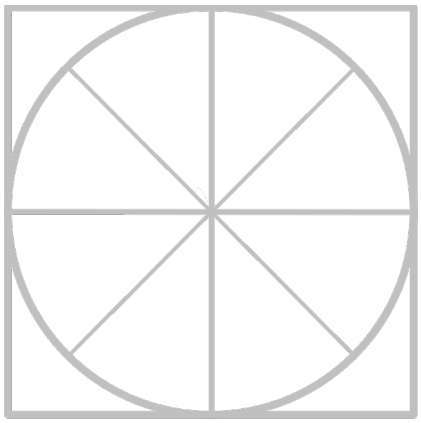
The Radicati Group, Inc.
Palo Alto, CA 94301
www.radicati.com

THE RADICATI GROUP, INC.

Corporate Web Security - Market Quadrant 2010



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

April 2010

TABLE OF CONTENTS

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

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

1. ***Top Players*** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as posses a solid vision for the future. Top Players shape the market with their technology and strategic vision. 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 to innovate.

2. ***Trail Blazers*** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.

    b. Established vendors that offer a niche product.

4. ***Mature Players*** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered "movers and shakers" in this market as 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, they may choose to slow development on existing products.

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product solutions adding features and functionality, it will move vertically along the "y" functionality axis.

The horizontal "x" strategic vision axis reflects a vendor's understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

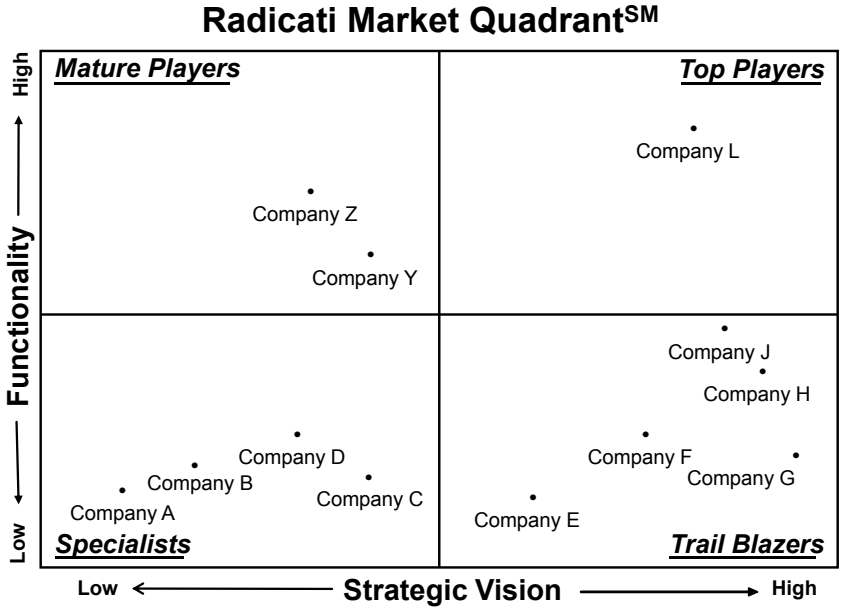


Figure 1: Sample Radicati Market Quadrant

MARKET SEGMENTATION – CORPORATE WEB SECURITY

This edition of Radicati Market Quadrants[SM] covers the "**Corporate Web Security**" segment of the Security Market, which is defined as follows:

- **Corporate Web Security:** is defined as any software, appliance, or hosted service that protects corporate users and networks from Web-based malware, helps prevent data loss, and enables organizations to control employee behavior on the Internet. Key players in this market include *Aladdin*, *Barracuda Networks*, *Blue Coat*, *Cisco IronPort*, *M86 Security, McAfee*, *Symantec, Trend Micro*, *Webroot*, *Websense*, 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 $1.1 billon million in 2010, to over $2.1 billion in 2014.

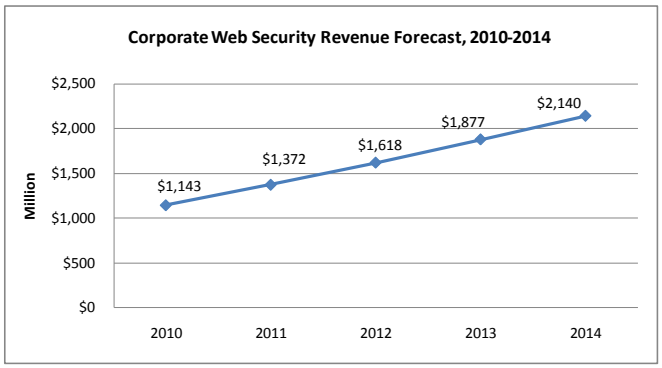


Figure 2: Corporate Web Security Market Revenue Forecast, 2010 – 2014

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the *Web Security* space are evaluated according to the following key features and capabilities:

- ***Malware detection*** is usually based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. Top players and trails blazers will usually go beyond the typical set up that usually includes multiple filters, one or more best-of-breed signature-based engines as well as the vendor's own proprietary technology. Malware can include spyware, viruses, worms, rootkits, and much more.

- ***URL filtering*** is a very common feature in Web security solutions. It helps promote productivity and a malware-free environment by filtering out unwanted websites based on URL. Vendors usually offer a number of different categories that administrators can choose to filter, which can range from around 10 to 100. Categories often include millions of pre-screened sites, which are updated daily. The number of categories that can be screened is irrelevant. The differentiation factors lie in how often they are updated (e.g. hourly vs. daily), what scanning techniques are used (e.g. scanning content on a website vs.URL name), the amount of latency introduced, and other factors.

- ***Reporting*** lets administrators view activity that happens on the network. Most Web security solutions offer interactive reports on detailed user activities. Summary views are available to give an overall view of the state of the network, such as how many threats were blocked. Most solutions offer similar levels of network-level detail. Differences, however, are mostly found in how long the activity becomes available for reporting after the activity takes place. Most solutions offer real-time or near real-time reporting. Reporting is traditionally included in a solution, but some vendors require it as an add-on to the base Web security offering.

- ***SSL scanning*** was not usually offered as a feature in the past since websites with SSL security were viewed as safe and trust-worthy. Now that malware frequently appears on legitimate websites, Web traffic over an SSL connection is also commonly monitored to enforce Web policies. SSL scanning has become a much more common feature in Web security solutions.

- ***Directory integration*** can be obtained via Active Directory or the LDAP protocol. By integrating Web security tools with a corporate directory, organizations can use employees' directory roles to assign and manage Web policies based on a user's function and role in the organization. Nearly all Web security vendors offer some form of directory integration.

The following capabilities are viewed as more advanced in the Web Security market, and further add to a vendor's placement in the right side of the quadrant:

- ***Social networking controls*** are becoming increasingly granular as organizations seek to control the features available on social networking sites, such as blocking access to applications. These types of controls have been some of the most frequently requested new features for Web security solutions.

- ***Data Loss Prevention (DLP)*** allows organizations to define policies to prevent loss of sensitive electronic information. Vendors can claim they offer DLP functionality based on the fact that some of the features that are standard in Web security solutions stop data from leaving the network, such as application blocking. Other vendors take a more vigorous approach and offer keyword blocking and deeper DLP functionality.

- ***Web 2.0 controls*** enable organizations to automatically block potentially malicious applications, and/or limit the use of non-work related applications. Web security vendors can vary greatly with regards to the number of protocols and Web 2.0 applications on which they can enforce policies.

- ***Bandwidth controls*** allow administrators to completely block bandwidth-hungry sites like YouTube, or they can impose quotas that limit time spent or data consumed. This preserves bandwidth for legitimate traffic and application use. Web security vendors can differ quite a bit in the level of bandwidth controls offered. Some may offer controls just based on amount of data consumed or time spent on a site, while others may offer detailed controls that can enact a broad variety of bandwidth policies.

- ***Blended attack prevention*** enables blocking of malicious websites that users are directed to via a link included in an email message. The malicious code is delivered via the link, while the email does not contain any malicious attachments. Sophisticated Web security solutions can detect and block this increasingly common form of attack.

Note*: On occasion, we may put a vendor on the right side of the quadrant (Top Player or Trail Blazer) if we feel that some other aspect(s) of their solution which may not be listed above is particularly unique and innovative.*

MARKET QUADRANT – CORPORATE WEB SECURITY

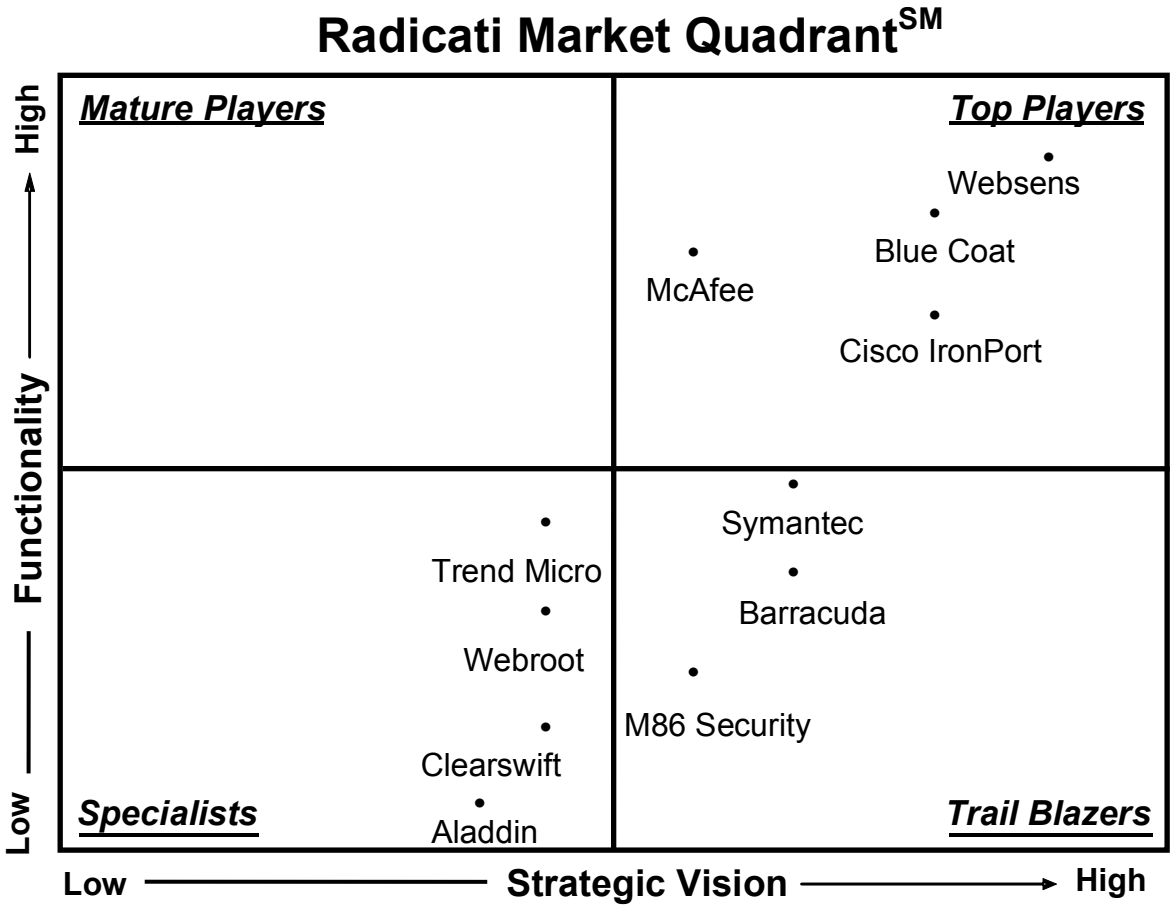


Figure 3: Corporate Web Security Market Quadrant, 2010

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are ***Websense, Blue Coat, McAfee***, and ***Cisco IronPort.***
- The **Trail Blazers** quadrant includes ***Symantec***, ***Barracuda*** and ***M86 Security***.
- The **Specialists** quadrant includes ***Trend Micro***, ***Webroot, Clearswift***, and ***Aladdin***. 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.
- There are currently no **Mature Players** in this market.

CORPORATE WEB SECURITY - VENDOR ANALYSIS

TOP PLAYERS

WEBSENSE, INC.

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

Founded in 1994, Websense provides security solutions to protect corporate Web and e-mail channels, as well as specialized offerings for data security. In 2007 Websense acquired *SurfControl* and *PortAuthority* to enhance its suites with advanced e-mail, Web, and Data Loss Prevention technology.

Websense Web security solutions are designed to protect corporate networks from malicious traffic, prevent loss of sensitive data, and monitor user productivity. In addition, they also enable management of popular Web-based social networks and applications, allowing users to effectively do their job, without compromising corporate security.

Websense offers one of the most comprehensive Web security suites available today. The company dominates the higher end of the market, constantly introducing new concepts and solutions. One of its latest offerings, Websense TRITON (introduced in February 2010), combines all the top features needed for both e-mail and Web protection in a hybrid architecture.

Websense Web Security Gateway (WSG) enables businesses to securely adopt Web 2.0 tools. It uses dynamic categorization capabilities to effectively protect users from potential threats without the need of reputation technology. Rather than blocking the whole website, it can just block the undesirable content within a website. The Web Security Gateway also offers outbound data loss prevention (both native and integrated options with its enterprise data loss prevention solution, the Data Security Suite) and hybrid deployment, combining on-premise and SaaS deployment. The Websense Web Security Gateway is available as software, on the Websense V10000 appliance, and as a service (SaaS).

Websense Web Security protects organizations from Web-based threats, such as spyware, phishing, and more, combined with the Websense Web Filter. The Websense ThreatSeeker Network offers real time analysis to recognize and stop known and unknown threats.

Websense Web Filter is a robust Web filtering tool that allows administrators to set acceptable use policies for the Web, providing multiple settings such as Allow, Block, Continue, Quota, Block by Bandwidth, and Block by File Type.

Websense Express is targeted towards SMBs with environments under 250 users. It enables monitoring of user productivity, and helps to eliminate Web threats.

Websense also offers **Hosted Web Security**, delivering web security technology as a service available integrated with Websense Hosted Email Security.

Websense V10000 – available since 2009, it is a virtualized hardware appliance with Web Security Gateway features and capabilities. The appliance also integrates seamlessly with Websense Hosted Web Security for hybrid deployment.

Websense TRITON – introduced in February 2010, includes unified policy management for on-premise and cloud-based deployments spanning Web, Email, and DLP protection in a unified solution.

Websense is also planning to introduce a new hybrid Web Security solution, which will combine a hosted filter to remove viruses and spam in the cloud, as well as an on-premises solution for outbound traffic control.

STRENGTHS:

- Websense Web security solutions can be deployed as appliances, services, or hybrid solutions.

- Websense offers one of the most comprehensive suites of Web security solutions for companies of all sizes. It covers all aspects of Web security – from employee productivity, to protection from malicious traffic, to data loss prevention.

- Websense is keeping up with emerging Web threats by ensuring that Web 2.0 based sites and applications are used safely. Instead of blocking complete websites and applications, Websense enables companies to block just the undesirable content within these applications.

- The latest Websense TRITON is a hybrid offering combining advanced e-mail and Web protection tools, including DLP features.

WEAKNESSES:

- Large deployments of Websense Web Security Suite can be rather costly.

- Various capabilities have to be purchased separately, rather than as a single solution.

- DLP capabilities are very basic. Although this is typical for Web Security vendors, Websense could be more at the forefront of the market, considering how advanced the rest of its Web security tools are.

BLUE COAT SYSTEMS

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

Founded in 1996, Blue Coat's original line of solutions included technologies to accelerate Internet browsing. Today, Blue Coat has combined its application acceleration and Web security products with its 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 it's ProxySG appliances and client software; and Secure Web Gateway technologies (to protect organizations against malware, and to help them monitor employees' productivity) through its ProxyAV appliance and ProxySG appliances and client software.

Blue Coat's solutions are known for their high-performance and, although Blue Coat sells primarily into large organizations, it is also currently beginning to target mid-size enterprises with its ADN solution set.

Blue Coat offers a comprehensive set of Web security solutions. Offered with five layers of defense, these solutions include: the WebPulse cloud service, ProxyAV (anti-malware protection) and ProxySG appliances (with DLP technology), and real-time remote user protection capabilities through ProxyClient.

The company's flagship ProxySG and ProxyAV solutions have the following capabilities:

ProxySG is an appliance 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 remove web threats.
URL filtering keeps users from visiting inappropriate sites, and application management can ensure that bandwidth is not wasted on non-work related activities. The latest version adds a number of new URL categories, bringing the total number of categories to 80.

ProxySG is continuously updated by the WebPulse community watch cloud service to detect and block malware downloads, phishing attacks, scareware, plus assess reputations and rate web content.

The **ProxyAV** appliance focuses on stopping malware and web threats from reaching the organization. The latest version offers better visibility of the inline traffic analysis (such as SSL webmail, etc).

Both ProxyAV and ProxySG can work with regular, as well as encrypted traffic. Blue Coat updates its solutions multiple times per day.

Over the past 12 months, Blue Coat has also enhanced the available Web reporting capabilities. The latest version of its Reporter (v9), comes with a new interface, customizable dashboards and reports per category and per user. It offers interactive graphs and charts for easier comprehension, and enables users to view reports online, as well as download them to CSV or PDF formats.

Blue Coat is starting to see more interest from its customers in its **Hybrid Web security solutions**, which combine appliances and Web security services.

STRENGTHS:

- Blue Coat's Web security solutions include appliance and services.
- Blue Coat appliances are high-performance solutions, deployed by very large organizations, with some deployments exceeding 100,000 seats.
- The appliances are known for their high performance, aimed at large enterprises.
- Both appliances and services offer protection against malware, as well as enable companies to monitor users' browsing habits.
- Not only HTTP, but also encrypted traffic can be analyzed and managed.
- Multiple updates are provided throughout the day.

- Hybrid architecture is available on a customized basis.

WEAKNESSES:

- Relatively expensive to deploy and manage.
- All capabilities are offered separately, so for complete protection organizations will have to deploy multiple appliances/services.
- DLP tools are rather basic, contrasting with the more advanced features of the rest of the Web security suite.
- Web Security solutions are not the main focus of Blue Coat. The vendor mostly targets its own (although quite large) customer base.

MCAFEE, INC.

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

McAfee is a leader in corporate and consumer security solutions, offering a wide variety of products across many different markets, including e-mail and Web.

In November 2008, McAfee acquired *Secure Computing*, enhancing its line of Web Security offerings with technology from one of the top players in the security appliances market.

In September 2009, McAfee also completed the acquisition of *MX Logic*, a provider of hosted security solutions for e-mail and Web.

Appliances:

- **McAfee Email and Web Security Appliance** - offers not only anti-virus and anti-spam protection (with a claimed 98% spam block rate), but also compliance, Web filtering, anti-spyware, and more for both e-mail and the Internet.

- **McAfee Web Gateway** (from Secure Computing's acquisition) - includes reputation-based web filtering, leveraging Trusted Source (Secure Computing's global reputation service), anti-malware and anti-spyware protection, SSL scanning technology, in-depth reporting, and data leak protection. 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 is available on multiple appliance models, a blade server architecture for the largest of enterprises and will soon be available for VMware environments.

SaaS Solutions:

- **McAfee SaaS Web Protection** – enables companies to protect all their users, including remote workers, from Web-based threats.

To protect against viruses, McAfee SaaS Web Protection utilizes signature-based anti-virus technology from *McAfee* and others. The company also incorporates proprietary worm detection technology to stop new outbreaks that have not been neutralized by a pattern file.

- **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.)

- **Total Control** – combines both Threat and Content control at a discounted price.

STRENGTHS:

- McAfee is able to offer Web security appliances and services (through the acquisition of MX Logic).

- McAfee offers proven anti-virus and anti-malware technology for both e-mail and Web. Its anti-malware solutions are widely used by many third party providers.

- The offered solutions enable granular monitoring of user Internet behavior, and provide basic protection from loss of sensitive information.

- Secure Web appliances can monitor and manage employee interaction with Web 2.0 applications.

WEAKNESSES:

- McAfee is mostly focused on e-mail, rather than Web security, which means that its Web security solutions are viewed mostly as an add-on to their e-mail offerings.

- Due to the Secure Computing acquisition, some of the features offered by the two companies are still complementary, and may be confusing for customers until a more proper integration takes place.

- McAfee SaaS Web Protection does not protect against encrypted traffic threats, and offers no content filtering or DLP capabilities.

CISCO IRONPORT

950 Elm Ave.
San Bruno, CA 94066
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 December 2009, Cisco acquired ScanSafe, a managed security solutions provider, offering Web security and content management solutions on a hosted basis. With the acquisition of ScanSafe, Cisco IronPort can now also offer Web security solutions as services. This is especially significant to its larger customers, many of which are now becoming interested in deploying a hybrid Web security solution, combining on-premises tools and in the cloud services.

Appliances:

The **Cisco IronPort S-Series** is a line of Web security appliances that combine comprehensive URL, reputation, and malware filtering. The appliances enable organizations to manage incoming and outgoing Web traffic, including encrypted connections.

Cisco IronPort's **SensorBase** reputation network scores the trustworthiness of Web sites using over 200 parameters. This score is used by S-Series to block URL requests to possible malicious Web sites or re-direct for further scanning by the AV engines.

For malware protection, IronPort uses integrated *Webroot* and *McAfee* engines to protect users from multiple malware attacks. In addition to blocking spyware, the S-Series blocks adware, Trojans, tracking cookies, and other forms of malware.

There are three models available: the **S660** for large enterprise deployments (over 10,000 users), **S360** (for mid-size companies with under 10,000 users) and **S160** (for small companies with under 1,000 users).

SaaS Solutions:

The recent ScanSafe acquisition has added the following line of hosted Web Security solutions:

- **Web Security** – protects organizations from various types of 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 1 billion Web requests a day, it analyzes all elements of a Web request, including HTML, JavaScript, Flash, active 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 through 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, if needed, 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.

- **Anywhere +** is a Web filtering service for roaming employees that combines malware protection with Web content control. It comes in the form of a small agent that can be deployed on an employee's laptop.

  The ScanSafe service comes with extensive reporting capabilities, offering 60 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.

  ScanSafe service is known for minimum latency, capable of analyzing a webpage in about 5 milliseconds. ScanSafe offers 100% availability thanks to

its extensive redundancy capabilities. The company uses 15 live data centers around the world.

STRENGTHS:

- Thanks to ScanSafe's acquisition, Cisco IronPort has expanded its line of Web security solutions to include services, and will also be able to offer hybrid offerings (in the near future).

- Cisco IronPort appliances offer high performance for efficient management of Web traffic in organizations of all sizes. The S-Series includes a built in proxy cache, so that Web traffic is always fast and responsive to end-users, despite the fact that it is being filtered for content and malware.

- Just like Cisco IronPort appliances, ScanSafe services offer multiple layers of protection, including signature, reputation-based, and proprietary heuristics filters, ensuring that companies are protected not only against known, but also brand new threats.

- Both Cisco IronPort and ScanSafe can monitor HTTP and encrypted Web traffic.

- ScanSafe offers a special solution for roaming workers to ensure that all employees and contractors have the same level of Web protection as in-house workers.

- Strong DLP capabilities are offered through partners.

WEAKNESSES:

- For Cisco IronPort appliances, initial setup can be complex.

- Cisco IronPort appliances are relatively expensive.

- No comprehensive Web 2.0 tools are offered on the appliance side.

- Basic DLP capabilities are only included with the ScanSafe service.

- ScanSafe used to derive the majority of its revenue from licensing its Web security technology to other providers. It's unclear whether or not these relationships will continue after the acquisition.

TRAIL BLAZERS

SYMANTEC

20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Symantec was one of the latest companies to enter the Web Security market, with the acquisition of MessageLabs in 2008. However, over the past few months, it has been actively gaining more presence. Its latest acquisition in April 2009, *Mi5 Networks*, added a new line of appliances (Web Gateway) to Symantec's Web security suite.

Appliances:

Symantec Web Gateway – offers Web anti-malware and URL Filtering capabilities. It analyses and manages both inbound and outbound Web traffic.

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 carrying out undesirable outbound activity. It uses behavioral analysis to detect botnets and pinpoint compromised endpoints. It is able to scan and manage all corporate ports and protocols used by an organization.

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

The latest version of the Symantec Web Gateway (4.5) was released in August 2009.

SaaS Solutions:

Managed Web Security Services provides real-time anti-spyware, web virus and URL filtering service.

- **Anti-Spyware and Anti-Virus** – offers protection against Web-based malware. It utilizes real-time scanning of web content, including media and other downloadable content.

- **URL Filtering** – enables companies to block user access to undesirable websites, and restrict or block usage of various media files. Companies can also specify when during the day (and for how long) employees can visit certain websites (i.e. entertainment, social networking, etc.)

Managed Web Security Services also offer agentless roaming user support.

In the near future, Symantec plans to unite Symantec Web Gateway and its managed Web Security services to offer customers a Hybrid solution. It will come with a centralized portal to manage all policies from a unified interface.

Among some of the other future plans is integration of both Web Gateway Web Security services with Symantec's DLP solution.

STRENGTHS:

- With the latest acquisition of Mi5 Networks, Symantec now is able to offer Web security solutions as appliances, as well as services.

- Symantec Web Gateway offers both anti-malware protection, as well as URL filtering.

- Bi-directional filtering enables Symantec to protect users from incoming, as well as outgoing threats and loss of sensitive information.

- With the help of Symantec Managed Web Security services, corporate policies can be centrally enforced for users on-premises, in remote offices, as well as mobile users.

- In addition to Web security, companies can get the whole corporate security package deployed, including Web, e-mail, and IM protection.

WEAKNESSES:

- The current DLP features being offered are very basic, however Symantec does have plans to integrate its Web Security offerings with its Vontu DLP services over the next few months.

- Better Web 2.0 application monitoring tools are needed to give Symantec an edge over the competition.

BARRACUDA NETWORKS, INC.

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

Founded in 2003, Barracuda Networks is a leading provider of appliance-based security, storage and networking solutions. The company quickly grew in popularity due to its affordable prices and simple pricing structure, favored by small and mid-market segments. 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 expanded its security product portfolio with the acquisition of phion, a network security firewall vendor based in Austria and subsequent launch of the Barracuda NG Firewall (February 2010), as well as the October 2009 acquisition of Atlanta-based SaaS Web security provider Purewire, adding cloud-based Web security capabilities to its suite.

Barracuda Web Filter is a plug and play appliance that offers malware protection, content filtering, and undesirable application blocking (IM, music downloads, etc.) Barracuda monitors and manages both inbound and outbound traffic.

For URL filtering, Barracuda Web Filter enables organizations to select from a range of actions, depending on the Web sites users visit, from straight blocking to warning users about potential dangers and/or internal policy violations, associated with certain sites. Web browsing policies can be applied to all users, groups of users, or individual users.

On the malware protection side, Barracuda Web Filter also offers spyware removal from infected PCs – this is a valuable tool, which not many competitors are able to provide.

The latest release comes with enhanced reporting capabilities, offering over 45 reports, which provide the ability to analyze data for the past 6 months.

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.

With the acquisition of Purewire, Barracuda now also offers **Barracuda Purewire Web Security Service**. The Barracuda Purewire Web Security Service offers inbound and outbound traffic control and management, anti-malware protection, as well as extensive reporting capabilities.

In addition, the Barracuda Purewire Web Security Service also comes with basic DLP capabilities, enabling organizations to control the types of Web applications users can access and use, including blog and Wiki's postings, Webmail, and others.

All Purewire services are 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 can offer enterprises any combination of the above Web security offerings – combining on-premise appliances (as an appliance, virtual appliance or Microsoft ISA plugin), the cloud-based Web security service, and the Barracuda Web Security Agent for remote and roaming employees. This comprehensive and flexible deployment is especially beneficial for larger organizations with multiple locations and traveling users. Over the next few months, the company will continue enhancing this hybrid Web security offering, with centralized management and reporting across the Barracuda Web Filter, Barracuda Purewire Web Security Service and the Barracuda Web Security Agent.

All Barracuda Web security solutions and services can be controlled and configured centrally.

STRENGTHS:

- With the acquisition of Purewire, Barracuda now offers three deployment options - appliances, hosted, and hybrid.

- Barracuda offers both malware protection and URL filtering.

- In addition to real-time malware protection, Barracuda also provides removal tools for the existing spyware.

- Competitively priced, with no per-user licensing fees.

- Both incoming and outgoing traffic can be monitored.

- Access to various sites can be managed based on users' roles, time of day, and other corporate policies.

WEAKNESSES:

- Undesirable applications can only be blocked, rather than managed.

- While the reporting capabilities have been significantly improved over the past few months, they currently only offer data analysis for the past 6 months (while most top vendors enable data analysis for the past 12 months).

- With the acquisition of Purewire, and with the addition of a hybrid solution, Barracuda is starting to go after larger accounts, venturing outside of its typical target market. It will now be competing for business with such players as Blue Coat, Cisco IronPort, McAfee, Symantec, and others. While Barracuda has all the basic features of a Web security solution, it currently doesn't offer anything truly unique, so many enterprise customers may prefer to buy their Web security solutions from a more well-known name.

M86 SECURITY

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

M86 is a global provider of Secure Web Gateway (SWG) and e-mail 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.

In November 2008, Marshal merged with US-based Web filtering appliance vendor, 8e6 Technologies. As a result of the merger, the company was renamed M86. The merger enabled both companies to capitalize on each other's strengths to create a more diverse portfolio of solutions. Before the merger, 8e6 Technologies, founded in 1995, was offering Linux-based security appliances (mostly for Web security), while Marshal specialized in Windows-based security software.

Today, M86 Security offers a diverse portfolio of Secure Internet Gateway solutions that range from anti-spam/anti-virus to government and internal compliance for e-mail and Web.

Secure Web Gateway – offers real-time protection against malware, together with URL filtering to monitor user behavior on the Internet. Secure Web Gateway also comes with DLP capabilities to manage outbound Web communications and prevent sensitive data from leaving the organization. It is able to monitor HTTP, as well as SSL traffic. All policies can be managed centrally, with integrated logging and reporting capabilities.

The solution enables organizations to protect workers on premises, in branch office, as well as mobile laptop users.

8e6 Professional Edition – is an appliance-based Web filtering solution for outbound traffic monitoring. It offers such features as URL filtering, application control (such as IM, etc.), outbound content security, spyware and malware control. A number of appliances can be managed centrally, with rules applied to users based on their directory-defined roles and established corporate policies.

8e6 Proxy Blocker – is an appliance designed to block unauthorized Web sites, IM, and other applications in real time by using patented signature-based tools.

WebMarshal - is a software application that offers 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.

Blended Threats Module – is a SaaS solution that finds, detects, and blocks malicious URLs in e-mails. It uses signature-less, behavior-based malware detection technology for more precise malware protection.

STRENGTHS:

- M86 Security offers Web security solutions as appliances, software, as well as services.
- Both incoming and outgoing communications are covered, including compliance and content security features with DLP capabilities.
- Anti-malware capabilities include behavior-based technologies for more accurate protection.
- Protection against blended attacks can be added to all Web security solutions.

WEAKNESSES:

- Rather than offering different versions for different customer sizes, M86's customers have to integrate and manage a large number of appliances when deploying large installations.
- Due to the company changing hands a number of times over the past few years, some customers may be weary of its stability and long-term financial health, which may affect their decision to deploy its solutions.

SPECIALISTS

TREND MICRO

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

A global leader in network and end-point security, Trend Micro provides multi-layered security for businesses across the globe. Since its founding in 1988, the Japanese company has expanded its product line to protect companies from e-mail and Web-based threats with its software, appliance, and hosted security solutions.

Trend Micro provides security solutions that protect organizations at various levels of the network, including at the desktop, server, and gateway.

The **InterScan** solutions offer Web and FTP traffic filtering, virus and spyware protection, phishing protection, as well as outbound traffic monitoring. URL filtering is an optional add-on. They can be deployed as software solutions (**Interscan Web Security Suite)** and software/virtual appliances (**InterScan Web Virtual Appliance).**

In the SMB space, Trend Micro offers more comprehensive solutions as part of its **Worry-Free** product line. This includes **Worry-Free Business Security Managed** (hosted security), **Worry-Free Business Security Standard** (end-point and server protection), and **Worry-Free Business Security** (end-point and hosted email scanning). These products are very low maintenance, easy to set up, and provide an all-in-one solution with anti-spyware, anti-virus, anti-bot, anti-spam, and a personal firewall.

STRENGTHS:

- Web security solutions can be deployed as software, appliances, or hosted services.
- Web Security solutions cover both malware protection, and employee productivity monitoring.

- Trend Micro's small business line of products, the Worry-Free line is affordable, easy to install, and requires minimum maintenance.

WEAKNESSES:

- Some elements (such as URL filtering) are offered at an extra cost, rather than included in the solution. Most web security vendors today offer both basic malware and URL filtering capabilities in a single package.

- The content filtering capabilities of InterScan Virtual Web Security are not as strong as those offered by some of the top Web security solutions today.

- The solutions haven't undergone significant updates in a long time.

WEBROOT SOFTWARE, INC

2560 55th Street
Boulder, CO 80301
www.webroot.com

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

Webroot Web Security Service - is a hosted web security service that protects corporate and mobile users against spyware, viruses, phishing and other types of malware attacks. Spyware protection is provided by Webroot's proprietary anti-spyware engine. Scanning both inbound and outbound traffic, Webroot also offers protection against sensitive data loss. The solution looks at the content of each website, rather than using a list of approved sites, enabling it to prevent infection from a legitimate website that might have been compromised. In addition, Webroot Web Security can also pinpoint which machines (if any) are infected, to enable easy infection clean up.

The URL filtering feature enables organizations to control the way their employees use the Internet, specifying the websites users can access, at what time, and which file types they can upload and download. The Web usage policies can be set up for groups of users and individual users based on their corporate roles.

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 category, bandwidth, infected applications, etc.

STRENGTHS:

- Webroot can manage and protect both inbound and outbound Web traffic.

- Webroot protects organizations not only from immediate threats, but can also scan and clean up existing spyware infections that occurred before the service was implemented, or that have been missed.

- 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.

WEAKNESSES:

- While Webroot's technology powers some of the Web security solutions of many larger vendors, it is not a well-known brand name on its own.

- The URL filtering capabilities can use more features, especially the number of categories of monitored Websites.

CLEARSWIFT

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

With nearly two decades of experience in security, Clearswift protects and manages corporate data traveling via diverse electronic channels, including e-mail and Web (http and https). The company is based in the UK, but maintains offices all over the world, including the United States, Spain, Germany, Japan, and Australia.

Clearswift Web Appliance – offers anti-virus and anti-spyware protection, together with URL filtering.

For anti-malware protection, it uses *Kaspersky* virus scanning, and other third party solutions. It offers bi-directional protection, enabling to not only stop incoming threats, but also prevent undesirable content from going out, produced by possible botnets and other infected applications. Clearswift Web Appliance can manage HTTP and encrypted traffic.

For content inspection purposes, Clearswift Web Appliance 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 over 70 categories of Websites for organizations to choose from to monitor user behavior.

Clearswift Web Appliance also comes with DLP capabilities to help companies minimize or eliminate loss of sensitive data, or prevent inappropriate employees' comments from being distributed via Web channels.

STRENGTHS:

- Clearswift offers a comprehensive Web security appliance with sophisticated compliance features, in addition to strong anti-malware protection.

- Clearswift Web Appliance comes with basic DLP features.
- Clearswift can manage both HTTP and SSL traffic.
- A large number of user management options enable organizations to easily customize the appliance to their specific business needs.
- Serving customers all over the world, Clearswift tailors products to different countries by employing local experts who understand the peculiarities of different markets.

WEAKNESSES:

- The solutions offered are mostly high-end, with no option for simpler deployments for customers who only want basic protection.
- The biggest focus is on user management, rather than malware protection.
- No comprehensive Web 2.0 management tools are currently offered.

ALADDIN

15 Beit Oved St.
Tel Aviv, 61110, Israel
www.aladdin.com

Founded in Israel in 1985, Aladdin provides enterprise security and Digital Rights Management solutions. In 2009, Aladdin was acquired by SafeNet, but continues to operate as an independent subsidiary.

eSafe Web offers protection against Web-based spyware, Trojans, viruses, worms, and other types of Web malware. Add-ons include:

- **eSafe Web SSL** - ensures that all encrypted traffic is legitimate and virus-free.
- **AppliFilter -** helps companies control various types of Web applications used by employees.
- **URL Filtering -** enables companies to control the types of Web sites users are allowed to access.

The latest version 7.1, adds the following capabilities: centralized management of multiple solutions, role-based URL filtering, integration with LDAP directories, better control of streaming media, improved application control and reporting capabilities.

STRENGTHS:

- Aladdin offers all the basic Web security features, including malware protection and URL filtering.

- Aladdin is able to analyze encrypted traffic.

- Web solutions can be deployed as software or appliances.

WEAKNESSES:

- No DLP protection is currently available.

- Aladdin sells all components separately, which adds up to the cost of the complete solution.

- Since the acquisition by SafeNet, Aladdin has not been actively seen competing for the Web security business. The eSafe solution hasn't been updated in almost a year.

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*
Microsoft Exchange & Outlook Market Analysis, 2010-2014	Apr. 2010	$3000.00
Microsoft SharePoint Market Analysis, 2010-2014	Mar. 2010	$3,000.00
Hosted Unified Communications Market, 2010-2014	Mar. 2010	$3,000.00
Microsoft Exchange & Outlook Market Analysis, 2010-2014	Mar. 2010	$3,000.00
Corporate Web Security Market, 2010-2014	Mar. 2010	$3,000.00
eDiscovery and Data Loss Prevention Market, 2009-2013	Dec. 2009	$3,000.00
On-Premises Email & Collaboration Market, 2009-2013	Dec. 2009	$3,000.00
Instant Messaging Market, 2009-2013	Dec. 2009	$3,000.00
Business User Survey, 2009	Nov. 2009	$3,000.00
Email Platforms for Service Providers Market, 2009-2013	Oct. 2009	$3,000.00
Email Archiving Market, 2009-2013	Oct. 2009	$3,000.00
Email Storage Market, 2009-2013	Oct. 2009	$3,000.00
Hosted Email Market, 2009-2013	Aug. 2009	$3,000.00
Corporate IT Survey – Messaging & Collaboration, 2009-2010	Aug. 2009	$3,000.00
On-Premises Unified Communications Market, 2009-2013	July 2009	$3,000.00
Hosted Email Market, 2009-2013	July 2009	$3,000.00
Email Security Market, 2009-2013	July 2009	$3,000.00

Upcoming Publications:

Title	To Be Released	Price*
Social Networking Market, 2010-2014	May 2010	$3,000.00
Email Security Market, 2010-2014	May 2010	$3,000.00

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

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

