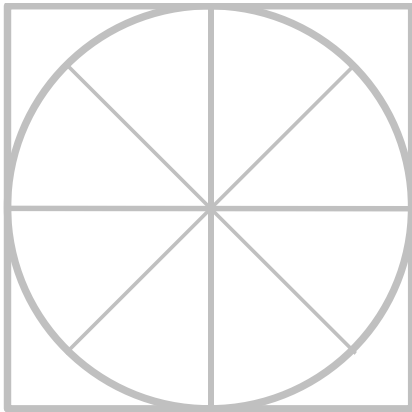




The Radicati Group, Inc.
1900 Embarcadero Road, Ste. 206
Palo Alto, CA 94303
Phone: (650) 322-8059
Fax: (650) 322-8061
www.radicati.com

THE RADICATI GROUP, INC.

Corporate Web Security - Market Quadrant 2011



*An Analysis of the Market for
Corporate Web Security Solutions,
Revealing Top Players, Mature Players,
Specialists and Trail Blazers.*

April 2011

* Radicati Market QuadrantSM is copyrighted April 2011 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market QuadrantsSM should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market QuadrantsSM are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED	3
MARKET SEGMENTATION – CORPORATE WEB SECURITY	5
EVALUATION CRITERIA	7
MARKET QUADRANT – CORPORATE WEB SECURITY	9
KEY MARKET QUADRANT TRENDS.....	10
CORPORATE WEB SECURITY - VENDOR ANALYSIS	13
TOP PLAYERS.....	13
TRAIL BLAZERS	25
SPECIALISTS.....	37
MATURE PLAYERS	45

=====

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.

=====

RADICATI MARKET QUADRANTS EXPLAINED

Radicati Market QuadrantsSM are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market QuadrantsSM are composed of four sections, as shown in the example quadrant (Figure 1).

1. **Specialists** – This group is made up of two types of companies:
 - a. Emerging players that are still very new to the industry and have not yet built up much of an installed base. These companies are still developing their strategy and technology.
 - b. Established vendors that offer a niche product.
2. **Trail Blazers** – These vendors offer cutting edge technology, but have not yet built up a large customer base. With effective marketing and better awareness, these companies hold the power to dethrone the current market leaders. “Trail blazers” often shape the future of technology with their innovations and new products designs.
3. **Top Players** – These are the current leaders of the market, with products that have built up large customer bases. Vendors don’t become “top players” overnight. Most of the companies in this quadrant were first specialists or trail blazers (some were both). As companies reach this stage, they must fight complacency and continue product innovation, or else they’ll be replaced by the next generation of “trail blazers.”
4. **Mature Player** – These vendors have large, mature installed bases of customers, but no longer set the pace for the rest of the industry. These vendors are no longer considered “movers and shakers” like they once were.
 - a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, it may slow development on one product line and start another.

- b. In other cases, a vendor may simply become complacent as a top vendor and be out-developed by hungrier “trail blazers” and other top players.
- c. Companies in this stage either find new life and revive their R&D, moving back into the “top players” segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market QuadrantSM. As a vendor continues to develop its product, it will move horizontally along the “x” axis. As market share changes, vendors move vertically along the “y” axis. It is common for vendors to move between quadrants over the life of a product, as their products improve and market requirements evolve.

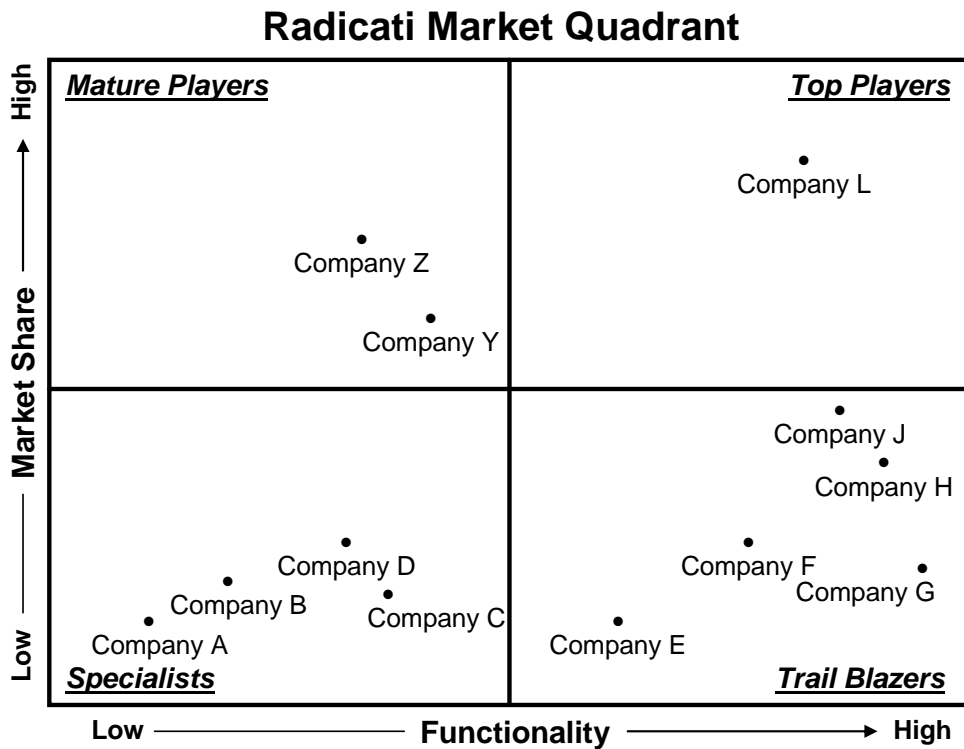


Figure 1: Sample Radicati Market QuadrantSM

- **Functionality** – is rated from 1 to 10, with 10 being the highest, and 1 – the lowest.
- **Market Share** – is assigned according to the company’s ranking in our latest annual reports, based on its user Installed Base (e.g. the company with the largest installed base market share is number 1, the one with the second largest installed base market share is number 2, etc.)

MARKET SEGMENTATION – CORPORATE WEB SECURITY

This edition of Radicati Market QuadrantsSM covers the “**Corporate Web Security**” segment of the Security Market, which is defined as follows:

- **Corporate Web Security:** this segment includes appliances, software, hosted services, and hybrid solutions that help to secure and manage Web traffic for corporate organizations. Key features of Web security solutions include malware protection, URL filtering, and data loss prevention. Some of the leading players in this market are *Barracuda Networks, Blue Coat Systems, Cisco IronPort, Clearswift, M86 Security, McAfee, SafeNet, Symantec, Trend Micro, Webroot, Websense, Zscaler*, and others.
- Solutions in this market can be deployed in multiple form factors, including software, appliances, hosted and hybrid models.
- While some product solutions included in this market target both, corporate customers and service providers, this report only looks at vendor installed base and revenue market share in the context of their corporate business.
- We do not include as part of this definition security solutions that protect Website servers and Web application servers. We also do not include desktop-based security solutions.
- The worldwide revenue for corporate Web security solutions is expected to grow from over \$1.3 billion in 2011, to over \$2.3 billion in 2015.

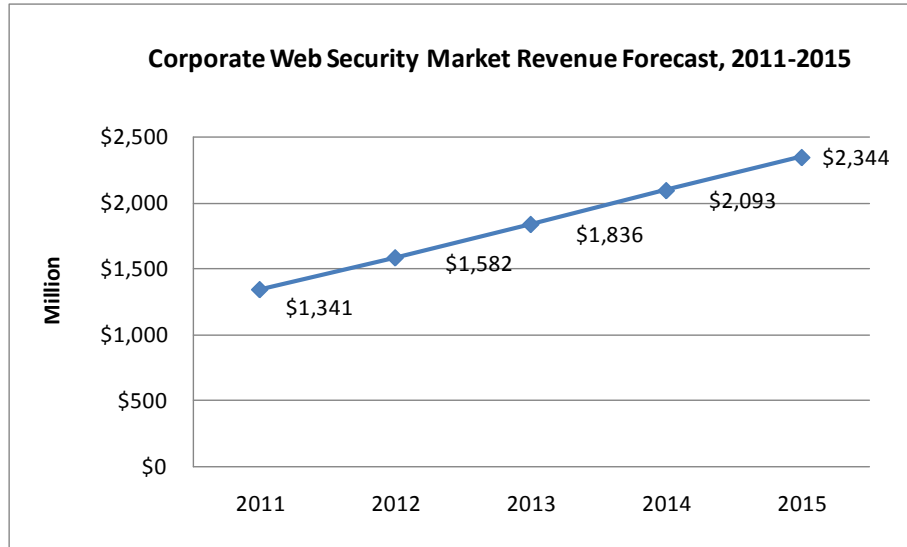


Figure 2: Corporate Web Security Market Revenue Forecast, 2011 – 2015

EVALUATION CRITERIA

Vendors are positioned in the quadrant, according to two criteria: Market Share, and Functionality.

Market Share – is based on the projected installed base published in our “Corporate Web Security Market, 2011-2015” report. The vendor with the largest projected installed base has a market share of 1, the one with the second largest projected installed base has a market share of 2, etc. Vendors with larger market shares are positioned either in Top Player or Mature quadrants. Vendors with smaller market shares, are positioned either in the Trail Blazer, or Specialist quadrants.

Functionality – we assess each vendor’s solution based on a number of key features that they offer out of the box. These capabilities do not necessarily have to be the vendor’s own original technology, but they should be pre-integrated and available for deployment when the solution is purchased.

In order for a Web Security vendor to be on the right side of the quadrant (*Top Player* or *Trail Blazer*), their solution should have the following capabilities:

- **Malware Protection** – protection against viruses, spyware, botnets, and other threats. The typical set up includes two or three popular signature based engines, combined with the vendor’s proprietary filter.
- **URL Filtering** – enables organizations to manage and control the types of websites their employees are allowed to visit, and their activities on those websites (i.e. application deployment, file downloads, etc.) Organizations can block particular websites, or select from a category of websites that have already been pre-screened by a Web security vendor.
- **Application Control** – enable organizations to automatically block potentially malicious applications, and/or limit the use of non-work related applications (i.e. video, music, chat, etc.).

- ***Social Media Web Site Management*** – enables organizations to control employees' behavior on dynamic social media sites, specifying what applications/pages employees can see and access, and how they can interact with other users.
- ***Data Loss Prevention*** – allows organizations to define policies to prevent loss of sensitive electronic information.
- ***Centralized Reporting and Management of Policies and Incidents*** – the solution should enable authorized users to monitor and manage all incidents, as well as create and distribute user management policies centrally.

Additional capabilities/features taken into consideration include:

- ***Integration with E-mail Security Solution*** – to enable organizations to manage both e-mail and Web security solutions centrally.
- ***Protection from Blended Attacks*** – enable blocking of malicious websites that users are directed to via a link included in an e-mail message, rather than via bookmarks, search engines, or going through other web sites.
- ***Encrypted Traffic Management*** – enable organizations to control data travelling over SSL channels to prevent data loss, as well as stop malicious traffic.
- ***Ability to Deploy the Solution in Multiple Form Factors*** – the ability to deploy Web Security as appliances, software, hosted services, or hybrid solutions.
- ***Other Unique Features and Capabilities.***

MARKET QUADRANT – CORPORATE WEB SECURITY

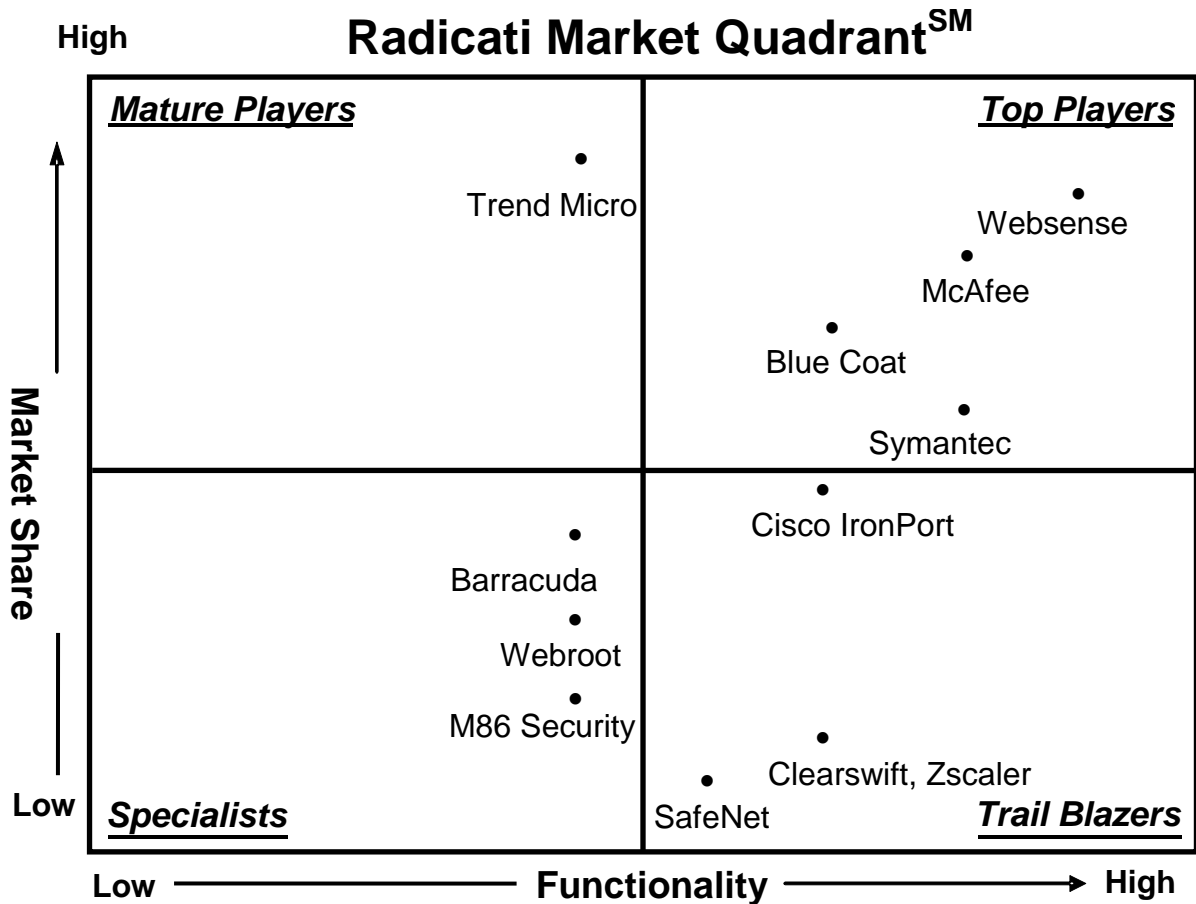


Figure 3: Corporate Web Security Market Quadrant, 2011

* Radicati Market QuadrantSM is copyrighted April 2011 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market QuadrantsSM should not be considered an endorsement, but rather a measure of The Radicati Group’s opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market QuadrantsSM are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT TRENDS

- The **Top Players** in the market are *Websense, McAfee, Blue Coat, and Symantec.*
 - **Websense** has been at the forefront of the Web security market for a number of years. The company dominates the higher end of the market, constantly introducing new concepts and solutions. Its full suite of Web security solutions includes anti-malware protection, URL filtering, application control, DLP, and reporting capabilities.
 - **McAfee** has been building its Web security business over the past few years, acquiring two Web security vendors – Secure Computing and MX Logic to enhance its Web security suite. Having a large e-mail security base to sell to, it quickly rose to the top of the Web security market, selling Web security capabilities on top of its existing e-mail security solutions. Today, the suite offers all the required Web security “ingredients” - strong malware protection (using traditional signature filters combined with reputation filters to protect from zero hour threats), URL filtering, and DLP.
 - **Blue Coat** focuses on high-performance solutions, and caters mostly to large organizations, with users often exceeding 100,000. Its leadership in the Web acceleration and URL filtering space has given it a commanding lead in terms of installed base and also helps position the company as a leader in the Web security space.
 - **Symantec** was a late entrant to the Web security market, however, over the past three years it has managed to quickly expand its market share, and today it successfully competes with the top Web security players. Symantec’s solutions cover all important aspects of Web security – malware protection, URL filtering, application control and DLP.

- The **Trail Blazers** quadrant includes *Cisco IronPort*, *Clearswift*, *Zscaler*, and *SafeNet*.
 - **Cisco IronPort** is a known name in the Web security space. Its original Web security technology came with the acquisition of IronPort in 2007, and later its line of Web security appliances was expanded with the acquisition of ScanSafe hosted services in 2009. Cisco IronPort's Web security solutions offer malware protection, URL filtering, and DLP capabilities. Over the past 12 months Cisco also introduced a hybrid offering, combining appliances and hosted services for large organizations that are looking for an extra layer of protection.
 - **Clearswift** addresses all corporate Web security needs, including malware protection, URL filtering, and DLP. Clearswift Web Gateway's strongest capability is its URL filtering engine. It offers a large number of customizable features for organizations to choose from to tailor the solution to their needs.
 - **Zscaler** is a new kid on the block, having offered the Web security service for less than three years. However, despite this short period of time, its suite is in line with the top Web security vendor's offerings. The suite provides all features that high-end customers are looking for - anti-malware protection, URL filtering, application control, DLP, and reporting capabilities.
 - **SafeNet's** eSafe Web Security Gateway offers a full-featured suite of Web security solutions, ranging from malware protection and URL filtering to DLP.

- The **Specialists** quadrant includes *Barracuda*, *M86 Security*, and *Webroot*. All of these players offer interesting features at an attractive price point, however, they do not offer sufficiently innovative features to be considered a Trail Blazer and also do not yet have a large enough installed base to place in the Top Player quadrant.

- **Barracuda** is one of the earlier Web security vendors with an established customer base in both Web and e-mail security markets. It offers incoming and outgoing data protection, providing anti-malware, URL filtering, and application control capabilities in a single solution.
- **M86 Security** suite provides coverage against e-mail and Web threats. Its Web security solutions cover the whole spectrum of services, including anti-malware, content filtering, DLP, and strong reporting capabilities. In addition, it also provides protection from blended threats, blocking malicious URLs in user e-mails.
- **Webroot** offers Web security on a hosted basis. Offering solutions to organizations of all sizes, Webroot is especially popular among small and mid-size customers due to its ease of use, and affordable pricing. Webroot provides anti-malware protection, URL filtering, and reporting capabilities in a single solution.
- **Trend Micro** is a **Mature Player** in this market.
 - **Trend Micro** is a major player in all aspects of the security market. Its Web Security solutions offer protection against malware, URL filtering, and application control capabilities. However, most capabilities need to be purchased separately for a complete suite.

CORPORATE WEB SECURITY - VENDOR ANALYSIS

TOP PLAYERS

WEBSense, INC.

10240 Sorrento Valley Road
San Diego, CA 92121
www.websense.com

Founded in 1994, Websense offers Web, data, and e-mail content security solutions to organizations of all sizes.

Websense Web security solutions are designed to protect corporate networks from malicious traffic, prevent loss of sensitive data, limit legal liability and help organizations manage user productivity on the Web.

The Web security solutions are available as appliances, cloud services, and hybrid appliance/cloud solutions.

- **Websense Web Security Gateway** offers Web anti-malware, content filtering, and DLP capabilities.

Web Security Gateway protects users against a wide range of malware (from zero hour attacks to blended threats). The solution can block only malicious script/content on a page, rather than the whole page, enabling users to see the rest of the legitimate business content.

The integrated DLP feature enables organizations to specify the type of data/content users are not allowed to post on social media sites or send via Web mail. This enables organizations to protect from sensitive data loss, while still allowing users to conduct business on interactive Web sites.

The content filtering capability enables organizations to manage user behavior on the Internet, blocking inappropriate sites and content to increase productivity and minimize

possible legal liability. This includes inappropriate content within legitimate sites like Facebook, YouTube, blogs, and others.

The Websense Web Security Gateway is available as software, on Websense V-Series appliances, and as a service in the cloud.

- **Websense Web Security** combines productivity, bandwidth and legal liability acceptable use policies with continuously updated malware protection. The Websense ThreatSeeker Network provides Websense Web Security with continuous threat updates (approximately every 5 minutes) to recognize and block access to sites known to be infected with malware, spyware, phishing, and other threats. Websense Web Security can be deployed with on-premise appliances or a cloud service.
- **Websense Web Filter** is a Web filtering tool that allows administrators to manage employee productivity, bandwidth and limit legal liability by setting Web acceptable use policies. Multiple policy actions are supported including Allow, Block, Continue, Quota, Block by Bandwidth, and Block by File Type.
- **Websense V10000** – is a hardware appliance with Web Security Gateway features and capabilities. The appliance also integrates seamlessly with **Websense Hosted Web Security** in hybrid deployments.
- **Websense V5000** – offers the same features as Websense V10000, but for smaller deployments. In addition to Websense Web Security Gateway, the V5000 also supports Websense Web Security.
- **Websense TRITON architecture** – introduced 2010, the TRITON architecture unifies policy management for on-premise and cloud-based deployments spanning Web, Email, and DLP security. The centralized management capabilities enable organizations to define and apply compliance and user management policies to all channels simultaneously. The common anti-malware engine helps protect users against blended attacks distributed via e-mail and Web.

Hybrid deployments of TRITON offer flexible capabilities, allowing combinations of cloud services and on-premises features to be deployed to fit the needs of individual

customers. For example, larger offices may be secured with on-premise appliances while remote offices and users are protected via the cloud.

Websense TRITON is built on a modular architecture, enabling users to add additional services/capabilities as needed.

All of Websense's Web Security solutions can be deployed with a full-featured DLP suite, offering protection of data in motion, data at rest, and data in use.

FUNCTIONALITY: 9

MARKET SHARE: 2

KEY STRENGTHS:

- Websense offers a full suite of Web security solutions, including anti-malware, URL filtering, application management, DLP and reporting capabilities.
- Web security solutions can be deployed as appliances, cloud services, or hybrid solutions.
- A full-featured DLP suite can be integrated with a Web security offering at an extra cost, if needed.
- Granular Web 2.0 controls to enable safe browsing and posting on social media sites.
- Websense TRITON offers a complete Web e-mail, and data security suite that can be deployed in any form factor, including hybrid.

KEY WEAKNESSES:

- Websense offers a full range of Web security capabilities, when deployed as a complete suite the solutions can be fairly expensive, however this is still competitive with assembling independent point solutions.

MCAFEE

3965 Freedom Circle
Santa Clara, CA 95054
www.mcafee.com

McAfee offers a wide variety of security products across many different markets, including e-mail and Web. The foundation for McAfee's current portfolio of security solutions came from two acquisitions - *Secure Computing* (in 2008), a provider of security appliances, and *MX Logic* (in 2009), a provider of hosted security solutions for e-mail and Web.

In 2010 McAfee was acquired by Intel, but it continues to operate as an independent subsidiary.

Appliances:

- **McAfee Web Gateway 7.0** – enables inbound and outbound protection for Web traffic. It includes malware protection (using McAfee anti-virus with McAfee Artemis technology), reputation-based web filtering (leveraging McAfee Global Threat Intelligence reputation service), and SSL scanning technology.

By utilizing proactive, reputation-based filtering, Web Gateway is able to keep up with the latest Web attacks that leverage Web 2.0 technology.

McAfee Web Gateway also comes with basic DLP features, managing the type of content users are allowed to post on the Internet. For deeper content inspection, McAfee Web Gateway can be integrated with McAfee Data Loss Prevention – a full-fledged suite offering protection for data in motion, at rest, and in use.

McAfee Web Gateway is available on physical or virtual appliances, or as a hybrid deployment.

- **McAfee Email and Web Security Appliance** - offers not only anti-virus and anti-spam protection but also compliance, Web filtering, anti-spyware, and more for both e-mail and the Internet.

Services:

- **McAfee SaaS Web Protection** – enables companies to protect all their users, including remote and mobile workers, from inbound and outbound Web threats. The key capabilities include:
 - *Threat Control* – offers protection from viruses, fraud, and Web malware.
 - *Content Control* – enables companies to manage employee Web-related activities. It can block access to potentially dangerous sites, and restrict or limit access to undesirable sites (i.e. networking, entertainment, etc.) It comes with over 100 pre-determined categories of Web sites for organizations to create customizable Web policies for access to undesirable sites.
 - *Total Control* – combines both Threat and Content control at a discounted price.

FUNCTIONALITY: 8

MARKET SHARE: 3

KEY STRENGTHS:

- McAfee's Web security suite of solutions offers malware protection, URL filtering, application control, as well as DLP capabilities.
- McAfee's Web security solutions are offered as appliances, services, and custom-built hybrid solutions.
- McAfee uses a shared reputation network for e-mail and Web solutions, to gain a better real-time insight into malware threats and protect users from blended attacks.
- The offered solutions enable granular monitoring of user Internet behavior, and provide basic protection from loss of sensitive information.

KEY WEAKNESSES:

- McAfee Web Gateway offers strong malware protection, however URL filtering controls are not as granular as those offered by other top vendors.
- McAfee SaaS Web Protection doesn't offer integrated DLP features.
- The Web security features offered as appliances vs. those offered as services in the cloud vary greatly.

SYMANTEC

350 Ellis Street

Mountain View, CA 94043

www.symantec.com

A relative newcomer to the Web Security market, Symantec has quickly grown its customer base to become one of the top players over the past three years. Initially entering the market in 2008 with the acquisition of *MessageLabs*, followed by the acquisition of *Mi5 Networks* in 2009, today it offers Web security solutions as services in the cloud, as well as appliances.

Appliances:

Symantec Web Gateway – offers Web anti-malware capabilities, combined with URL filtering for managing user behavior on the Internet.

For malware protection, Symantec Web Gateway offers six layers of protection (using proprietary and third party filters) with bi-directional scanning, enabling to stop not only incoming threats, but also prevent infected machines from sending out spam and viruses. It uses behavioral analysis to detect botnets and pinpoint compromised endpoints. The malware protection engines are backed up by the Symantec Global Intelligence Network that collects threat data from monitored devices in over 70 countries around the world.

The application control feature enables organizations to define the types of applications that are allowed, and the way they can be used.

Symantec Web Gateway comes with extensive Web reporting and alerting capabilities, enabling administrators to monitor user behavior, as well as network threats in real time.

The gateway is highly efficient at analyzing Web traffic, capable of analyzing a Web page in about 2 milliseconds.

While Symantec Web Gateway comes with basic DLP capabilities (application blocking, etc.) for deep content inspection features organizations will need to deploy Symantec's Data Loss Prevention Suite (or one of its components).

Services:

Symantec MessageLabs Web Security.cloud provides real-time malware protection and URL filtering service.

- *Malware Protection* – uses Symantec’s and third party engines for scanning of web content, blocking viruses and spyware in real time, protecting users from malicious script on websites, as well as downloaded content.
- *URL Filtering* – enables organizations to block user access to undesirable websites, and restrict or block usage of various media files and applications. Organizations can also specify when during the day (and for how long) employees can visit certain websites (i.e. entertainment, social networking, etc.)

For social networking sites administrators can specify what users are allowed to read, access, post, etc.

Web Security.cloud comes with a range of reporting capabilities, enabling administrators to access real-time data on malware threats, network performance, and Web usage statistics. Data is provided in both summary and detailed form in a variety of formats.

Web Security.cloud also offers a choice of solutions for roaming users. Customer can choose from a client side agent that is installed on laptops, which in addition to ensuring traffic is directed at the .cloud infrastructure, also encrypts traffic between the device and the infrastructure. An agentless solution is also offered that allows users to authenticate with the .cloud infrastructure as an alternative.

FUNCTIONALITY: 8

MARKET SHARE: 5

KEY STRENGTHS:

- Symantec offers a full range of Web security capabilities, including malware protection, URL filtering, application control and DLP.

- Web security solutions are offered as appliances and services in the cloud.
- Bi-directional filtering enables Symantec to protect users from incoming, as well as outgoing threats and loss of sensitive information.
- Organizations with remote offices and traveling users can centrally create and enforce policies for users in all locations.
- In addition to Web security, Symantec also offers e-mail protection, and a full-featured DLP suite.

KEY WEAKNESSES:

- The Web security solutions Symantec offers as appliances and services vary significantly in features.
- Advanced Web 2.0 application monitoring tools are currently not available with the appliances.

BLUE COAT

420 N. Mary Avenue
Sunnyvale, CA 94085-4121
www.bluecoat.com

Founded in 1996, Blue Coat's original line of solutions included web content security and anti-malware technologies. Today, Blue Coat has combined its web security products with its application acceleration and application visibility solutions to offer complete enterprise network control through its Application Delivery Network (ADN) solution set.

Blue Coat's ADN solutions cover three areas: Application Visibility, Classification and Performance Monitoring (to detect and fix network problems); WAN optimization (to help accelerate performance of business applications) through its ProxySG appliances and client software; and Secure Web Gateway technologies (to protect organizations against malware, and to help them monitor employees' productivity) through its **WebPulse** real-time web defense with web gateways (**ProxySG, ProxyOne**) and client software for both enterprise and mid-market companies.

In February 2011 the company introduced the **Blue Coat Cloud Service** beginning with the Web Security Module with plans to extend the service with more modules.

Blue Coat's Web security offerings can be deployed as appliances and/or services. The flagship Web Security solutions include appliances and services.

Appliances:

- **ProxySG** is an enterprise grade appliance with a proprietary and secure OS that ensures that everything from simple browsing to complex Web applications runs smoothly and efficiently. It gives administrators the ability to monitor and manage the browsing habits of end users and protect them against web threats with real-time security intelligence from **WebPulse** and inline threat analysis from **ProxyAV** using a choice of leading anti-malware engines.

Remote users are protected by **ProxyClient**, both web gateways and clients have over 80 web filtering categories nested up to four ratings deep, plus real-time web ratings of new content from **WebPulse**. Web application controls and management features ensure that bandwidth is not wasted on non-work related activities.

- **ProxyOne** is the latest appliance, introduced in early 2011. Targeted at small and mid-size customers, a single appliance can be deployed to protect and manage up to 2,000 users. **WebPulse** provides a real-time web defense for ProxyOne, plus on-box features include inline malware protection, URL filtering, control of Web 2.0 applications, and a number of reporting features. ProxyOne also comes with Web and video caching capabilities for network performance optimization, to prevent video feeds from slowing down more important network traffic.

Services:

- **WebPulse** a cloud hosted security intelligence service that unites real-time inputs from over 70 million users from six Blue Coat product solutions to rate new web content, detect web threats and provide controls of web applications by name and operation.
- **Blue Coat Cloud Service / Web Security Module** – is Blue Coat's new Web security service. **WebPulse** provides a real-time web defense and security intelligence for the service, plus cloud hosted inline threat analysis, web filtering and web application controls. Cloud based reporting and management is role-based, multiple connectivity options are provided for office networks or remote users. Designed for organizations of all sizes, Web Security Module can also be deployed together with appliances to create a hybrid solution.

All Blue Coat Web security products and services are updated multiple times per day. Note that WebPulse also collects and provides security intelligence and web ratings for ProxyClient, CacheFlow, PacketShaper and K9 Web Protection solutions.

FUNCTIONALITY: 7

MARKET SHARE: 4

KEY STRENGTHS:

- Blue Coat offers a full-featured suite of Web security solutions, including malware protection, URL filtering, application control, and DLP.
- The Web security solutions can be deployed as appliances, services, and Hybrid offerings.
- The appliances are known for their high performance, aimed at large enterprises.
- Not only HTTP, but also encrypted traffic can be analyzed and managed.
- Multiple updates are provided throughout the day.
- The new ProxyOne appliance is targeted at small and mid-size organizations.
- Blue Coat has over 300 real-time web rating libraries, one of the largest collections available to gateways and clients.

KEY WEAKNESSES:

- Except for ProxyOne, all Web Security capabilities are offered separately, so for complete protection organizations need to deploy multiple solutions.
- Administration options and custom policy development may be complex for new web gateway administrators.

TRAIL BLAZERS

CISCO IRONPORT

950 Elm Ave.

San Bruno, CA94066

www.ironport.com

www.scansafe.com

Founded in 2000, IronPort is one of the leading providers of Web security appliances. The company was acquired by Cisco in 2007, but continues to operate as an independent subsidiary.

In 2009, Cisco also acquired ScanSafe, a SaaS security company, offering Web security and content management solutions in the cloud.

Today, Cisco's Web security solutions can be deployed as appliances, SaaS services, or Hybrid solutions.

All Cisco Web security solutions are powered by Cisco Security Intelligence Operations (SIO) that correlate threat data from web and e-mail security solutions, as well as firewall and IPS appliances deployed in customer networks around the globe. This centralized threat view enables Cisco to update all Cisco security solutions based on correlated threat data.

Appliances:

The **CiscoIronPort S-Series** is a line of Web security appliances that combine comprehensive URL, reputation, and malware filtering, along with granular application controls for popular web applications. The appliances enable organizations to manage incoming and outgoing Web traffic, including encrypted connections.

For malware protection, organizations can choose between *Webroot*, *McAfee*, and *Sophos* engines combined with Cisco IronPort's **SensorBase** reputation network feeds. SensorBase scores the trustworthiness of Web sites in real time using over 200 parameters.

This score is used by S-Series to block URL requests to possible malicious Websites or re-direct for further scanning by the AV engines.

Application visibility and control functionality are now available within the S-Series appliances, enabling users to safely use social media websites and related applications. In addition, safe search functionality for search engines has now been extended for popular media portals like YouTube, Flickr and others, allowing organizations greater control for filtering objectionable content for their users.

The **CiscoIronPort S-Series** comes in three versions: the **S670** for large enterprise deployments (over 10,000 users), **S370** (for mid-size companies with under 10,000 users) and **S160** (for small companies with under 1,000 users). All appliances can be managed and configured centrally.

Services:

The **Web SecurityService** (from the ScanSafe acquisition) offers the following capabilities:

- *Web Security* – protects organizations from Web malware, including viruses, spyware, zero-hour threats, and others. It uses a combination of signature, reputation-based, and proprietary heuristics filters (Outbreak Intelligence service), defending corporate networks from common, as well as brand new threats. Scanning over 7 billion Web requests a day, it analyzes all elements of a Web request, including HTML, JavaScript, Flash, active and obfuscated scripts, and others. This helps it to protect users not only from the typical malicious web sites, but also potentially compromised legitimate sites that otherwise users would have been given access to by using the traditional techniques.
- *Web Filtering* – helps companies control the way employees use the Internet. Policies can be created for individuals and groups of users. Policies can range from the types of sites that can be visited, when they can be visited, and for how long users can stay there. In addition to simple blocking of complete websites, the service can block undesirable content within allowed websites. In addition,

companies can also specify what Web-based applications users can deploy, and what type of content can be downloaded.

- *Secure Mobility* enables consistent security and filtering policy for mobile users and devices through integration with the Cisco AnyConnect Secure Mobility client. A single client can offer consistent security even for off-VPN web communications. The Cisco AnyConnect client can support Windows, Macintosh, iPhone and iPad platforms.

The service comes with extensive reporting capabilities, offering around 100 pre-configured reports, and an unlimited number of custom reports. It can analyze up to 12 months of data, making it available for analysis within 2 minutes of an event.

In addition to Web security appliances and services, Cisco also offers hybrid solutions for large organizations with complex Web security needs that require a combination of on-premise and cloud based functionality.

FUNCTIONALITY: 7

MARKET SHARE: 6

KEY STRENGTHS:

- Cisco IronPort offers a complete suite of Web security solutions, including malware protection, URL filtering, application control, and some DLP capabilities.
- The solutions are offered as appliances, services in the cloud, and Hybrid offerings.
- The solutions are designed for customers of all sizes, including organizations with very large environments.
- The Web security solutions can monitor HTTP and encrypted Web traffic.
- Centralized management of all users and solutions.

KEY WEAKNESSES:

- Basic DLP capabilities are included with the ScanSafe service. Advanced DLP features are offered as a separate partner deployment for an additional fee.
- No comprehensive Web 2.0 tools are offered for the appliances.
- Cisco IronPort appliances are relatively expensive.

CLEARSWIFT

310 Waterside, Arlington Business Park
Theale
Reading
Berkshire, RG7 4SA
UK
www.clearswift.com

Based in the UK, Clearswift offers content-aware e-mail and Web security solutions to organizations around the world. Clearswift's security solutions can be deployed as hardware or virtual appliances.

Clearswift SECURE Web Gateway – offers anti-virus and anti-spyware protection, URL filtering, DLP, as well as extensive reporting capabilities.

The anti-malware protection offers a number of virus scanning engines, including *Kaspersky*. Clearswift offers bi-directional malware protection, enabling to stop not only incoming threats, but also prevent undesirable content from going out, produced by possible botnets and other infected applications.

For content inspection purposes, Clearswift Web Gateway can monitor and block user access to websites according to corporate policies. Organizations can implement schedules when certain types of websites can be visited, and for how long users can access them. The access schedule can be based on groups of users (based on their corporate roles), as well as individual users. Currently, Clearswift offers 77 categories of Websites for organizations to choose from to monitor user behavior.

The appliance's DLP feature offers content inspection capabilities, enabling organizations to create rules specifying the types of documents users are not allowed to upload to various sites, as well as the content that can or can not be posted on the Web.

Clearswift Web Gateway can manage HTTP and encrypted traffic. Clearswift Web Gateway and Clearswift Email Gateway share a common content engine, enabling organizations deploying both to centrally create and apply the same content filtering rules for their users for the e-mail and Web channels.

Clarswift Web Gateway can be deployed as a hardware or virtual appliance.

Some of the latest features added over the past 12 months include the following:

- *On-Box Caching* – to optimize network usage and enable faster access to data.
- *Report Anonymisation* – for some European countries with stringent privacy regulations, such as Germany, this feature enables compliance with regulations by preventing administrators from creating reports focused on individual users, while still offering an insight into the overall traffic statistics.
- *Large File Support* – Cleaswift Web Gateway can now analyze and apply rules to large files (over 4 GB) and treat them according to established policies.
- *Safe Search* – organizations can now prevent users from accessing undesirable content on the Web by only allowing them to browse in Safe Search mode on Google, Yahoo and Bing. This feature is especially important for educational institutions.
- *Transaction log report* – now can be retained for 1 year.

FUNCTIONALITY: 7

MARKET SHARE: 10

KEY STRENGTHS:

- Clearswift's appliances offer one of the best URL/content filtering features on the market, in addition to strong malware protection.
- Clearswift Web Gateway comes with integrated DLP features.
- Clearswift can manage both HTTP and SSL traffic.

- Clearswift Web Gateway can be deployed as a physical or virtual appliance.
- Serving customers all over the world, Clearswift tailors products to different countries by employing local experts who understand the peculiarities of different markets.

KEY WEAKNESSES:

- The solutions offered are mostly high-end, with no option for simpler deployments for customers who only want basic protection.
- Clearswift's focus is URL/user management, while all the malware protection engines are OEMed.

ZSCALER

392 Potrero Avenue,
Sunnyvale, CA 94085
www.zscaler.com

Founded in 2007, Zscaler offers comprehensive, modular e-mail and Web security solutions in the cloud. A newcomer to the Web security market, it has grown quickly over the past three years, attracting attention from organizations of all sizes. In addition, Zscaler launched its cloud based e-mail security solution in 2010 which leverages the existing web security infrastructure, uniquely positioning it as a truly integrated solution. Today, it has over 40 data centers, protecting office and mobile users around the world with a uniform policy.

Zscaler Web Security Cloud – available in five configurations, it offers multi-tenant cloud architecture with 99.99% availability, protecting and managing customer data from over 40 data centers around the world. The service does not require the installation of any hardware, software or agents, greatly simplifying deployment.

The key features include the following:

- *Anti-malware protection* – includes protection against viruses, spyware, botnets, phishing, and other threats. The proprietary *Interrogator Technology* enables protection from zero day threats by using a number of parameters, such as comprehensive sites (obscure, previously blocked site/domain, etc.), host (non-standard ports, previous malicious incidents, self-resolving DNS, etc.) and user analysis. The combined score of the above parameters is used to instantly determine whether a requested URL is suspicious or legitimate, and whether it should be blocked or allowed.

The available *Web 2.0 controls* are designed to enable safer interaction on dynamic content web sites (such as Facebook and others), blocking only malicious components on pages, rather than whole pages and/or websites.

The included *Vulnerability Shielding* feature offers an extra layer of protection by ensuring that the browser of every user is up to date with the latest security patches before the user can access the Web.

In addition to offering its own anti-malware technology, Zscaler also works with best of breed partners, including Google, Verisign, PhishTank, Microsoft, and others.

- *URL Filtering* – Zscaler uses a combination of URL category lists, combined with a dynamic content classification engine to help organizations design comprehensive policies to maximize user productivity and minimize possible liability.
- *DLP* – Zscaler uses lexical analysis, custom phrases, and looks at the document type to identify and stop sensitive content from leaving an organization, based on the established rules.
- *Bandwidth Control* – enables granular policies on web application usage that can be enforced to ensure appropriate bandwidth allocation based on business needs rather than wastage due to leisure web browsing.

In addition to Web, Zscaler also offers services for e-mail protection, with centralized management capabilities for policy creation and user management controls across all protected channels. Furthermore, integrated reports across web and email provide comprehensive visibility across the organization within a single dashboard.

FUNCTIONALITY: 7

MARKET SHARE: 10

KEY STRENGTHS:

- Zscaler offers a full suite of Web security features, including malware protection, URL filtering, application control, DLP, and reporting.
- Zscaler offers Web 2.0 controls for safer social media sites browsing.

- Vulnerability Shielding offers an extra layer of protection by making sure that all browsers are up to date with the latest patches.
- Basic DLP protection is included.
- The bandwidth preservation feature enables organizations to free up their networks for the important traffic.

KEY WEAKNESSES:

- While Zscaler does offer a full suite of Web security solutions, the service is so brand new that it needs time to build up enough of a customer base that can fully test the reliability of its offering.

SAFENET (ALADDIN)

15 Beit Oved St.

Tel Aviv, 61110, Israel

www.safenet-inc.com

Founded in 1983, SafeNet is an information security company, offering solutions in over 100 countries around the world. Its Web security technology came from the 2009 acquisition of Aladdin Knowledge Systems, an enterprise security and Digital Rights Management solutions vendor.

SafeNet is owned by Vector Capital.

eSafe Web Security Gateway offers real-time malware and content filtering protection. It comes with a number of modules that can be mixed and matched for a tailored solution.

The key modules include:

- **Security** - provides real-time anti-malware protection, using eSafe's deep content inspection engine to protect against zero hour threats, combined with Kaspersky's signature-based engine.
- **Application and Web 2.0 Control** – enables organizations to limit or block the use of malicious, inappropriate or undesirable 2.0 applications, including malware and spyware, P2P file sharing, IM chat and file transfers, unauthorized protocol tunneling, etc.
- **Data Leak Prevention** – prevents sensitive data from leaving an organization by using lexical and file type analysis. The policies can be designed for groups of users, as well as individual users.
- **Content Filtering** – prevents employees' access to malicious, infected websites, as well as limits or blocks access to non-work related sites. Organizations can customize Web browsing policies for their users by selecting from a list of over 150 million categorized web sites, updated multiple times a day.

- **SSL Inspection** – inspects all SSL encrypted traffic to prevent malicious content from entering an organization’s network.
- **Anti-spam and Anti-Phishing** – offers a 99% spam detection rate.
- **Management and Reporting** – offers centralized management of all eSafe modules using an interactive, Web-based dashboard.

FUNCTIONALITY: 6

MARKET SHARE: 11

KEY STRENGTHS:

- eSafe Web Security Gateway offers a full-featured suite of Web security solutions, ranging from malware protection and URL filtering to DLP.
- The SSL traffic inspection module is able to analyze encrypted traffic, to prevent malicious content from getting through.
- The Application and Web 2.0 Control module enables organizations to control the type of applications users deploy to block malicious, as well as inappropriate or undesirable traffic.

KEY WEAKNESSES:

- All the modules of the eSafe Web Security Gateway are sold separately, often resulting in a higher cost of the total suite, compared to other solutions with similar capabilities sold as a bundle.
- Since the acquisition of Aladdin in 2009, SafeNet has been keeping a low industry profile, and is rarely seen competing for Web security business against other top vendors.

SPECIALISTS

BARRACUDA

3175 S. Winchester Blvd.
Campbell, CA 95008
www.barracudanetworks.com

Founded in 2003, Barracuda Networks is a leading provider of appliance-based network security solutions. Headquartered in the US, the company has a worldwide presence with sales and support offices in 10 countries, including Australia, Canada, China, Japan, Taiwan, and the UK.

In 2009, Barracuda Networks acquired SaaS Web security provider Purewire, adding cloud-based Web security capabilities to its suite. Today, Barracuda's Web security solutions can be deployed as appliances, hosted services, as well as Hybrid solutions.

Appliances:

Barracuda Web Filter is a plug and play appliance that offers malware protection, content filtering, and undesirable application blocking.

In addition to protecting users from infected web content in real time, Barracuda Web Filter can also detect, block and clean spyware from infected PCs.

Barracuda Web Filter offers flexible URL filtering options, enabling organizations to select from a number of actions, ranging from straight blocking to warning users about potential dangers and/or internal policy violations, associated with certain sites. Barracuda Web Filter can enable management of over 100 popular web applications.

Web browsing policies can be applied to all users, groups of users, or individual users. The access to various Web sites can also be regulated with customizable time and bandwidth quotas per user.

The latest version also offers a local caching feature for performance optimization and bandwidth preservation.

The integrated reporting engine offers over 45 pre-defined reports that can be used to analyze data for the past 6 months.

Barracuda Web Filter monitors and manages both inbound and outbound traffic.

The Barracuda Web Filter is backed by Barracuda Central, the 24/7 security center to monitor and block the latest Internet threats. Data collected at Barracuda Central is analyzed and used to create the latest signatures against spyware and viruses as well as Web site categorization updates that are sent automatically via Energize Updates to the Barracuda Web Filter and the rest of Barracuda Networks products.

Services:

Barracuda Web Security Flex (formerly Barracuda Purewire Web Security Service) is a cloud based content filtering and malware protection service with centralized management and reporting capabilities.

It also offers application blocking capabilities, enabling organizations to control the types of Web applications users can access and use, including social media, Webmail, and others.

Baracuda Web Security Flex is available for in-house, as well as remote users (by either installing the Barracuda Web Security Agent, a tamper-proof piece of software that can be installed into users' laptops, or via browser proxy configuration changes) and mobile users (via BlackBerry Enterprise Server configurations).

Barracuda's Web security services can be deployed as appliances (physical or virtual), SaaS services, or hybrid solutions. All Barracuda Web security solutions and services can be controlled and configured centrally via **Barracuda Control Center (BCC)**.

FUNCTIONALITY: 5

MARKET SHARE: 7

KEY STRENGTHS:

- Barracuda offers incoming and outgoing data protection, providing anti-malware, URL filtering, and application control capabilities in a single solution.
- Barracuda's Web security solutions can be deployed as appliances, services in the cloud, or hybrid solutions.
- Flexible user management policies enable to not simply block, but also selectively limit access to various non-work related web sites.
- The caching feature helps optimize network performance and preserve bandwidth.
- Both appliances and services are affordable for organizations of all sizes.

KEY WEAKNESSES:

- No DLP capabilities are currently available.
- Limited social media and Web 2.0 management features.

M86 SECURITY

828 West Taft Avenue
Orange, CA 92865-4232
United States
www.m86security.com

M86 is a global provider of e-mail and Web security products. The company was formed through the merger of UK-based Marshal and US-based 8e6 Technologies in November of 2008. Marshal was founded in 1997 in New Zealand. The company was acquired by NetIQ in 2002, and later broke off as a private company in 2005.

M86 Security offers a diverse portfolio of security solutions that range from malware protection to content filtering and compliance for e-mail and Web. Its Web security solutions can be deployed as hardware, virtual appliance, services in the cloud as well as hybrid solutions.

Secure Web Gateway 10.1 – offers real-time protection against malware (using a combination of *McAfee, Sophos, Kaspersky*, and proprietary filters), together with URL filtering to monitor and manage user behavior on the Internet, including when accessing Web 2.0 applications.

The solution can be deployed as a physical or virtual appliance, or a hybrid solution.

M 86 WebMarshal - is a software-based application that offers real-time anti-malware, anti-spam and DLP features, as well as protection from blended attacks. In addition, it provides URL filtering capabilities, to make sure that users comply with corporate policies when accessing the Internet.

M86Web Filtering and Reporting Suite – is an appliance-based solution for URL filtering, application control, outbound content security, spyware and malware protection. It also offers reporting options ranging from regularly-scheduled template reports to forensic, drill-down reporting that can show “user intent” by offering such details as full-length URLs visited.

FUNCTIONALITY: 5

MARKET SHARE: 9

KEY STRENGTHS:

- M86 offers malware protection, URL filtering, and DLP capabilities in a single solution.
- M86's Web security solutions can be deployed as appliances, software, as well as services in the cloud.
- Both incoming and outgoing communications are monitored to stop undesirable, as well as malicious traffic from coming in, or going out.
- Granular social media controls.
- Protection against blended attacks is offered as an add-on.

KEY WEAKNESSES:

- While the overall set of capabilities offered is very comprehensive, for a complete Web security solution organizations need to deploy a number of appliances/services, which increases the final cost and adds to the management complexity.
- M86 has an established customer base all over the world, however the company still has a low profile, and tends to focus mainly on its existing customers, rather than competing for new business.

WEBROOT

385 Interlocken Blvd. Suite 800
Broomfield, CO 80021
www.webroot.com

Founded in 1997, Webroot Software offers cloud-based based Web, Email, Email Archiving, and Endpoint security solutions for organizations of all sizes.

Over the past 12 months, Webroot has completed two acquisitions - Prevx (a cloud-based security service provider) and BrightCloud (a URL content classification and Web site reputation provider).

Webroot Web Security Service - is a cloud security service that protects users against Web malware (spyware, viruses, phishing, etc.), combined with content filtering, DLP, and reporting capabilities.

Spyware protection is provided by Webroot's proprietary anti-spyware engine. Scanning both inbound and outbound traffic, Webroot not only protects users from outside threats, but also makes sure that the infected machines inside organizations don't send out spam/malware. Webroot Web Security can also identify infected machines to enable infection clean up.

The URL filtering feature enables organizations to specify the categories of websites users can access, the amount of time they can spend there, and the types of file they can upload or download. The Web usage policies can be set up for groups of users based on their corporate roles and other parameters, and individual users.

To make the browsing experience user-friendly, the solution color-coordinates results of Web searches, instantly allowing users to see which sites they are allowed to access, which sites are blocked, and which sites can be accessed, but the behavior will be logged and reported.

The reporting capabilities enable organizations to analyze data for the past 12 months, using over 15 different parameters, including top users by various categories, bandwidth used, infected applications, etc.

In addition to protecting user computers and laptops, Webroot Web Security service also offers protection for mobile devices.

The latest version (4.0) added a number of capabilities, some of which include:

- *Updated Reporting Engine* – with real-time, interactive capabilities, reports can be generated using a number of parameters, including bandwidth usage, top categories/sites visited, time spent on sites, malware incidents, and so on.
- *Vulnerability Scanning Updates* – enables administrators to identify vulnerabilities in software and operating systems, detecting over 3,500 types of common spyware infections.
- *Localization* - Webroot Web Security Service now supports Japanese for end users.

The acquisition of BrightCloud also added a new classification engine (with over 260 million classified URLs), and additional reputation analysis technology.

FUNCTIONALITY: 5

MARKET SHARE: 8

KEY STRENGTHS:

- Webroot offers anti-malware, URL filtering, and reporting capabilities in a single solution.
- Both inbound and outbound Web traffic is analyzed and protected.
- Webroot can also scan and clean up existing spyware infections.

- Due to the nature of the service, the created policies can be applied to all users in all locations, including those accessing the system via mobile devices.
- The policy controls are granular for administrators, and user-friendly for employees. Webroot enables analysis of data for up to 12 months.

KEY WEAKNESSES:

- No DLP protection is offered.
- No advanced Web 2.0 sites management is available.

MATURE PLAYERS

TREND MICRO

Shinjuku MAYNDS Tower, 1-1,
Yoyogi 2-Chome, Shibuya-ku
Tokyo, 151-0053, Japan
www.trendmicro.com

Founded in 1988, Trend Micro provides multi-layered network and end-point security solutions for businesses across the globe. Its e-mail and Web-based security solutions are available as software, appliance, and hosted security solutions.

Interscan Web Security Virtual Appliance 5.1 (IWSVA) offers the following key capabilities:

- *Anti-malware* – offers real-time protection against viruses, spyware, bots, keyloggers, drive-by downloads and other malware, including zero hour threats. In addition to the traditional anti-virus and anti-spam engines, it also uses reputation scoring, powered by Trend Micro’s proprietary Smart Protection Network. IWSVA can monitor and manage HTTP, HTTPS, FTP, and IM traffic that tunnels over HTTP.

To prevent infection from malicious mobile code, IWSVA also enables Java and ActiveX code validation and threat detection.

- *URL Filtering* – using dynamically updated information from the cloud, it automatically blocks access to malicious Web sites, as well as enforces corporate policies concerning Web browsing for employees. Policy actions include allow, block, monitor, and warn. If needed, it can also enforce SafeSearch practices for all users.
- *Damage Cleanup Service* – offered as an add-on solution, it enables organizations to quickly clean up damages caused by virus infections (disabling spyware, rootkits, worms, virus remnants and Trojans), as well as automatically repairing system registries and memory.

- Integrates with the *Advanced Reporting and Management* module to offer a centralized policy management, monitoring, and reporting of for multiple IWSVAs.
- Integrates with Trend Micro Control Manager for centralized malware policy and summary reporting when deployed with other endpoint, server, or messaging security solutions from Trend Micro.

TrendMicro Advanced Reporting and Management – an add-on solution for managing multiple IWSVA instances. It can replicate policy and configuration to multiple, independent groups of geographically dispersed IWSVAs. It offers a consolidated real-time insight into the network activity and threats, as well as user actions. With a large number of customizable dashboard options, it can generate over 150 reports on all users, groups of users, as well as individual users and events. It also enables administrators to track real-time behavior of individual problem users, if needed, to prevent future undesirable activity from occurring.

All Web security solutions come with a content caching feature to reduce latency and preserve bandwidth.

FUNCTIONALITY: 5

MARKET SHARE: 1

KEY STRENGTHS:

- Trend Micro’s solutions offer protection against malware, URL filtering, and application control.
- Web security solutions can be deployed as software, appliances, or hosted services.
- Both HTTP and HTTPS traffic can be monitored.

- Java and ActiveX code validation to prevent malicious mobile code from infecting corporate networks.
- Comprehensive, drill-down reports that enable real-time, detailed tracking of individual user actions.

KEY WEAKNESSES:

- A number of capabilities (i.e. URL filtering, comprehensive reporting, damage cleanup, etc.) are offered at an extra cost, adding up to the final price of the solution.
- No comprehensive DLP features are offered.

THE RADICATI GROUP, INC.
<http://www.radicati.com>

The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- **Email**
- **Security**
- **Instant Messaging**
- **Unified Communications**
- **Identity Management**
- **Web Technologies**

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim.

The Radicati Group, Inc. was founded in 1993, and is headquartered in Palo Alto, CA, with offices in London, UK.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Whitepapers
- Strategic Business Planning
- Product Advice
- TCO/ROI Analysis
- Investment Advice
- Multi-Client Studies

*To learn more about our reports and services,
please visit our website at www.radicati.com.*

MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition. Current and upcoming publications include:

Currently Released:

Title	Released	Price*
Social Networking Market, 2011-2015	Mar. 2011	\$3,000.00
Microsoft SharePoint Market Analysis, 2011-2015	Mar. 2011	\$3,000.00
Microsoft Exchange and Outlook Market, 2011-2015	Feb. 2011	\$3,000.00
Google Email and Collaboration Market, 2011-2015	Jan. 2011	\$3,000.00
Inbox Management Solutions Market, 2011-2015	Jan. 2011	\$3,000.00
On-Premises Email and Collaboration Market, 2010-2014	Dec. 2010	\$3,000.00
Data Loss Prevention Market, 2010-2014	Dec. 2010	\$3,000.00
Email Platforms for Service Providers Market, 2010-2014	Nov. 2010	\$3,000.00
Wireless Email Market, 2010-2014	Oct. 2010	\$3,000.00
Instant Messaging Market, 2010-2014	Oct. 2010	\$3,000.00
eDiscovery Market, 2010-2014	Oct. 2010	\$3,000.00
Corporate IT Survey – Messaging & Collaboration, 2010-2011	Aug. 2010	\$3,000.00
Hosted Email Market, 2010-2014	Aug. 2010	\$3,000.00
Email Archiving Market, 2010-2014	July 2010	\$3,000.00
Hosted Unified Communications Market, 2010-2014	July 2010	\$3,000.00
On-Premises Corporate UC Market, 2010-2014	July 2010	\$3,000.00
APAC Hosted Email Market, 2010-2014	June 2010	\$3,000.00

Upcoming Publications:

Title	To Be Released	Price*
IBM Lotus Notes/Domino Market, 2011-2015	Mar. 2011	\$3,000.00
Email Statistics Report, 2011-2015	Apr. 2011	\$3,000.00

* Discounted by \$500 if purchased by credit card.

All Radicati Group reports are available online at <http://www.radicati.com>.

EDITORIAL STAFF

Masha Khmartseva

Senior Analyst

Masha has an extensive background in the Directory Services, Messaging and Identity Management markets. She authors a number of annual studies and is a contributor to the company's monthly newsletter that analyses leading technologies driving the Internet economy. She frequently speaks on topics related to anti-spam, anti-virus, e-mail archiving and directory services.

Prior to joining the Radicati Group, Inc., Masha conducted market research for international companies in the U.S and Europe.

Current areas of research:

- E-mail Archiving
- eDiscovery and DLP
- E-mail and Web Security

Masha received a B.S. with honors in Marketing from Santa Clara University.

Sara Radicati, Ph.D.

President & CEO

Dr. Sara Radicati is a widely recognized industry consultant and analyst expert in Messaging and Collaboration, Directory and Metadirectory Services, PKI/Security, Unified Communications, Wireless and Internet applications. Sara was one of the leading designers of the X.500 standards for directory services, and has played an active role in numerous major international standards organizations. She is a past Director of the European Electronic Messaging Association (EEMA).

Her company, The Radicati Group, Inc., is an international consulting and market research firm with offices in Palo Alto, USA, and London, UK. The company assists corporate clients, vendors and network operators on planning, deployment and business strategies in all areas of messaging, directory services, unified communications, wireless and Internet applications. The company also performs due-diligence and advises investment firms in identifying new opportunities. Dr. Radicati is a widely published author and speaks frequently at industry events worldwide.

Prior to founding The Radicati Group, she held senior technical and business planning positions at Xerox, 3Com and Novell.