



EMAIL APPLIANCES FOR THE
SMALL/MEDIUM-SIZED BUSINESS MARKET

DECEMBER 16, 2007

IT departments spend almost 10% of their time managing email filtering solutions.

(InformationWeek Research Survey, Nov. 2006)

An IT Manager's time and budget are limited, and the ideal solution is one that best matches both the company's needs for security and its needs for IT efficiency and productivity.



In this review:

CLEARSWIFT MIMESWEEPER 2.6

IRONPORT C150

SOPHOS ES1000

Email today is the cornerstone of corporate communication. In our world of always-on connectivity, it is expected to be available and reliable around the clock. Users also expect it to be free from spam, phishing and malware, as these threats severely impact its ongoing effectiveness as a business tool. In many small and medium companies, maintaining a safe and reliable environment is a top IT priority.

A November 2006 InformationWeek Research Survey found that IT departments spend almost 10% of their time managing email filtering solutions. With all the other demands on their time, there is great pressure to ensure that the email security solution in place meets or exceeds expectations on protection, administration and support. After all, while email might be a strategic necessity, managing email security probably is not.

This review evaluates appliance-based options from the perspective of performance and day-to-day administrative effort for small- and medium-sized businesses. Our testing scenario assumes that for this market, an IT Manager's time and budget are limited, and the ideal solution is one that best matches both the company's needs for security and its needs for IT efficiency and productivity.

THE EVOLVING NATURE OF EMAIL SECURITY

According to the Gartner Group's report, Magic Quadrant for Email Security Boundary, 2006, "efficient and accurate spam and virus filtering remain essential to buyers; however, it is generally the secondary features that win deals." The report cites features that lower administration overhead, policy-based outbound content inspection, encryption and appliance MTA (Mail Transfer Agent) capabilities as increasingly important, driven by a desire to consolidate e-mail infrastructure. Emerging concerns about compliance and data leak prevention are also stimulating demand for enhanced outbound inspection and encryption. The report goes on to say that a complete solution would require a spam catch rate of at least 95%, and that keeping the email infrastructure up and running is priority #1 for IT managers.

WHO WE TESTED

In this review we looked at three popular appliances that are currently marketed to small and medium businesses, which we define as having between 100 to 1000 users. We tested a Sophos ES1000, Clearswift MIMESweeper 2.6, and Ironport C150. We looked carefully at ease of installation but then focused in on everyday ease of use, management, policy creation, reporting features and how reliably the appliance carried out its mission, since those are the things that an IT manager will end up living with daily. Since all three appliances were able to handle the same volume of mail with similar throughput speeds, we chose to ignore this as a test criterion.

Overall, the Sophos ES1000 provided the best combination of security, functionality, ease of use and price for SMBs.

THE RESULTS

Our test reveals that all three products deliver reliability and protection, often exceeding the criteria defined in the Gartner Group report. That said, the products clearly have different strengths, and an IT Director will want to choose wisely depending on the organization's specific requirements. In putting each of the appliances through their paces we found one – the Sophos ES1000 – to be changing the landscape of email appliances, as well as to be offering IT Directors a persuasively innovative way to simplify their operations. It was this forward-thinking and somewhat future-proofing approach that set the Sophos ES1000 ahead of its peers as a more valuable solution for SMBs.

The ES1000's integrated support complete with real-time security updates and its highly intuitive management console make this product a standout in the group. Spam catch rates were the highest we tested at 99.4%, and the GUI reliably delivered minimal click-through management and day-to-day ease of use. Automatic self-maintenance and remote monitoring (standard) are especially beneficial to SMB administrators, as was the ability to remotely tunnel into the device (also standard) for extended troubleshooting support. Compliance is enabled through solid protective controls, and reporting is informative. Overall, the Sophos ES1000 provided the best combination of security, functionality, ease of use and price for SMBs.

	Clearswift	IronPort	Sophos
Installation / Deployment	7	8	10
Managability / Usability	7	8	10
Reporting / Compliance	10	9	8
Price	8	6	7
Totals	32	31	35
Weighted Scores	7.6	8.0	9.4
Summary	Robust feature set; Wide range of reporting; Complex management	Decent reporting; Acceptable installation; Low spam protection	Ease of management; Good vendor support; Basic reporting

The IronPort C150 from Cisco is a robust solution, but installation and configuration is more complicated, requiring more effort than is typically expected by the SMB market. The appliance is administered via a combination of Web-based interface and command-line access, which we found to be cumbersome and time-consuming. The product delivers all the standard must-haves for an all round email gateway but other than logging into the device, there is no effective monitoring capability. Reporting



APPLIANCE SPECIFICATIONS

Clearswift MIMESweeper:

Dual Intel Xeon processors, 2GB RAM, two 250GB SATA drives in Raid 1, Linux OS

IronPort C150:

Single Intel processor, 2GB RAM, two 80GB SATA drives in RAID 1, AsyncOS

Sophos E1000:

Single Intel Celeron D processor,, 1GB RAM, one 160 GB SATA drive, FreeBSD OS

capabilities are limited although we liked the scheduling and mailing feature that was available. Protective controls for compliance are adequate. The C150 detected 96.9% of spam during our test, which unfortunately ranked it last of the three appliances. The device can be fine-tuned by the administrator to increase its effectiveness, but this adds administrative burden and reduces its overall attractiveness to our target market. The company states that the C150 is positioned to be affordable, however, it was significantly more expensive than both the Sophos and the Clearswift appliances.

The MIMESweeper 2.6 from Clearswift finished third in our ranking. After getting over initial difficulties adapting to a less-than-intuitive interface and complicated configuration rules, it did provide reliable email security. Its broad functionality includes features such as lexical pattern matching and a wide range of customizable reporting. It offers extensive support for compliance with policy violation alerts and protective controls. Unfortunately, all this means that the MIMESweeper 2.6 has all the attendant complexity of such a large feature set, coupled with little built-in support. Documentation was poorly organized and not clearly written. While the MIMESweeper came in as the least expensive solution - only marginally more than Sophos - its complexity and lower spam catch rate caused it to lose ground in our test.

Price Breakout:

(for 1,000 users, 1 year license, hardware included, all figures in US dollars)

Clearswift MIMESweeper: \$17,699

IronPort C150: \$29,500

Sophos ES1000: \$20,795

All these appliances require subscription renewals.



We evaluated each appliance against one another in the following categories:

- Installation and deployment
- Usability and management
- Reporting and compliance
- Price

THE eVISION IT LABS TEST BENCH

We used a test environment that emulates a business of 1,000 users divided into groups to represent the Sales, Human Resources, and Accounting departments, as well as an executive level. Users were simulated using custom-built scripts representing various email patterns including both "live" spam feeds and "canned" spam, and attachments of various lengths with viruses attached. Keeping security in mind when the devices were tested in a "live" environment, we used the Internet standard EICAR to emulate virus testing while the DUT (Device Under Test) was under heavy load.

The goal of each test is to get approximately 10,000 messages sent through the device under test (DUT). We used a scaled approach; starting with 100 messages and increasing to 1,000 inbound per minute weighted across each department. Attachments were set to two different parameters – 64Kb and 1Mb. We used a ratio of 50% spam, 20% spam with a known virus attachment, 20% varied virus, and 10% content specific (for testing content filtering).

We evaluated each appliance against one another in the following categories:

- Installation and deployment
- Usability and management
- Reporting and compliance
- Price

Each appliance was scored on a scale of 1 to 10, 1 being poor and 10 being excellent. Keeping the needs of the SMB in mind – compared to the large enterprise which might have different priorities – each category was then assigned a weighted ranking based on relative importance. The weighted rankings are as follows:

Category	Weighting
Installation / Deployment	30%
Managability / Usability	45%
Reporting / Compliance	15%
Price	10%

INSTALLATION AND DEPLOYMENT

Here we evaluated the ease of initial setup and configuration for our 1,000-user test bench for each appliance. This included elements such as the sales ordering process, accuracy of delivered product, and the initial physical installation. We considered the clarity and simplicity of Quick Install or Setup Guides. We also measured the ease of use of any tools and/or wizards that were built in to assist us in the setup and configuration. Deployment was defined as the setup for the test bench – similar to an organization configuring the device for their unique environment.



Data leakage prevention (DLP) is a growing concern for companies of all sizes and industries.

IT administrators usually assume a degree of responsibility in safeguarding confidential data.

USABILITY AND MANAGEMENT

For this part of the test, we evaluated the experience during common administrative activities such as managing users and groups and changing policies. We considered the number of steps it took to create a policy (e.g. filtering outbound messages for keywords), update the software and make other configuration changes. The ability to search for quarantined messages and retrieve information from message logs was also tested as a day to day operation.

REPORTING AND COMPLIANCE

For reporting and compliance testing, we analyzed and evaluated the standard reports (both quantity and detail), as well as the ability to meet output requirements and generate custom reports. These features are increasingly important to both security and general business policy; visibility of email traffic is vital to enforcing acceptable use of email and to planning infrastructural changes. Knowing what to do next is often dependent on the data that can be extracted. We looked at ease of access to reports, intuitiveness, and availability of options and templates. The ability to export data was also noted, as were alerts and other forms of notification on system performance. We also looked at how reporting enabled business managers to evaluate the implementation and effectiveness of IT policies.

Data leakage prevention (DLP) is a growing concern for companies of all sizes and industries. Customer records, financial documents, trade secrets and similar information are not only vital business records, but they also represent potentially serious legal, financial and public-relations landmines should they fall into the wrong hands. The news is filled with stories of organizations like United States Veteran Affairs, Salesforce.com, TJX and the UK government's customs department losing confidential data and suffering both financially and reputationally.

Since as much as 80% of business records are contained in email, and email is owned by the IT department, IT administrators usually assume a degree of responsibility in safeguarding confidential data. Since email security solutions play a key support role, we investigated what each appliance offered in terms of data leakage prevention capabilities.

PRICE

While price is a key factor, we see Total Cost of Ownership (TCO) as a more important measurement. Total Cost of Ownership includes the cost of the hardware, software, and all the costs associated with implementation, including administrator time, outside consulting, ongoing support, and maintenance. It also includes the cost of running the device for two years after implementation. This is when the administrator really begins to "learn" the true cost of owning a system, as they begin to run through their day-to-day operations.



Sophos support centers span the globe, proactively monitoring every Sophos email appliance 24/7.

Automatic self-maintenance and remote monitoring (standard) are especially beneficial to SMB administrators, as was the ability to remotely tunnel into the device (also standard) for extended troubleshooting support.



ABOUT EACH PRODUCT

Sophos ES1000

Sophos takes a visionary approach with its ES1000 appliance. At the source is a unique global network of spam and malware analysis centers, sorting through millions of email messages, web sites and malware samples every day in search of new threats. Sophos is consistently ranked as a top-5 vendor in threat response, as per organizations such as av-test.org and secunia.com. Sophos support centers span the globe, proactively monitoring every Sophos email appliance 24/7. An example of this is rather than go the SNMP route, which is an insecure system prone to error and interruption, Sophos will monitor the appliance directly, through a system of built-in sensors that watch everything from unit temperature to disk space to update status, etc. topping at upwards of 50 different alerts. The appliance will trigger alerts to the admin and/or to Sophos in the event of an abnormal condition being met. This refreshingly unique approach actually caused us to be notified by email and telephone when, as a part of the test, we took the device off-line.

Sophos offers a full range of security solutions built for business. Alongside the ES1000, there is a second email appliance – the ES4000 – designed for larger enterprises, a web appliance built for SMBs, a Network Access Control solution and an endpoint security suite that combines anti-virus, anti-spyware and application control. Sophos claims to protect more than 100 million customers in nearly 150 countries.

INSTALLATION AND DEPLOYMENT

From the very start, it was evident that one of the ES1000's strong suits was ease of use. Simple and easy to read instructions, clearly defined steps, and an activation key that was emailed to us before we received the unit made for faster than expected initial setup of DNS settings, domains, internal mail hosts, and even basic policy. The setup wizards were intuitive and efficient to use. Upon completing the wizard, the device runs diagnostics to ensure connectivity, a simple yet effective method of confirming proper configuration.

Documentation included a Setup Guide in print as well as on online PDF version. Default settings allow instant anti-spam and anti-virus protection in one of three deployment modes, with "full" mode allowing filters to be set across the entire user base. Once we completed the installation process the summary page allowed us to review our configuration, make edits, and print our settings

USABILITY AND MANAGEMENT

Again, Sophos scored well in this regard. Consistently easy to use and very intuitive to our testers, the ES1000 simplified many of the tasks that would be required to keep email secure. Sophos relies on HTTPS web based administration, however SSH connections can be used as well. Had we needed technical assistance, we could have established an SSH tunnel to Sophos, granting a Sophos support technician access to the device to help resolve the issue. The secure tunnel would have automatically expired in 4 hours – a feature designed to preserve device integrity and security.

The ES1000 provides administrators with plenty of flexibility when it comes to directory service integration. It is fully integrated with LDAP and can synchronize automatically with Microsoft Active Directory.

We were able to capture 99.4% of spam emails, change policies, add trusted mail relays and more, easily and efficiently.

By default the device is configured with security in mind. Emails are scanned both inbound and outbound, and the interface provided us with the flexibility to changes policies based on groups and users and custom groups. Policy configuration was the easiest of the appliances we tested; we found it took us about three steps to generate an outbound content inspection policy. Policies can be added or deleted, enabled or disabled as well as re-ordered with a simple drag and drop process in the Web-based UI. Additionally, message action features make easy work of the notification and disclaimer/banner process, a critical part of demonstrating compliant email practices.

Overall, the device performed well above expectations. The ES1000 is able to disinfect many common file types such as ZIP, ARJ, CAB, RAR and LHA formats. We were able to capture 99.4% of spam emails, change policies, add trusted mail relays and more, easily and efficiently.

SOPHOS ES1000 DASHBOARD



REPORTING AND COMPLIANCE

The ES1000's reporting capabilities are sufficient for the majority of organizations in this target market, although not as broad as Clearswift's or as flexible as IronPort's. The ES1000 has an informative and easy to read main reporting page that provides an excellent summary of recent activity. A good range of policy, usage and traffic reports can be printed, exported and saved if required. Detailed reports can be modified for period and type (line or bar, with or without data tables).

Like its counterparts in this test, the ES1000 provides good tools for companies to avoid leakage of confidential information via email. It can scan outbound emails for keywords – regular expressions and strings – attachment types and message size, and it can add customer banners/disclaimers as well. These actions can be applied globally or for defined groups and users, and can trigger customized policies in the event of a rule hit.



Status	Monitor	Message	Potential remedies	Last exceptions at	Exceptions
●	Disk space	Non-critical disk space has acceptable usage patterns.	Not applicable.	Never	None
●	System fans	All fans are operating normally.	Not applicable.	Never	None
●	CPU	The appliance has not detected any CPU problems.	Not applicable.	Never	None
●	System memory usage	The appliance is consuming an acceptable amount of physical memory.	Not applicable.	Never	None
●	System memory	Appliance system memory is working correctly.	Not applicable.	Never	None
●	System temperature	The appliance is operating within an acceptable temperature range.	Not applicable.	Never	None

Status	Monitor	Message	Potential remedies	Last exceptions at	Exceptions
●	Sophos license	The appliance's license has expired. The appliance will no longer process mail until an updated license is installed. Please contact Sophos immediately.	To avoid any service disruptions, please contact Sophos to discuss license renewal options.	2007/12/14 17:01	None

The ES1000 doesn't come pre-populated with specific lexicons, but industry- or company-specific keyword lists can be uploaded and edited quite easily through the management console.

Also on the compliance side, the ES1000 logs all admin actions and stores a file locally. Should the need arise to review administrator work flow, e.g. to see when a policy was changed, a setting altered or a search performed, the administrator can open an SSH connection to Sophos Support, and a Sophos technician can retrieve the admin log (important note: as is the case with SSH troubleshooting, Sophos cannot access the appliance or see the logs until asked). For security purposes, the admin cannot retrieve the logs without assistance from Sophos. To maintain transparency, all actions taken by the Sophos support technician are logged as well.



IronPort appliances are designed for Internet Service Providers and large corporate users. We found day-to-day management to be overly complicated.

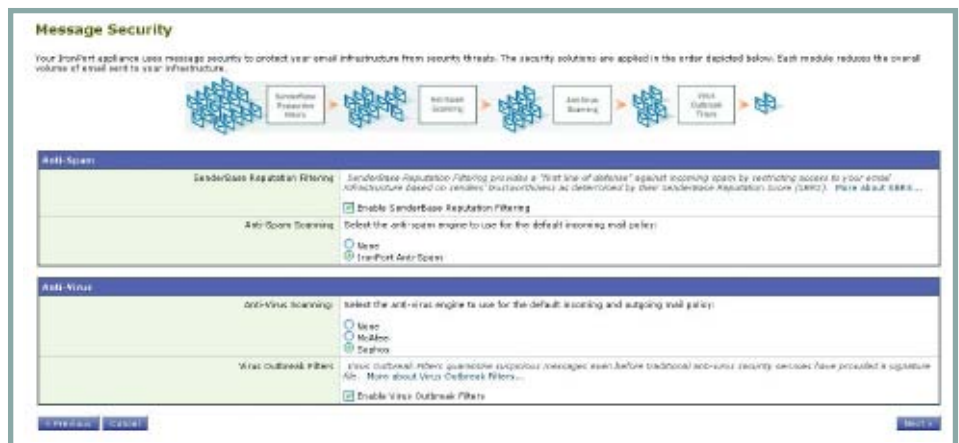
IronPort C150

IronPort is recognized by IDC as a leader in email security, with an estimated market share of 14.3% (IDC Expands Worldwide Security Appliance Tracker to Include Secure Content Management Appliances, July 18, 2007). A popular choice among Internet Service Providers and large corporate users, the company was purchased in June 2007 by networking giant, Cisco. In the C150, IronPort has delivered a powerful, feature-rich device based on its larger appliances. While the C150 is not as elegant or as easy to use as the Sophos ES1000, it did offer some breadth in its feature set that some administrators might like. However, keeping the needs of an SMB in mind, we found that most of these options overly complicated both the configuration and the day-to-day management of the device.

INSTALLATION AND DEPLOYMENT

Initial setup for the C150 was straightforward, but configuring the appliance for our test bench was a bit more cumbersome and less intuitive than the Sophos to setup. Administrators must use both the Web-based interface and the command line interface to configure the C150. The setup wizard only covers the basics, and we quickly had to refer to the Advanced Users Guide for assistance. Here is where the device lost some points for ease of use. While the manuals were detailed, hunting for specific information was difficult and time consuming. Once back to the interface, we noted that system warnings communicate well with administrators as they make changes, and confirmations are logical and clearly communicated when offered. The hierarchical organization of the options and menus in the Web-based interface is consistent and intuitive. One feature we liked was the summary information upon login that included general health of the system as well as some summary statistics. Overall, however, the deployment process was not as smooth or simple as it was with the Sophos ES1000.

IronPort C150 Message Security

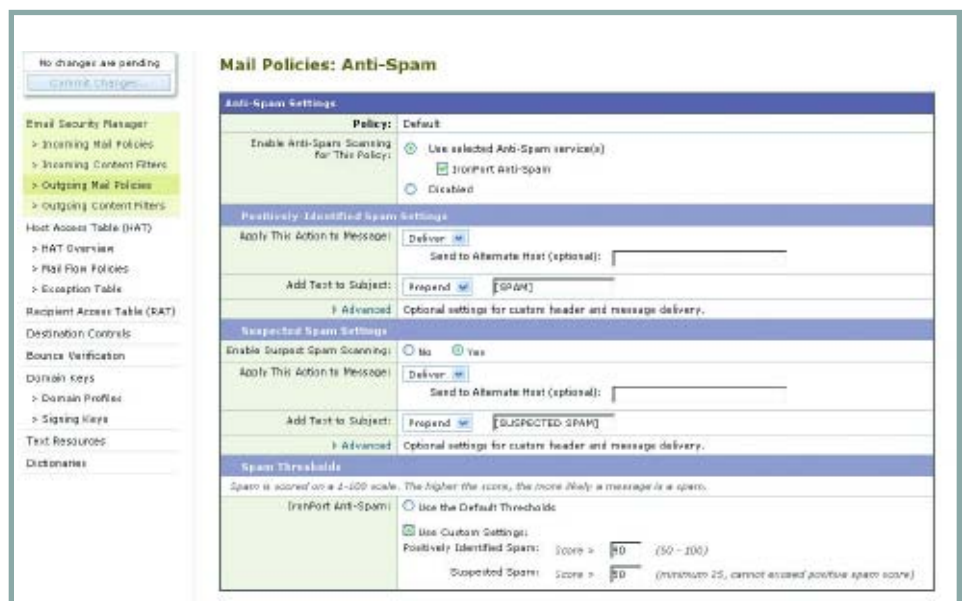


We believe that the C150's lower catch rate is due in large part to its limited range of anti-spam techniques, and to the fact that today's botnet-driven spam campaigns are increasingly difficult to block based solely on the reputation of the sender IP.

USABILITY AND MANAGEMENT

While the IronPort C150 exceeds the minimum spam catch rate requirements we referenced in the Gartner Group report, it fared the poorest of the three devices tested, blocking just 96.9% of spam compared to 99% for the MIMESweeper and 99.4% for the ES1000. The C150 relies heavily on reputation filters to block spam. Reputation filters look at suspect email volume, for example a large number of messages from one IP or a range of IPs, as a possible sign of a spam campaign or virus outbreak. It then cuts back bandwidth or completely blocks the email, depending on how the appliance is configured. We believe that the C150's lower catch rate is due in large part to its limited range of anti-spam techniques, and to the fact that today's botnet-driven spam campaigns are increasingly difficult to block based solely on the reputation of the sender IP.

IronPort C150 anti-spam policy page



Like the other appliances tested, the C150 offers full LDAP integration. It can be managed in a variety of ways including HTTP or HTTPS for the Web interface and SSH or Telnet for the CLI. Communications are encrypted for compliance. Policy creation isn't as straightforward as we had expected. The appliance does have a default policy and additional customized policies can be built, but we found this required considerable effort, particularly when opting for an action other than following the defaults. We would like to see the initial creation screen contain all available settings to simplify this process. Other improvements would be to enable customized reports and the addition of an administrative log. For day-to-day management the IronPort did not score as well as the Sophos, but was a close second.

IronPort does not have its own anti-virus scanning technology. Customers can add the Sophos anti-virus engine to the C150, with one significant protection difference: whereas Sophos customers receive threat updates directly from Sophos every five minutes, IronPort customers cannot. IronPort must first receive the updates from Sophos and then repackage them for distribution to their customers.



REPORTING AND COMPLIANCE

The IronPort C150 scored slightly better in reporting and compliance than the ES1000, due to greater flexibility in policy customization and report scheduling. For example, if an administrator so chooses they can elect to send pre-built reports to multiple recipients at different scheduled times. However they can't customize those reports. While not as robust as the MIMESweeper for reporting, the IronPort did provide a nice suite of information for administrators to begin tracking outbound communications for compliance.



The MIMESweeper scored well in security, reporting and compliance, but did not fair as well as its competitors in the other areas, and therefore finished third in our scoring.

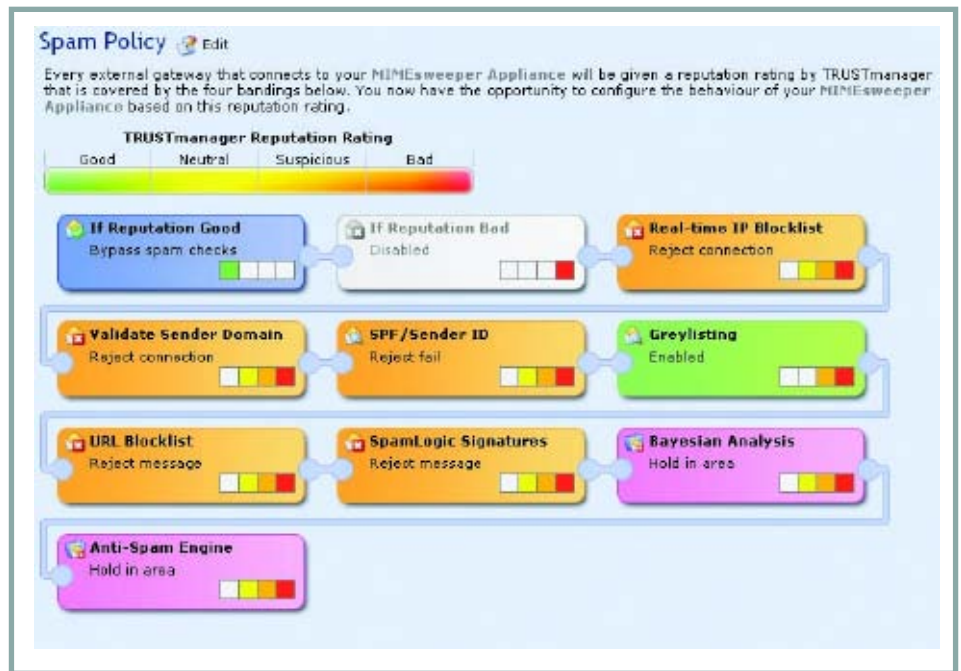
Clearswift MIMESweeper

Clearswift is an established security vendor based in the UK, with good market presence there and in Europe despite being not too well known in North America. Originally a software vendor, Clearswift introduced an appliance-based version of its MIMESweeper solution in late 2005. According to the company, the hardened Linux core in the appliance supports up to 2,500 users. It scored well in security, reporting and compliance, but did not fair as well as its competitors in the other areas, and therefore finished third in our scoring.

INSTALLATION AND DEPLOYMENT

Initial setup was achieved via a wizard that operated as advertised, allowing us to gain access to the Web-based management console within minutes. However, the wizard is for very basic parameters only, and does not include any ability to configure policies. Complete configuration and deployment followed a more manual and time-consuming process.

Clearswift MIMESweeper anti-spam policy page



The MIMESweeper has an abundance of configuration options, more than either of the other two appliances tested.

Clearswift MIMESweeper message policy page



USABILITY AND MANAGEMENT

The MIMESweeper is clearly designed to focus more on content filtering than on security. The company says their default settings are pre-configured and set to block viruses. However, the unit we received for some reason was not doing so out of the box. It was not until we got into the testing phase that we realized the setting was not on and the device was not blocking our test viruses. Once we corrected this issue, blocking was initiated.

The MIMESweeper has an abundance of configuration options, more than either of the other two appliances tested. However, along with these choices comes the requisite configuration complication. Not as intuitive as the Sophos and more convoluted than the IronPort, the MIMESweeper actually proved to be cumbersome to manage on a day-to-day basis. Setting up policies proved to be far more complex than the process on the other appliances. We consistently found ourselves running through multiple screens and configurations to Edit, Change, Edit and Apply before finally being able to commit changes to the policy. The process of confirming settings and reviewing policies was more complicated than it needs to be, resulting in a lack of confidence that the appliance was set up properly. We would like to see a Summary screen to review and confirm every policy that would drill down to a required detailed review from within the policy if we wanted to review and verify.

In keeping with its strengths in filtering, Clearswift recently added a feature called "lexical search" which enables extensive searching through emails and attachments for specific words, phrases and expressions. Boolean operators, regular expressions, and contextual awareness operators (before, after, with, etc.) can all be combined into tightly tailored scanning algorithms. After almost forty-five minutes of experimenting, we began to get the general feel of how to operate the device, although we'd like to see a more intuitive process.



Clearswift's SpamLogic™ technology, coupled with its TRUSTmanager reputation service that helps avoid delays to legitimate email, scored very closely to the Sophos ES1000, with only a slight variance in catch rate over the other devices tested. The latest version of TRUSTmanager now returns finer reputation information and policy flexibility: whereas the email appliance previously had the function to either Accept or Reject email, version 2.6 provides additional levels of trust, which streamline messages through the system. The four reputation bands are now Good, Neutral, Suspicious and Bad.

Like IronPort, Clearswift does not have its own anti-virus technology, relying instead on third parties to provide protection. Customers must purchase a separate license from Kaspersky Lab, effectively requiring them to deal with two vendors for the same appliance.

REPORTING AND COMPLIANCE

Reporting and compliance are MIMESweeper's strong suit, and one of its primary differentiators in this test. It comes with 13 pre-built reports with multiple customized sub-categories. Alerting functionality ranked highest in our review, given its ability to schedule, customize, and review every level of the device. The MIMESweeper appliance had the most enterprise-level tools, including advanced logging, SNMP, and alerting. The benefit to larger organizations is obvious, but for small- and mid-sized organizations, these features may not be as useful, as they typically require an investment in additional infrastructure in order to be fully utilized.

eVision IT Labs



**The "Blue Collar" test lab.
Specializing in competitive
product evaluations, technical
documentation, and security
and compliance testing.**

Contact: info@e-vision-it.com

This comparative review, conducted independently by eVisionIT Labs, was sponsored by Sophos. eVisionIT Labs aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab, and gives each company whose products are included the opportunity to participate by providing input on eVisionIT Labs' test plan and feedback on findings.