Technology Audit

Security

Clearswift
MIMEsweeper™ Web Appliance

Written by: Andy Kellett

Date: January 2007

Abstract

The new MIMEsweeper Web Appliance from Clearswift is an integrated, single-source Web filtering solution that has been developed to protect organisations against the threats posed by viruses, spyware, and other forms of Web-sourced malware threats that can be downloaded from or uploaded to the Web during the course of everyday business and private Web interactions. The integrated components of the Clearswift MIMEsweeper Web Appliance bring together an exclusive blend of leading Anti-Virus (AV) – Kaspersky; Anti-Spyware (AS) – Aluria; content inspection and day-zero threat protection – MIMEsweeper; and a leading URL content filtering solution, within the confines of a hardened, Linux security appliance. Utilising a common, Graphical User Interface (GUI) look-and-feel, each component of the MIMEsweeper Web Appliance has its service delivery role regulated and controlled by the solution's centrally-managed policy generation engine, that enables security managers to build and create security policies that fit the security needs of the organisation. Today, Web-driven attacks against business systems are predominantly controlled by highly-motivated criminal sources, they are well-resourced and their activities are underwritten by a need to make money from the most open and readily available sources. In Butler Groups opinion, what is required from the security community are solutions that remove normal business contact activities from harm and this is the role that has been set for Clearswift's latest Web-based protection appliance.

KEY FINDINGS

Key: ✓ Product Strength ✗ Product Weakness *i* Point of Information

✓	Hardened, Linux-driven, Web filtering security protection appliance.	✓	The solution provides HTTP content, FTP browser, and HTTPS protection.
✓	Integrated Web protection that covers AV, AS, URL filtering, and content inspection services.	✓	A tightly integrated set of protection components driven by a centrally-managed policy engine.
✓	As standard the appliance is delivered on a hardened Linux OS on Dell 1U rack servers.	*i*	AV, AS, and URL content filtering is provided by leading third-party providers.
i	Enterprise scalability will be addressed with a free 1.1 release in Q2 2007.	✗	Multi-box reporting and policy management is not as yet available.

LOOK AHEAD

Clearswift has a specific roadmap development strategy in place for its new MIMEsweeper Web Appliance. During 2007 versions 1.1 (Q2) and 1.2 (Q3) will address enterprise scalability and user-policy management by enhancing the coverage of ThreatLab updates, Lexical Analysis, Multi-box (multi-appliance) policy management and reporting, and associated user-based policy and reporting services for Active Directory AD/LDAP directories.

▶ FUNCTIONALITY

It used to be the case that a large percentage of business and end-user security threats came from sources that could be fairly described as talented amateurs; people who caused irritating and/or malicious damage simply to prove that they could. There was always a worry about corporate information falling into the wrong hands, but generally the drivers were seen as not-for-profit. Today the situation has changed completely. A high percentage of IT security threats are driven by criminal activity, by the need to make money from fraudulently accessing corporate systems, stealing company and financial information, or duping users into releasing systems/account access codes. Therefore, based on the principle that all information has a value, and that all business systems need to be adequately protected to ensure that normal operational activities cannot be disrupted, there is an overriding need to put in place protection and management solutions that deal with the ever-increasing range of threat models that continually present their credentials and attempt to exact systems access. At the same time as security threats against business systems continue to grow more pervasive, it has also become a fundamental imperative of doing business to satisfactorily address the raft of regulatory and compliance issues that impact upon each organisation's accountability for the information that they hold and how it is allowed to be used. The role that has been set by Clearswift for its MIMEsweeper Web Appliance products involves covering and providing protection against all of the above threats as they impact upon Web traffic and Web content security.

Product Analysis

First released at the end of November 2006, Clearswift's MIMEsweeper Web Appliance range of products (CSW250, CSW500, CSW1000, and ENW10) have been developed to provide organisations with an effective solution for dealing with Web content. The key task that has been set for the product is to efficiently manage Hypertext Transfer Protocol (HTTP) gateway perimeter security. This is an access channel that has the potential to deliver a wide ranging set of, extremely difficult to control, security threats. The MIMEsweeper Web Application achieves its protection objectives through its ability to handle virus threats; Spyware iterations (using signature-based detection and prevention, preventing 'call home' spyware activity, and tracking, detecting, and removing cookies); URL filtering; Signature-based file identification and control; File name identification and control; and Recursive decomposition (deals with up to 50 levels of zipped file activity). The same levels of protection are provided when using File Transfer Protocol (FTP) browsers, and in addition the solutions' Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) controls provide 'allow or block' protection on a per machine and per domain basis.

Targeted for use by the average IT administrator; rather than requiring the specific security management skills of IT security experts, Clearswift has designed the MIMEsweeper Web Appliance to have a common look and feel across all of its active security components. The product's administration console provides full systems visibility to all product areas for authorised users, with roles-based administration controls in place to maintain control over who is allowed to undertake activities, such as changing system and network security settings. The system's centrally-administered management controls are complemented and supported by the availability of an extensive and highly-visible range of 'System Health' and the automated reporting capabilities. This Butler Group believes is a key deliverable for the solution as it enables security administrators to have the visibility to confirm performance protection levels, and at the same time have the facilities that are needed to access all security components using a common GUI.

The four core protection components of the MIMEsweeper Web Appliance are:

- **For Content Security** – Clearswift's leading MIMEsweeper content control engine provides full recursive decomposition of Web traffic. This the product combines with a comprehensive range of signature-based Web file recognition facilities. It facilitates deep content inspection and content management levels that enable IT security managers to effectively enforce their organisation's Web access and content control policies.
- **URL Filtering** – using 'the best available URL filtering product on the market today' the Clearswift solution provides high-performance filtering with 40 site categories and is supported by a URL database of over 18 million categorised Web sites. This quality URL filter, although it cannot be publicly named due to licensing agreements, has been rated as a premium Web filter engine that is capable of blocking, reporting, and logging all illicit browsing activity, including specific chat categories and Instant Messaging (IM) blocking.

- **Anti-Spyware (AS)** – Clearswift has chosen to partner with Aluria to provide the solutions spyware protection facilities. Aluria is recognised as one of the most definitively effective gateway spyware solutions available. It provides comprehensive, bi-directional, spyware blocking. This is then aligned with a multi-faceted and layered approach to protection.
- **Anti-Virus (AV)** – AV protection services are provided by Kaspersky. This company's high-speed AV and malware-scanning engine is recognised as a strong, reliable performer, with consistently high virus-detection rates. Kaspersky AV is seen as being particularly competent at dealing with complex malware objects which makes the solution an ideal and complementary AV partner for the Clearswift MIMEsweeper Web Appliance solution.

Dependant upon the network setup of an organisation the MIMEsweeper Web Appliance solution can be operated in standard- or transparent-proxy mode. If standard- proxy mode is being used client browsers will need to be explicitly reconfigured to access the Internet via the MIMEsweeper Web Appliance. In operational use, this means that all Internet requests are serviced by the MIMEsweeper Web Appliance. In transparent-proxy mode, Web traffic is intercepted and redirected to the Web Appliance using a switch facility. In either mode the MIMEsweeper Web Appliance takes responsibility for monitoring all Web traffic entering and leaving an organisation. Its role involves routing, relaying, analysing, and processing Web traffic in line with the organisations content-security policy.

Product Operation

The Clearswift MIMEsweeper Web Appliance has been built to be easy to use for security managers – common, non-technical, GUI – and, unless it identifies user actions that are in breach of an organisation's security policy, it is positioned as being seamless and non-intrusive to end-users and their Web-based processes. This approach Butler Group recognises as being extremely important as the non-intrusive nature of the solution allows users to go about their normal operational activities without being impaired by the security that is in use to protect those activities, but at the same time MIMEsweeper Web Appliance makes a positive security impact and shows its presence when required.

As identified in the Figure 1 architecture diagram, the solution is driven by a Web proxy approach that handles all requests and responses from browser clients when accessing the Internet.

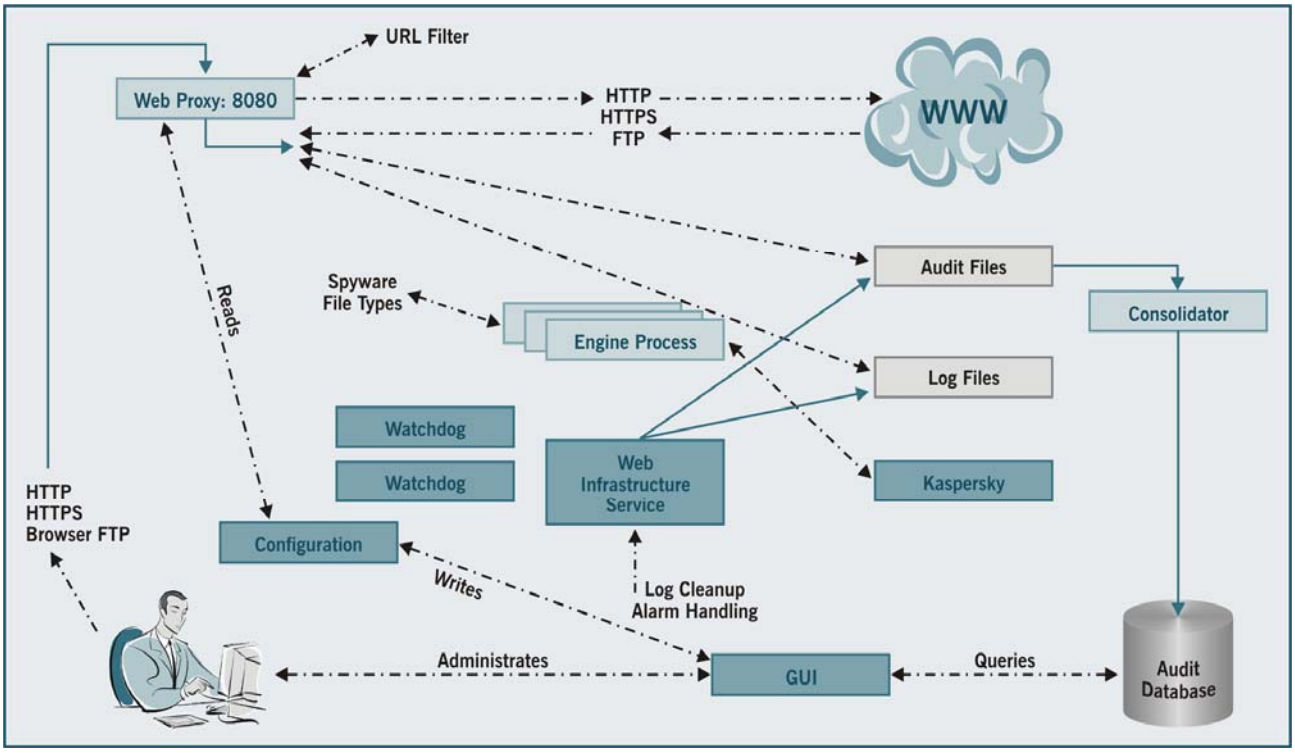

Figure1: The MIMEsweeper Web Appliance Process Infrastructure for Dealing with Web Traffic

In operational use the Web proxy initiates a range of engine processes that security check data before it is allowed to be transmitted in or sent out of the organisation. If, after checking against existing security policy rules, content is blocked, or the user needs to be informed of progress, then the appropriate Web page responses are generated via the proxy and delivered back to the browsing client. For completeness, and in order to ensure that regulatory compliance requirements can be adequately dealt with, all processed transactions are logged in the solution's audit database via the consolidator. Audit database entries are available to be queried using the administration console GUI and from there to produce reports, with all transaction entries being logged in the systems log files in standard World Wide Web Consortium (W3C) format.

The MIMEsweeper Web Appliance System Center takes responsibility for all system management deliverables. It enables security managers to monitor and control the running of the appliance, and the core components consist of:

- View Systems Health – a facility that gathers in real-time data from various parts of the system and provides overview and detailed views of the health of the system.
- Logs and Alarms – accumulates and records log files and alarms that have been generated by the MIMEsweeper Web Appliance.
- Service Control – monitors the status of each service running on the appliance.
- System settings – configures and controls how the appliance is integrated into the corporate network.
- Proxy Settings – manages proxy connection details for the appliance.
- Mail Settings – configures communication details with other existing mail servers.
- Apply My Configuration Changes – applies the configuration new settings and changes to existing settings that affect the live running of the appliance.
- Manage Configuration Settings – identifies changes made to the policy configuration and maintains previous versions so that, where necessary, roll-back to a previous safe version of the system can be achieved.

Finally, the associated User Center facility takes responsibility for user management. It enables user administration functions to be delegated to specific administrators, controls which areas each administrator has access to view, enabling appropriate roles and access controls to be maintained. At this point in time, failover and resilience is achieved by deploying multiple appliances and using a suitable third-party load balancing solution to optimise traffic flows to and from the appliance, and where necessary by directing traffic to another appliance.

Product Emphasis

The Clearswift MIMEsweeper Web Appliance integrates the protection and security facilities of a strong range of leading security solutions. Clearswift's own MIMEsweeper content and day-zero protection technology with its ability to analyse, and where necessary block, an extensive range of file types is combined with security technology from Kaspersky (AV and anti-malware), Aluria (AS), and the facilities of a leading URL content filtering product.

▶ DEPLOYMENT

Clearswift's MIMEsweeper Web Appliance has been designed to facilitate an out-of-the-box plug-and-play approach to product implementation, and as all components of the solution come as a standard active offering, it arrives as a non-modular one-time deployment. In support of this approach, it has been determined that a typical deployment, working in Transparent Proxy mode, will take less than 30 minutes to complete. On arrival each appliance comes with a preloaded set of master security policies/operating rules that are intended to support the basic needs of an average organisation. The implementation skills required to complete the exercise include: basic networking and security management abilities, and the ability to follow a simple-to-use, seven-step deployment guide. For systems administrators and engineers full product training is provided. For systems administration functions this training can be covered using a half-day on-line facility, with one-day classroom-based training available for systems engineers and Systems Integration (SI) partners.

Once deployed, and after the standard security policies have been refined and report requirements agreed to meet the specific needs of the organisation, the product is easy to manage and involves few administrative overheads. The system's administration console provides security managers with full-systems visibility through the use of 'Systems Health' and its associated reporting facilities, and while direct appliance access is required to support roles-based administration activities such as changing system/network integration settings, all operational activities share a universal GUI interface that delivers a common look and feel to all elements of the solution.

Technical support for the MIMEsweeper Web Appliance is provided as a standard component of Clearswift's year-one licensing agreement (including ClearSupport), and going forward is then subject to the customer renewing its annual subscription. Hardware support for the appliance is automatically provided for three years and can be upgraded from the standard Bronze level on the CSW appliance range to Silver, and for the ENW range up to Gold. Technical support is available using telephone, Web, and where necessary on-site engineering support. In addition, 24x7x365 ClearSupport is available as an additional support option – ClearSupport is a comprehensive support package that has been designed to protect the value of Clearswift product investments. It includes all standard support features and then builds in an additional range of premium support services.

The Clearswift MIMEsweeper Web Appliance is provided as a hardened Linux OS on a range of Dell 1U rack mounted servers, there are currently four models available:

- CSW250 for up to 250 users.
- CSW500 for up to 500 users.
- CSW1000 for up to 1000 users
- ENW10 has a flexible usage base and is designed to support up to 3,000 users.

For the CSW range, each appliance has been designed to support the specified number of users on a single unit. If additional failover protection is required Clearswift offers an additional matching appliance at a significantly discounted cost so that an Active/Active deployment can be made utilising the services of a third-party load balancer. In the case of the ENW10 product, if more than 3,000 users need to be supported additional appliances can also be deployed by making use of third-party load balancing mechanisms. Prices for the CSW appliance range starts at UK£5,900 and goes up to UK£17,900. The ENW10 product has a price tag of UK£31,600 for 2,000 users. These prices include year 1 support.

▶ PRODUCT STRATEGY

Clearswift has started out with an open-market strategy for its new MIMEsweeper Web Appliance. The company believes that there are no particular vertical or horizontal restrictions on where the product can be used. Clearswift positions the solution as having the potential to be of value to all enterprise-level and SMB organisations that are looking to address dual-directional Web gateway security; organisations with regulatory and compliance requirements that need to be addressed; and those organisations that have a need to control and enforce Web content policies. In terms of company and user sizing, using single and multiple MIMEsweeper Web Appliance CSW and ENW deployments, enables Clearswift to support user communities of between 150 and 30,000 users.

Return On Investment (ROI) can be measured from savings made in operational support time and administrative costs. In addition, there are the efficiency and security protection issues that are improved through the protection provided by the solution against key forms of malware and spyware, and from reduced help desk overheads. Additional ROI gains can be made through the use of the products URL browsing controls that can be used to control inappropriate Web browsing and to deal with associated legal and compliance issues.

The product will be brought to market using reseller and distribution channel partners, whilst continuing to utilise Clearswift's own direct and telesales resources to support the service. Key business partnerships that support this product include:

- Computerlinks (US, UK, and Ireland).
- Altech (US).
- Commtech (Ireland).

- Cosyco (Benelux).
- Bell Micro (UK).
- Inter Engineering (Greece).
- IT2Trust (Nordic region).
- Networks Unlimited (South Africa).
- Norsoft (Nordic region).
- Noxs (France).
- Renaissance (Israel).
- Infonet (Turkey).

In addition, in the UK, the company also has a large number of reseller agreements with key organisations including SI vendors such as Computacenter and Integralis.

The Clearswift range of MIMEsweeper Web Appliances is licensed on a user-banding basis. For the three appliances that make up the CSW range, user bands run from 1 to 250; 251 to 500; and 501 to 1,000 users. Single and then multiple deployments of the ENW appliance currently take the user range for the product up to 30,000. In the purchase price all year-one costs (including support and maintenance) are included. Renewals costs after year one and going forward represent around 64% of the year-one costs for CSW appliances and 54% in the case of ENW deployments.

As the product is at the first release stage the company has no direct records on which to project average deployment costs. However, Clearswift expects that a typical 500-user deployment will come in at around UK£9,000, a 1,000-user deployment is expected to cost UK£17,000, and a 3,000-user deployment will cost around UK£44,000.

▶ COMPANY PROFILE

Clearswift is a privately owned IT security organisation that has been in business for more than twenty years. It offers a comprehensive range of policy-based content security solutions that cover the three key technology formats of: software-driven solutions, appliance-based offerings, and managed security services. The company, which has its Corporate Head Office in the UK in Reading, also has US headquarters in Redwood City, California, with further US offices in New York and Washington State. Other regional offices are located in Hamburg, Germany; Madrid, Spain; Tokyo, Japan; and Sydney, Australia.

During its twenty-plus year history Clearswift has supplied security solutions to many of the world's leading business organisations and today has a customer-base in excess of 17,000 organisations. Although the Clearswift MIMEsweeper Web Appliance is new-to-market, and only currently, has received BETA site exposure (limited to seven customer sites using one signed-up distributor). The company currently employs just over 200 staff in support of its overall operations and these are split between Research and Development – 27.1%; Sales and Marketing – 39.8%; Support Services – 17.5%; and Administration – 15.6%.

▶ SUMMARY

Without doubt, Clearswift with its new-to-market MIMEsweeper Web Appliance has put together a strong package of security solutions that are capable of dealing with the vast range of threats and information management vulnerabilities that conspire to work against organisations that do business or pass information over the Web. However, in Butler Group's opinion, what differentiates the MIMEsweeper Web Appliance product from its security-content-inspection competitors is the quality of the respective individual protection components. But, that notwithstanding, the real value to business comes from the product's overall ability to integrate and combine the layered threat protection capabilities of the overall solution alongside an inclusive Systems Health and threat-reporting package, that not only delivers protection but also properly informs all users on performance levels.

Contact Details

Clearswift Limited UK (International Headquarters)
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
UK

Tel: +44 (0)118 903 8903
Fax: +44 (0)118 903 9000

E-mail: info@clearswift.com

www.clearswift.com

Clearswift Corporation US Headquarters
100 Marine Parkway
Suite 550
Redwood City
CA 94065
USA

Tel: +1 800 982 6109
Fax: +1 888-888-6884

E-mail: info@us.clearswift.com

www.clearswift.com

Butler Group
a Datamonitor Company

Headquarters:

Europa House,
184 Ferensway,
Hull, East Yorkshire,
HU1 3UT, UK

Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Australian Sales Office:

Butler Direct Pty Ltd.,
Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000, Australia

Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

End-user Sales Office (USA):

Butler Group,
245 Fifth Avenue, 4th Floor,
New York, NY 10016,
USA

Tel: +1 212 652 5302
Fax: +1 212 202 4684

For more information on Butler Group's Subscription Services please contact one of the local offices above.