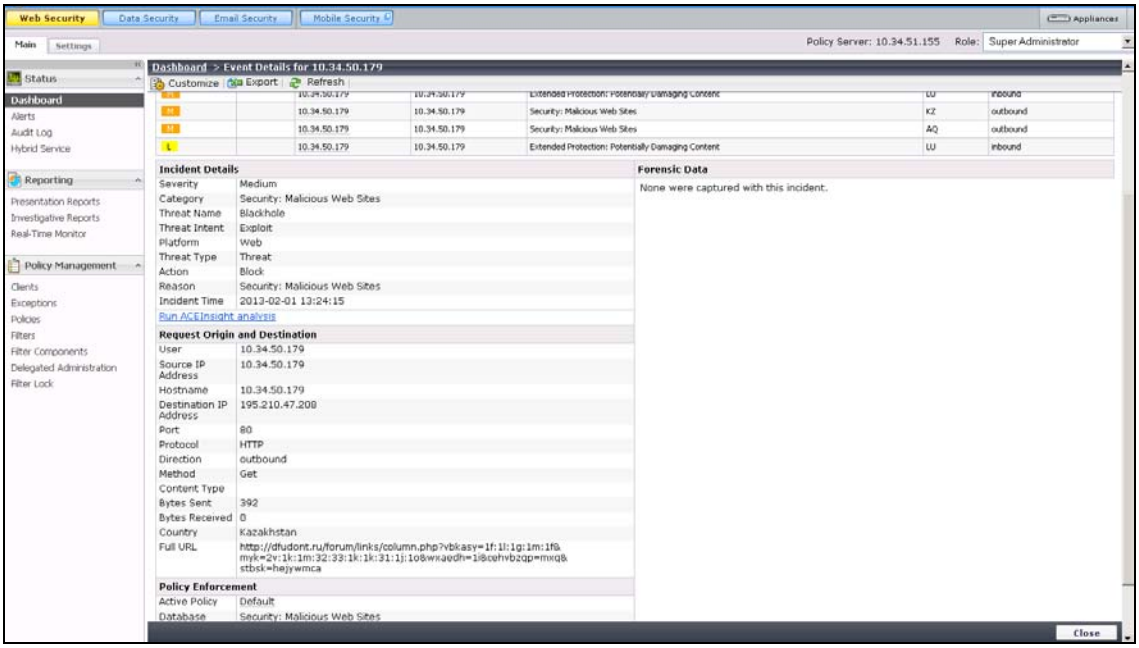
Threat Dashboard Categorizations and Features

Product	Suspect Clients	Malware Activity	Severity Level	Incident Details
Websense	●	●	●	●
FireEye	▲	▲	●	■

Websense TRITON WSGA provides a clear description and detailed graphics to make it easier to obtain information on suspected malware clients. The information can be obtained by severity level and/or severity incidents. Websense also offers a detailed incident report with choices for the client, severity or malware. Information that was presented in the Incident Details screen was: threat name, content type, action taken, full web request and other data points. Also

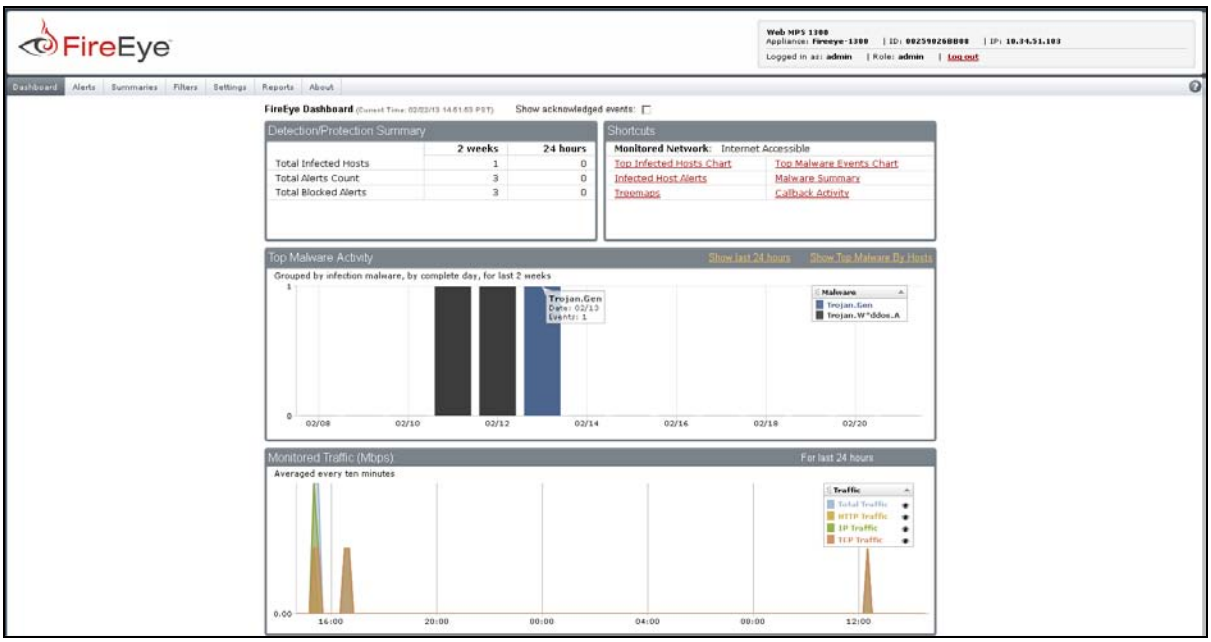
included on this screen is Policy Enforcement: active policy and database. Policy enforcement is the policy that was created either by default or customized by the admin specifying what types of features and subjects will be denied or allowed.

Figure 12: Threat Dashboard Forensic Reporting - Websense



For the FireEye solution, the forensics dashboard was not as intuitive as the Websense TRITONN WSGA threat dashboard. Once a user or incident was selected in the FireEye console, not much more information was retrieved. The user would have to navigate to other areas within the console to obtain all the information that Websense gives you in one location.

Figure 13: Threat Dashboard Forensic Reporting - FireEye



Customizable Severity Levels

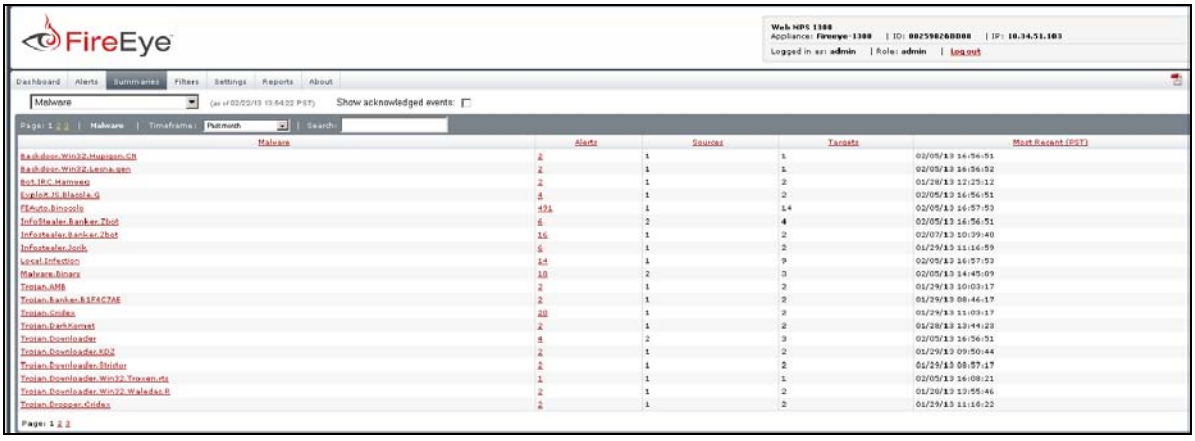
Product	Number of Screens	Number of Sub Screens	Number of Clicks	Average Time to Complete
Websense	2	0	2	1 minute
FireEye	4	0	4	10 minutes

Websense had a clearly defined tab to customize the severity report. Once the tab is clicked, a customized column screen appears that allows you to change ten different severity categories.

Figure 14: Customized Severity Reporting - Websense

FireEye customizable features were not as detailed as Websense. The solution lacked pull down menus to select options. This made it very time consuming from an administrative perspective.

Figure 15: Customized Severity Reporting – FireEye



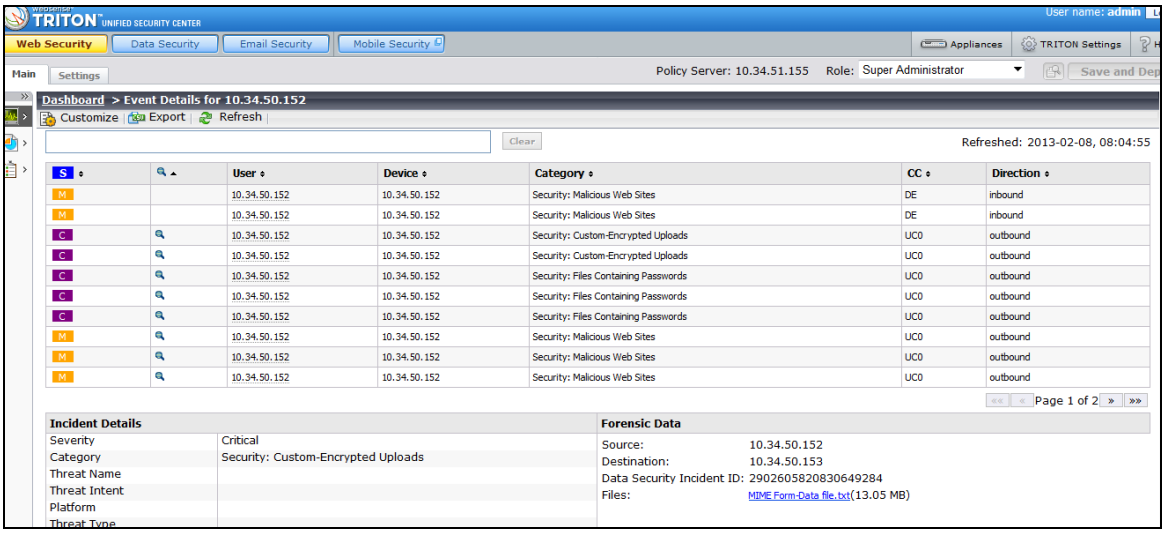
Advance Malware Forensic Report

Product	Malware Type	Malware Intent	Target Platform	Attack Name	Show Actual Document
Websense	●	●	●	●	●
FireEye	●	▲	■	■	■

The Websense TRITON WSGA Threat Dashboard provides forensic reporting including who was attacked, how the attack operates, where communications were destined and what data was targeted. Analyzing malicious files further in the ThreatScope malware sandbox provides detailed analysis across seven reporting areas including: registry and file system modifications, global system events, process modifications, resolved hostnames, IP addresses, and requested URLs.

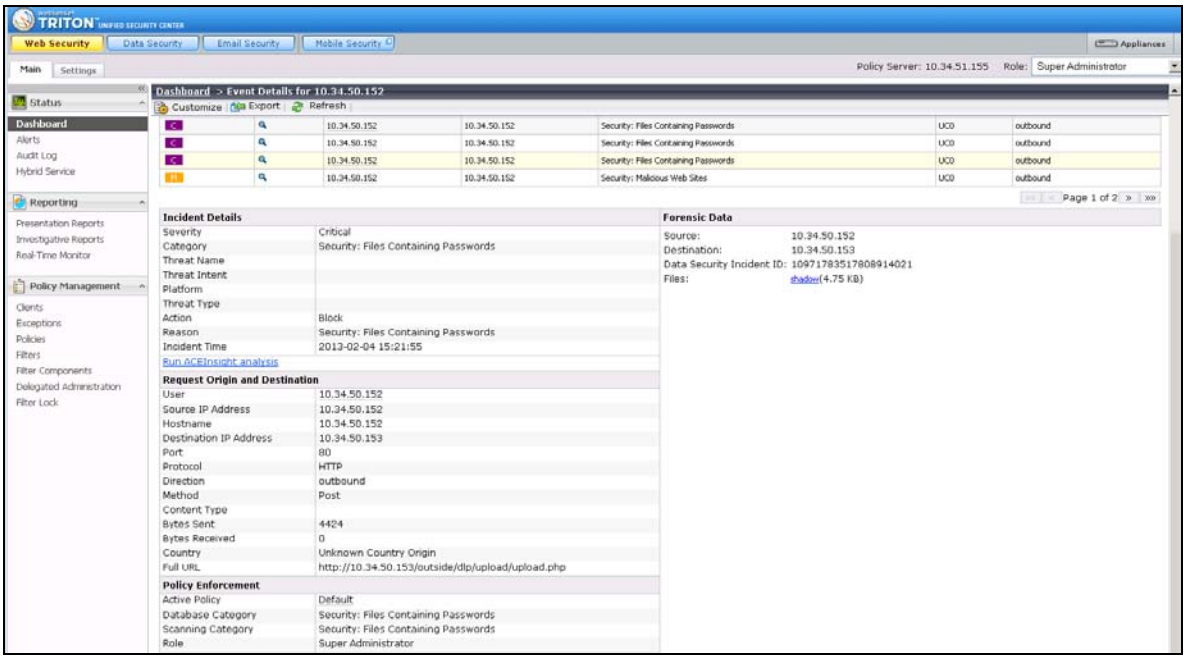
Several tests with encrypted password files, encrypted files and malicious embedded links were completed. This was to determine if Websense defenses would detect them and accurately display all forensic information associated with the threat or security incident.

Figure 16: Advanced Malware Forensic Report



Websense correctly detected and blocked the password file and the custom encrypted file which were headed outbound through the security gateway. This detection is a great tool for protecting company confidential information as noted in the DTP and DLP section. It also detected and correctly categorized malicious embedded websites for both in and outbound as seen below.

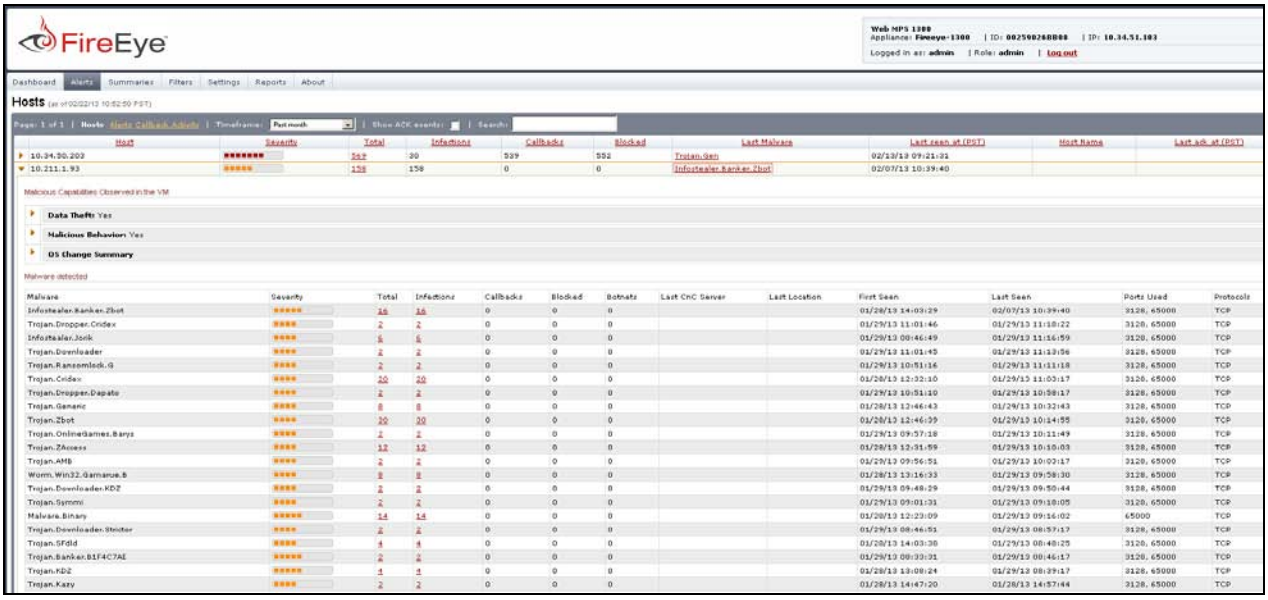
Figure 17: Forensic Reporting Drill Down – Websense



All data/files that are associated with a malware threat are blocked, and Websense populates the Forensic tab with an icon for further investigation.

To further investigate the details regarding this file, clicking on the forensic icon will open the Advanced Malware Forensic Report. This report is neatly categorized by Incidents, Incident Details, Forensic Data, Policy Enforcement, and Request Origin and Destination. In this screen, you can easily export this data to a SIEM by clicking on the export tab or by customizing it to only include the details you require.

Figure 18: Forensic Reporting Drill Down - FireEye



In FireEye alerts, the user has to navigate through several tabs to gather data like Incident details, Forensic Data, Policy Enforcement, and Request Origin and Destination. Additionally, there appears to be no way to drill down to specific malware incidents directly from their Dashboard.

ThreatScope Analysis Report

Product	Threat Level	File Details	Technical Details
Websense	●	●	●
Fire Eye	▲	▲	▲

The Websense ThreatScope sandbox malware analysis report initially displays a table reporting the threat level and the assessment of that threat, such as Threat “Critical”, Assessment “Injects and executes code in remote processes”. The report also includes screen shots, file details such as file size, time and hashing in three different forms (MD5, SHA-1 and SHA-256). For the technical details, ThreatScope provides requested HTTP URLs, resolved hostnames, IP addresses, file system modifications, process modifications, plus registry and global system events. The report is easy to understand and flows nicely with detailed graphics to support the text.

FireEye Web MPS 1300 report did not provide the same ease and flow to generate as did Websense. The report, although detailed in many aspects, however does not summarize the findings nor does it provide any recommendations for the administrator to help mitigate the threat.

8.0 Manageability and Effectiveness

This section focuses on administrative measurements recorded for the performance of common management tasks to judge the overall effectiveness and deployment of the product. The review provides quantified time and motion analysis of common management tasks. Tasks to be included: creating block policies, ad hoc reports, review dashboard graphs, drill-down reporting, and other typical management tasks.

Measurements were recorded for the amount of time and number of steps required to perform common management tasks. Scoring was based on factoring in the amount of time to complete a specific task, the number of steps (clicks) and the number of different screens or pages accessed, 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 botnets, malicious content such as malicious direction, malicious obfuscation, malicious exploits, objectionable sites, adult/porn, gambling, illegal activities, hacking, proxy avoidance and inbound malware.
- Create and apply a policy to block outbound transmission of sensitive document 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
- Dashboard reporting
- Policy configuration (security features)

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 WSGA	**Cisco IronPort**	**McAfee Web Gateway**	**Blue Coat SG900**	**Palo Alto Networks**
Actionable Dashboard	●	▲	⯃	⯃	⯃
Unified Policy Management	●	⯃	⯃	⯃	●
Custom Security Report Generation	●	⯃	⯃	⯃	●
Drill Down Reporting	●	⯃	⯃	⯃	▲

Scoring Key:

● = Full coverage

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

⯃ = No coverage

Manageability Time Requirements in Minutes					
	Websense TRITON WSGA	**Cisco IronPort S370**	**McAfee Web Gateway**	**Blue Coat ProxySG 900 Series**	**Palo Alto Networks PA-2020**
Actionable Information Retrieval	.5	.52	N/A	N/A	10
Policy Creation	5	10	20	30	15
Custom Security Report Generation	2	N/A	N/A	N/A	5

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
Palo Alto Networks	3	2	4	30 seconds	

Websense initial dashboard screen included two graphs, one showing the inbound threats and outbound risks by country, where the threat was generated and a bar indicating the type of threats along with the date and time. In either graph, you can click on the threat and drill down to users or devices.

Palo Alto Networks did require creating a filter when looking up an individual user. The filter then retrieved information about that user and the associated threats. This action was not a drill down method, but a search inquiry.

Management Task: Create and apply a policy to block botnets, malicious content such as malicious direction, malicious obfuscation, malicious exploits, objectionable sites, adult/porn, gambling, illegal activities, hacking, proxy avoidance and 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	
Palo Alto Networks	3	6	25	10 minutes	You must create an object profile then bind it to the policy

Creating a policy for Websense was a bit complicated, however, not as complicated as McAfee. The tutorial/help function was extremely useful and informative to get the job done in a timely manner.

Creating a policy for McAfee was very complicated. The appliance would be more geared toward a savvy administrator who can get more granular in policy making.

Palo Alto Networks had a straight forward approach that most beginner administrators could configure.

Blue Coat appearance is in a more text-base form, however, an intermediate administrator could configure a policy.

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	
Palo Alto Networks	3	6	25	10 minutes	You must create an object profile then bind it to the policy

Websense GUI became instrumental in creating a policy.

Palo Alto Networks is a relatively simple setup, however, it acts more like a firewall.

McAfee creation of a policy is complex and geared towards a Security Admin rather than beginner users.

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
Palo Alto Networks	2	2	5	5 minutes	

Creating an ad hoc report listing top security risks by user is user friendly, intuitive with either self explanatory tabs and easy to drill down mode for Websense.

For Palo Alto Networks, you need to create a filter for the user or users to create a report. These steps were not as intuitive as Websense.

Management Task: Create an ad hoc report on top Malware threats.

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
Palo Alto	2	2	3	5 minutes	

Real-time Blocking Effectiveness Results:

The Websense TRITON WSGA 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 TRITON WSGA.

The McAfee user interface was feature rich and granular, though not always intuitive.

Both Palo Alto Networks and Cisco's global policy has a predefined list of URLs which are selectable by checkbox and can be scheduled. However for Palo Alto Networks, an object profile needed to be created specifying the URLs to be blocked from their predefined list. After which the two needed to be bound. An object profile specifies if it is a URL filtering, antivirus, malware or so on. Once this is created, then it needs to be bound, or associated with a policy. A policy describes the inbound/outbound traffic and whether it is allowed, blocked or denied.

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. Cisco IronPort lacks native customized reports but third party applications can be used. The McAfee Web Gateway and Blue Coat ProxySG products need separate reporting products to state threat information. Palo Alto Networks had standard reports for tracking alarms by threat, attacker or victim.

9.0 The Bottom Line

Websense TRITON Web Security Gateway Anywhere (WSGA) achieved high scores in security tests for:

- **Detecting and Blocking of Multiple Types of Malware Threats**

  Websense TRITON WSGA discovers and blocks web threats and malware attacks with Advanced Content Engine (ACE). The gateway prevents over 90% of advanced malware attacks with the main emphasis on security related threats.

- **Manageability and Effectiveness**

  Websense TRITON WSGA was easy to setup, had exceptional graphical interfaces, intuitive policy creation with detailed logging and reporting. When compared to other products, the Web Security Gateway Anywhere was superior in manageability measurements, such as the ease of report customization, the number of drill-down screens, and the number of steps to complete a standard task.

- **Implementing Data Theft Prevention (DTP) and DLP Policies**

  The Websense TRITON Web Security Gateway Anywhere presents the most effective DTP and DLP policy controls that include password file theft detection and the use of custom encryption. The OCR feature is capable of detecting and blocking outbound images that contain confidential information. Detecting slow data leaks and blocking by geo-destinations for outbound traffic enhances the security provided by the Websense solution.

- **Sandboxing and Forensic Reporting**

  Websense advanced threat dashboard and forensic reporting provides full details on who was attacked, how they were attacked, where communications were destined, and what data was targeted. The ThreatScope malware analysis sandbox provides detailed forensic reporting on malware infection steps, systems changes and call-home communications.

Overall, Websense TRITON WSGA is a superior web security appliance, providing network protection from malicious attacks while guarding business-critical information from data theft schemes.

Other Notes and Comments

About Miercom

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including *Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony* and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.