

# Magic Quadrant for Secure Web Gateway, 2007

Gartner RAS Core Research Note G00148895, Peter Firstbrook, Lawrence Orans, Arabella Hallawell, 4 June 2007, R2327 06072008

**Secure Web gateway solutions protect Web-surfing PCs from infection and enforce company policies. Incumbent providers have been slow to respond, while new vendors are struggling to get the product mix right and prove their mettle in the demanding enterprise market.**

## WHAT YOU NEED TO KNOW

There is no clear secure Web gateway (SWG) leader that completely satisfies all functional categories across all company types. Buyers will need to make more-strategic purchases and sacrifice current functionality for road maps or accept tactical solutions that solve current needs.

If URL filtering reporting is a key requirement, the traditional URL filtering vendors still represent the best choice.

If malicious software (malware) filtering is a key requirement, products must offer proactive as well as signature-based detection techniques and should inspect bidirectional Layer 4 through Layer 7 network traffic across all ports and protocols.

Application control is the most-immature SWG feature.

Large enterprises will have a much-smaller field of candidates to select from because of scalability and reliability demands.

## MAGIC QUADRANT

### Market Overview

A Secure Web gateway is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance. To achieve this goal, SWGs must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype.

This market is still emerging, and vendors are approaching it from different areas of expertise. Buyers should be careful not to blindly shortlist vendors in the Leaders category in this market. No product completely satisfies all functional categories in a single product, and buyers will definitely need to make some sacrifices. Vendor road maps should be an important consideration.

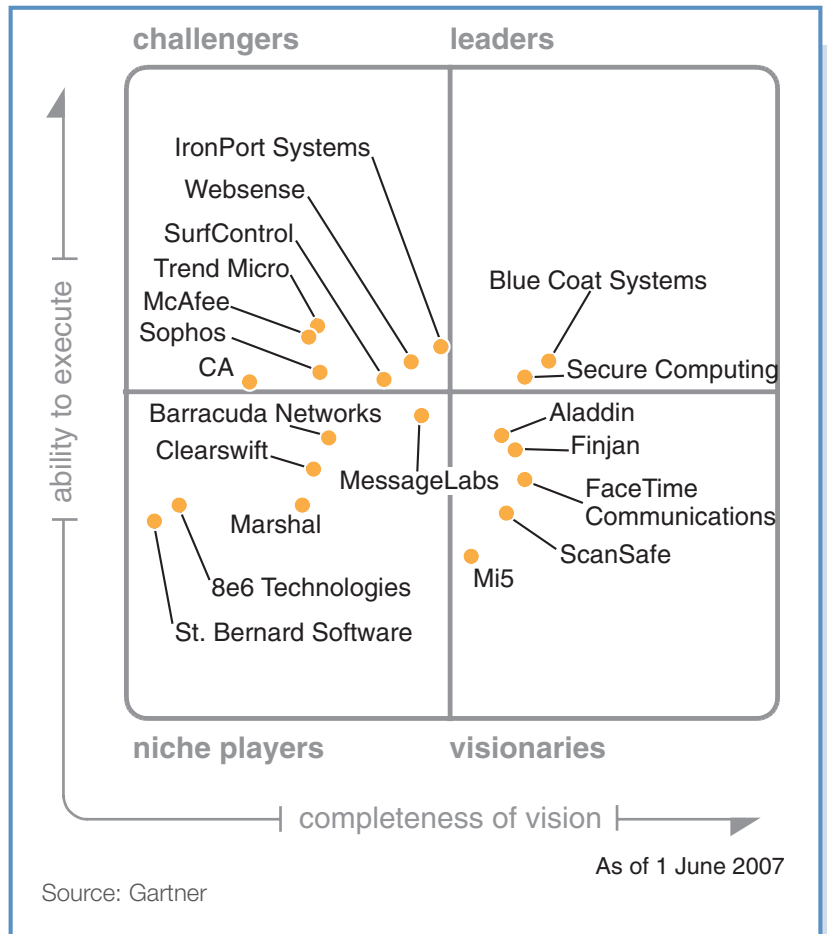
The traditional URL filtering vendors (for example, Websense, SurfControl, Secure Computing, 8e6 Technologies) remain the best choice for scalable, granular Web usage reporting, especially for larger organizations. Malware filtering is increasingly important and provides an

immediate return on investment (ROI) for companies struggling to clean and maintain desktops. Almost all organizations that implemented a bidirectional malware filtering SWG found numerous adware, spyware and other malicious content on their networks. If malware filtering is a key requirement, products must offer proactive (for example, Finjan, Secure Computing, Aladdin, Mi5) as well as signature-based detection techniques, and they should inspect bidirectional Layer 4 through Layer 7 network traffic across all ports and protocols (for example, Mi5, IronPort). A major feature is its ability to identify infected PCs and perform remote remediation (for example, FaceTime, Mi5). Application control is the most-immature SWG feature. IM, Skype and peer-to-peer (P2P) applications are the most commonly supported (for example, FaceTime); however, few SWG solutions can do more than block or allow access on a group or user level. Even fewer actually use application network signatures versus more easily evaded URL or IP address blocking. Secure Sockets Layer (SSL) traffic, in particular, is a notable blind spot for many SWG solutions.

Large enterprises will have a much-smaller field of candidates to select from because of scalability and reliability demands. Scanning large network pipes for malware with low latency is difficult. In-line scanners tend to scale best, but they typically lack fine-grained application control. The ability to seamlessly cluster and manage multiple appliances or software instances is still rare (for example, Blue Coat, IronPort). One of the primary advantages of an e-mail security vendor in the Web gateway is the coordination of content policy across all communications channels; however, only a few of the current crop (for example, Clearswift, Marshal, McAfee, Trend Micro, Sophos) actually share a common content inspection or data leak (or loss) prevention (DLP) policy across both e-mail and Web traffic.

The form factor of SWG products is rapidly morphing from software-based products to scalable appliances and to managed services. We expect more virtual appliances (for example, Finjan) that allow for server hardware standardization but still provide the low total cost of ownership (TCO) of appliances. Many appliance vendors plan to provide software as a service (SaaS) SWGs in the near future, and we anticipate hybrid solutions that allow for common management of appliances in the data center, with services to protect mobile users and branch offices. Some vendors (for example, Websense, SurfControl) offer client-side

Figure 1. Magic Quadrant for Secure Web Gateway, 2007



solutions to enforce policy on mobile devices; however, enterprises have been reluctant to manage yet another client-side software product, and we did not give this feature significant weight. Leading antivirus vendors (for example, Trend Micro, McAfee, Sophos, CA) that already have a client-side presence and the management capabilities have the best chance to make this type of deployment model (in other words, gateway and client) successful.

This Magic Quadrant analysis excludes unified threat management (UTM) devices. UTM devices are traditional network firewalls that also combine numerous network security technologies – such as anti-spam, antivirus, network intrusion prevention system (IPS) and URL filtering – into a single box. UTMs are compelling for the small

The Magic Quadrant is copyrighted June 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2007 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

or midsize business (SMB) market; however, in most circumstances, enterprise buyers should not consider UTMs as replacements for SWGs.

### Market Definition/Description

The SWG market is an emerging composite market made up of multiple existing security markets. URL filtering is the largest submarket in the broader SWG market. Other submarkets that we include in the SWG market are antivirus filtering for Web traffic, dedicated application control, such as IM hygiene, and proxy/cache devices. We estimate the total composite market to be \$700 million in 2006. We expect growth rates to be in the 20% to 25% range. This growth will be fueled by increased penetration of SWG devices, incremental feature revenue and the impact of appliance-based products replacing software.

URL filtering functionality is already deployed in roughly 75% to 95% of enterprise networks, and malware filtering is deployed in only less than 15% of enterprise networks. Penetration of the SWG product – which combines these features with application control – is only sparsely deployed. There is significant growth opportunity for vendors because the market is in only the early stages.

### Inclusion and Exclusion Criteria

The following criteria must be met to be included in this Magic Quadrant:

- Vendors must own unique content capability in at least one of the following categories: URL filtering, anti-malware or application-level controls. This includes granular active content policies, dynamic classification of Web sites and Web “reputation” systems, in addition to traditional anti-spyware and anti-spyware engines and URL lists.
- Vendors must have at least 50 production enterprise installations.

### Added

This Magic Quadrant is new; no vendors were added.

### Dropped

This Magic Quadrant is new; no vendors were dropped.

### Evaluation Criteria

#### Ability to Execute

Vertical positioning on the ability to execute axis was determined by evaluating the following factors:

- Product or Service – The quality of the product, availability and adherence to product road maps, and the timeliness of version releases

- Overall Viability – The company’s financial strength as well as the SWG business unit’s visibility and importance for multiproduct companies
- Sales Execution/Pricing – A comparison of pricing relative to the market
- Market Responsiveness and Track Record – The size of installed base relative to the amount of time the product has been on the market
- Marketing Execution – Brand and product awareness based on frequent inclusion on Gartner’s shortlists
- Customer Experience – Quality of the customer experience based on reference calls and Gartner client teleconferences
- Operations – Corporate resources (in other words, management, business facilities, threat research, support and distribution infrastructure) that the SWG business unit can draw on to improve product functionality, marketing and sales.

### Completeness of Vision

The completeness of vision axis captures the technical quality and completeness of the product and the vendor’s SWG market awareness.

In the product evaluation, we ranked vendors on the following capabilities:

- URL Filtering – Databases of known Web sites categorized into groups to enforce acceptable usage and productivity and to reduce security risks. The URL filtering capability was heavily weighted in this Magic Quadrant. To displace incumbent URL filtering products and “steal” allocated budget, SWG vendors will have to be competitive in this capability. Quality indicators, such as the depth of the page-level categorization, the categorization of new sites/dynamic risk analysis of uncategorized sites and pages, and the categorization of search results, were considered.
- Malware Filtering – The second-most-important capability is filtering malware from all aspects of inbound and outbound

**Table 1. Ability to Execute Evaluation Criteria**

Evaluation Criteria	Weighting
Product/Service	low
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	low
Market Responsiveness and Track Record	high
Marketing Execution	low
Customer Experience	high
Operations	low
Source: Gartner	

Web traffic. Signature-based malware filtering is standard on almost all products evaluated; consequently, extra credit was given for non-signature-based techniques as well as the range of inspected protocols, ports and traffic types. Products that can identify infected PCs and the infection by name and enable prioritized remediation got extra credit.

- **Application Control** – Granular, policy-based control of Web-based applications, such as IM, multiplayer games, Web storage, wikis, P2P, public voice over IP (VoIP), blogs, data-sharing portals, Web backup, remote PC access, Web conferencing, chat and streaming media, is still immature in most products and represents a significant differentiator. The ability to selectively block or manage features of applications based on numerous policy parameters and the presence of pre-developed policies to simplify deployment were given extra weight.
- **Manageability/Scalability** – Features that enhance the administration experience and minimize administration overhead were compared. Extra credit was given to products with a mature management interface, consolidated monitoring and reporting capability, and role-based administration capability. Features such as policy synchronization between devices and multiple network deployment options enhance the scalability and reliability of solutions.
- **Delivery Models** – Appliance- and/or service-based delivery models get extra credit compared with software only, and extra credit was given to vendors that offer all three deployment types. Also, the quality of the form factor was considered; for example, appliances that fail open and are hardware-optimized for the job. Software that comes as a virtual appliance gets credit compared with software that requires a base operating system (OS). For services, infrastructure quality was considered.
- **Application Acceleration** – Extra credit was given for caching and other application acceleration techniques; while not mandatory, these are useful to have to scale and reduce latency.
- **Integration With E-Mail** – Integration of e-mail and the Web gateway will increase, driven by communications provisioning requirements and content inspection needs. Consequently, vendors that can share a common policy, the management interface and threat intelligence across these gateways are more visionary than others. However, we did not give extra credit to vendors that simply inspected SMTP traffic for malware in the same box.

Consideration was also given to organizational characteristics, such as how well the vendor understands this market, its history of innovation, and its marketing and sales strategies, as well as its geographic presence.

### Leaders

Leaders are high-momentum vendors (based on sales and “mind share” growth) with emerging track records in Web gateway security, as well as vision and business investments that indicate they are well-positioned for the future. Leaders do not necessarily offer the best products for every customer project; however, they provide solutions that offer relatively lower risk.

### Challengers

Challengers are established vendors that offer SWG products but that do not yet offer strongly differentiated products, or their products are in the early stages of development/deployment. Challengers’ products perform well for a significant market segment but may not show feature richness or particular innovation. Buyers of challenger products typically have less-complex requirements and/or are motivated by strategic relationships with these vendors rather than tactical requirements.

### Visionaries

Visionaries are vendors that are distinguished by technical and/or product innovation but have not yet achieved the record of execution in the SWG market to give them the high visibility of the leaders or those that lack the corporate resources of challengers. Expect state-of-the-art technology from the visionary vendors, but buyers should be wary of a strategic reliance on these vendors and should monitor the vendors’ viability closely. Given the maturity of this market, visionaries represent good acquisition candidates. Challenger vendors that may have neglected technology innovation and/or vendors in related markets are likely buyers of visionary vendors. As such, these vendors represent a higher risk of business disruptions.

### Niche Players

Niche Players’ products typically are solid solutions for one of the three primary SWG requirements – URL filtering, malware and application control – but they lack comprehensive features of visionaries and the market presence or resources of the challengers. Customers that are aligned with the focus of a niche vendor often find such providers’ offerings to be “best-of-need” solutions.

**Table 2. Completeness of Vision Evaluation Criteria**

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	low
Sales Strategy	low
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	no rating
Innovation	standard
Geographic Strategy	low
Source: Gartner	

## Vendor Strengths and Cautions

### 8e6 Technologies

#### Strengths

- 8e6 Technologies is an appliance-only URL filtering solution vendor that targets primarily the education market and large enterprises.
- Its R3000 filtering appliances are positioned out-of-band, so they do not require integration with proxy caches or firewalls (URL blocking is achieved by sending a TCP reset message to break a connection).
- Reporting, ease of implementation and scalability are strengths of 8e6's URL filtering solution.
- The company offers two reporting appliances. Its Enterprise Reporter enhances filtering scalability and performance by off-loading log scanning and report generation functions from the R3000 filtering appliance. The level of detail collected in Enterprise Reporter provides excellent forensic analysis.
- In 2006, 8e6 introduced its Threat Analysis Reporter appliance, which provides real-time monitoring of an organization's Web usage and real-time alerting of policy violations.
- 8e6's filtering appliance has the ability to block traffic sent to anonymous proxies, a problem that is becoming increasingly widespread in K-12 schools. Students can bypass traditional URL blocking solutions by first accessing an anonymous proxy, from which they can then access inappropriate Web sites. 8e6 has developed approximately 20 signatures for blocking popular implementations of anonymous proxies.
- In 2007, 8e6 plans to move into the content monitoring and filtering (CMF) and data loss (or leak) prevention (DLP) market via its partnership with GTB Technologies (GTB will be integrated into existing 8e6 solutions).

#### Cautions

- The R3000's out-of-band positioning prohibits its ability to provide inbound malware protection.
- It cannot scan for viruses or spyware signatures, nor can it hand off content to be scanned by a separate appliance.
- The R3000 has limited application control, in that it can prevent IM and other P2P sessions using signatures that it has developed. However, because the R3000 cannot function as a proxy, it lacks the ability to provide granular policy control over these applications.
- While it offers a strong URL filtering solution at a moderate price, it lacks the ability to dynamically classify unknown URL addresses in real time.

### Aladdin

#### Strengths

- Aladdin is an early visionary entrant into the SWG market, although it is perhaps better-known for its identity token business.
- The installed base of the SWG product line is a good distribution of large and small enterprises across a wide geography.
- Aladdin gets very high marks for malware detection across all ports and protocols.

- The company was an early antivirus vendor and continues to utilize its own malware signatures in addition to several real-time malware detection techniques.
- Its embedded URL filtering database is licensed from IBM (IBM's ISS division owns a URL filtering database, but the quality of the list and the reporting are not considered best of breed).
- The product has an extensive list (more than 1,000) of pre-developed application filter policies and will develop new policies on demand as required by customers.
- SSL decryption support is available with a separate appliance; however, it does allow policy-based decryption.
- The SWG product line consists of a virtual appliance (a hardened Linux OS and the eSafe SWG application) and two appliance models – the largest of which can satisfy up to 2,000 users.
- The eSafe SWG is an in-line filter and supports an extensive list of deployment options that provide for scalability for more than 20,000 seats.
- The management capability is improving and gets good marks overall for management ease, policy synchronization and directory integration.

#### Cautions

- The biggest challenge for Aladdin is improving its brand awareness, especially in North America, and its SWG product mind share.
- The reporting capability gets good reviews from smaller clients, but larger clients would like more granularity.
- The eSafe product is an in-line filter which, while extremely fast, can be more difficult to add a much-needed granular application control capability.
- While it is definitely advantageous to have malware experience and labs, it is not clear that SWG vendors should attempt to keep up with the exploding volume of malware signatures when there are plenty of good malware databases they could license.
- Finally, although Aladdin also offers SMTP spam filtering, few users we talked to relied on this capability as a primary anti-spam defense, and the ability to do policy-based outbound content inspection on Web communications is lacking.

### Barracuda Networks

#### Strengths

- Barracuda Networks' (Barracuda's) mission is to become the value provider of appliances in high-growth markets. Its initial focus was the e-mail security market. Next, it tackled the SWG market. Its main competitive weapons are its sales channel and fast supply chain.
- To keep costs low, Barracuda exploits numerous open-source technologies, but it has been adept at adding many required features and functionality within its appliances in a timely manner.
- Barracuda raised the bar for many vendors in the markets it entered by being quicker to market with features than some of its incumbent competition and by providing best-of-need appliances at a very reasonable price.

- Barracuda customers tend to SMBs that are willing to forgo enterprise-class functionality for a good price and fast service.
- Barracuda will face increased competition from UTM vendors and from Micro Trend and McAfee because they deliver SWG appliances bundled with their anti-spyware suite licenses.

#### Cautions

- Barracuda's Web security gateway appliance (WebFilter) was first offered in 2005, but it has not been met with quite the same success as the vendor's e-mail products.
- User reports indicate there have been stability and latency problems, especially with earlier versions.
- Users also report some false positives with the URL filtering as well as authentication and reporting challenges.
- Group- and user-level policy via LDAP integration was only recently delivered, and Kerberos authentication is not yet available.

### Blue Coat Systems

#### Strengths

- Blue Coat's flagship product is its ProxySG family of proxy/cache appliances, which provide a strong platform for an SWG, given their ability to support URL filtering, malware filtering and application control.
- Blue Coat is one of the few vendors in this market that has proved its scalability and performance via widespread deployment in large data centers. Customer references report that performance does not degrade, even when running thousands of lines of custom policy scripts.
- Blue Coat's proxy platform offers on-box deployment of nine different URL filtering lists – many common and some regionally based. One of the nine options is Blue Coat's own WebFilter, a good database that it prices aggressively. Blue Coat also offers a strong solution for dynamically classifying unknown URLs.
- Reporting capabilities are good, but they are not quite as mature as those of SurfControl and Websense.
- Malware filtering is offered via Blue Coat's ProxyAV appliances, which offer a choice of many popular antivirus engines. Blue Coat has no malware filtering capabilities of its own; it relies solely on its partners for this purpose.
- Blue Coat's proxies recognize and filter many common P2P applications and enable flexible policies to control these applications (for example, user-based, strip active content and others).
- In 2006, Blue Coat purchased the Network Appliance NetCache customer base, its main competitor for high-end proxy appliances, and Permeo Technologies, which gave it a solution for client-side filtering, application control and acceleration. Both moves strengthened Blue Coat's dominance of the proxy market.

#### Cautions

- Blue Coat is about to face competition from a reinvigorated Secure Computing, IronPort and Websense's new Content Gateway solutions. These vendors have yet to match Blue Coat's proven scalability, rich feature set and performance, but

they are much more focused on broader and less-expensive integrated malware filtering options.

- Blue Coat chose in 2006 to focus on application acceleration (its Mach5 offering), which has the potential to mitigate latency inherent in additional security functions.
- We expect Blue Coat to refocus on security in 2007.
- In addition to less-mature or less-scalable URL filtering reporting capabilities, Blue Coat also lags Websense and SurfControl in the area of client-based filtering for mobile clients (although its endpoint agent will add this function later in 2007).
- Although its URL filtering option is inexpensive compared with the market leaders, Blue Coat's SWG and anti-spyware is an expensive solution overall.

### CA

#### Strengths

- CA's main SWG product is the eTrust SCM WebFilter, which includes antivirus and anti-spyware, Web URL filtering, and content filtering. The SCM WebFilter is often bundled by CA in various suites that include other desktop and e-mail gateway security functionality.
- The CA SCM WebFilter is a software-based Web proxy solution, which shares a common management console with the other components of the suite.
- Its URL filtering database is licensed from Secure Computing's SmartFilter.
- CA provides its own internally developed, signature-based malware protection, but it lacks significant zero-day protection.
- The CA SCM WebFilter provides basic application control based on a URL classification to block or allow Web applications. NTLM integration enables user- or group-level policy enforcement.
- CA's main strength is the ability to bundle a broad suite of malicious protection mechanisms into a suite of products under common management and reporting.

#### Cautions

- With a few notable exceptions, the CA SCM customer base is mostly (95%) SMBs (fewer than 500 seats) that are looking for an all-in-one security solution (e-mail security, DLP and SWG functions).
- Like other desktop antivirus vendors in the SWG market (for example, McAfee, Sophos, Trend Micro), the primary challenge is demonstrating significant diversity between client and gateway malware detection techniques, such that malware detection rates are increased, rather than malware simply being caught in a different location.
- The proxy is not a caching proxy, and it does not support other common protocols (for example, SSL, Telnet and others) outside of HTTP – a liability when dealing with evasive spyware – and it does not proxy the common IM applications (AOL, MSN and Yahoo), so it cannot strip off inbound attachments or URLs, nor can it provide other, more-granular policies.
- Because it runs strictly on Windows platforms, the CA SCM WebFilter will be hard-pressed to match the performance,

scalability and security of purpose-built appliances for larger data center customers. Support and cost of the underlying Windows hardware and software should also factor into the TCO.

## Clearswift

### Strengths

- Clearswift is considerably better well-known for its e-mail security solution, but it also has MIMESweeper for Web appliances and a software product line, which is used by roughly 25% of its clients.
- The primary advantage of a combined Clearswift product is a common outbound content inspection/DLP policy capability across SMTP and Web communications modalities (Web mail, IM). Indeed, Clearswift has adopted a strategic focus on better enabling enterprise content governance.
- The URL filtering database, licensed from one of the best-of-breed URL vendors, is augmented with dynamic classification of uncategorized sites.
- Clearswift has excellent deep-file inspection and handling capabilities, which are exploited in application control for Web applications, thereby allowing access while still providing significant control over the types of files and/or data that can be uploaded or downloaded.
- MIMESweeper is available as both software and an appliance product, but anti-spyware is not included in the software version.
- Clearswift is a natural shortlist vendor for its existing installed base and prospects looking for integrated e-mail and IM gateway content inspection/DLP.

### Cautions

- Clearswift is a very Europe, Middle East and Africa (EMEA)-focused company, with 74% of its revenue in EMEA and only 14% in North America. It has started to focus on building a stronger U.S. and Asia/Pacific organization and channel, but it presently has less brand awareness in these markets.
- The appliance malware detection techniques rely on signatures (Aluria and Kaspersky Lab), Multipurpose Internet Messaging Extensions (MIME)-type analysis or static, policy-based content controls, such as limiting active code.
- The software product does not bundle anti-spyware signatures. Scanning is limited to port 80 and standard Web protocols.
- More-granular IM, Skype and P2P traffic controlling is handled by an additional solution (MIMESweeper IM Enterprise Edition) licensed from FaceTime.
- Reporting and policy enforcement is not yet fully integrated across all products, and consolidated reporting across multiple boxes is missing.
- Enhancements to address these deficiencies are expected to be in the next release in June 2007.

## FaceTime Communications

### Strengths

- FaceTime Communications is a best-of-breed IM hygiene vendor.
- The company's IM installed base is on the smaller side for SWGs, but it has a disproportionate share of large enterprises, especially in the financial industry, because of its early focus on IM.
- Its primary differentiation is its deep focus on allowing the granular management of real-time, Web-based communications networks (for example, IM, Skype) and P2P networks (for example, Roddi, BitTorrent, hopster, iMesh).
- FaceTime recently added a choice of Secure Computing or SurfControl for the URL database option.
- Malware detection is delivered through integration of standard anti-spyware engines (for example, Symantec, Trend, McAfee or CA) backed by its spyware research from the XBlock Systems and spywareguide.com acquisitions.
- FaceTime recently added "endpoint inoculation," which provides a manageable Microsoft Software Restriction Policies (SRP) and ActiveX kill bits to inoculate clients from known threats. A primary advantage of FaceTime is target remediation, which allows dynamic cleanup of infected PCs.
- To get the full capabilities, organizations need to acquire the FaceTime Enterprise Edition, which consists of multiple optional modules and both a gateway appliance and a software management console.
- Several e-mail security vendors license the core FaceTime IM capabilities for integration into their e-mail boundary solutions.

### Cautions

- Despite its recent spyware focus, FaceTime is still the best fit for organizations looking for an IM hygiene security product that can also offer spyware security.
- The company remains a good acquisition target for e-mail security vendors seeking to enhance Web communications support, especially IM.
- The lack of integration with e-mail policy makes it difficult for companies to invest in IM hygiene, fearing multiple silos of communications policy.
- Proactive malware detection in HTTP traffic needs to be improved.
- We anticipate FaceTime will integrate its multiple component architecture into a single appliance product with a simpler pricing scheme later in 2007.

## Finjan

### Strengths

- Finjan is an early Web security vendor with extensive experience in malware research.
- The company is maturing its ability to execute with a new board and numerous vice president and chief corporate officer additions to support rapid growth. It also raised \$10 million (February 2006) in new capital, with notable investments from Microsoft and Cisco.

- The company boasts an impressive North American and EMEA customer list, including a significant number of deployments with more than 20,000 seats.
- Finjan's primary differentiation is its proactive malicious-code detection technique, which can scan a broad array of programming languages (for example, HTML, JavaScript, VBScript, Java) for malicious intent.
- Finjan's code analysis may also catch poorly written custom applications that may not be malicious but that violate secure coding practices. Disposition actions include the ability to remove or repair malicious code.
- Limited URL list management (for example, whitelist/blacklist) is provided by Finjan. Supplemental integrated URL filtering is licensed from SurfControl.
- A limited number of popular applications can be detected using protocol attributes (headers, payload, URL) and managed via the policy engine; however, setting up policy is slightly more cumbersome than with other tools.
- The Vital Security product line consists of four, different-size full-HTTP(s)/FTP proxy appliances developed on a hardened Linux Debian OS, the largest of which can process more than 650 Mbps of Web traffic and can use load balancers to scale. Finjan also anticipates offering a SaaS delivery model in late 2007.

#### Cautions

- Finjan offers one of the stronger anti-malware solutions, especially for targeted or zero-hour threats, but Finjan should add bidirectional inspection across more ports and protocols to detect evasive malicious traffic.
- Finjan is relatively well-known in the European Union (EU), but the brand is slightly tarnished from past fumbles and is unfamiliar in North America.
- Rapid growth may be contributing to reportedly inconsistent service levels.
- Strong technology and a blue-chip installed base make Finjan an attractive acquisition target for networking or security companies late to the SWG market.
- Some customers complain about the number of false positives the product blocks, which increases administration time to manage a whitelist of poorly written but not malicious Web sites. Moreover, troubleshooting false positives may require more application development than network engineering experience.

#### IronPort Systems Strengths

- IronPort Systems, which has garnered a stellar reputation for its high-performing e-mail security appliances, recently launched its proxy-based Web security gateway – the S-Series – designed to support multiple simultaneous filtering/scanning engines.
- The initial anti-spyware scanning (with databases licensed from Aluria Software and Webroot Software) was recently supplemented with anti-spyware scanning (McAfee) and URL filtering (licensed from a leading URL vendor).

- The URL categorization engine is augmented with IronPort's own URL reputation data from its SenderBase reputation service.
- Malware protection is also enhanced with an outbound Layer 4 traffic monitor, which is capable of intercepting non-HTTP outbound traffic going to URLs and IPs that are a security threat.
- The S-Series also offer application control using application signatures to identify and block/allow Web-based applications, including Skype and popular IM applications. IronPort's experience in large enterprises has helped it design the S-Series for complex enterprise environments.
- In January 2007, Cisco agreed to acquire IronPort in the second quarter of 2007. Given Cisco's resources, we expect IronPort to be a leader in 2008 and an especially potent threat to Blue Coat in large enterprises, as the product and installed base matures, and the company can take advantage of the reach of the Cisco sales force.

#### Cautions

- Despite its promise, so far, the S-Series installed base is very small, and some early beta customers experienced the "teething" problems expected from a first-generation product. Specifically, users commented on false positives with the URL reputation data and the lack of detail for malware and end-user URL activity reporting.
- Early customers also indicate that the performance of the box – always the big question mark associated with anti-spyware scanning of Web traffic – has met expectations.
- Despite a common code base, policy management and reporting across the e-mail and Web appliance are not yet integrated, and cross-protocol DLP capabilities are lacking.
- The proxy needs to rapidly support more Web protocols (for example, sockets, streaming media, native FTP).
- To control its service levels, it will be important for IronPort to start to own more of the "content" for SWG functionality, especially for URL categorization.
- Application control is still rudimentary; we anticipate IronPort will make some acquisitions after the Cisco merger is complete to rapidly improve this capability.

#### Marshal Strengths

- Marshal is another SWG vendor that is better-known for its e-mail security product, but it also has a presence in the Web gateway market.
- WebMarshal is a software-based proxy product that can also be attached to a Microsoft ISA server via an ISAPI plug-in, making it attractive to the SMB market.
- WebMarshal can integrate with SmartFilter, but most existing customers prefer Marshal's less-expensive categorization database. Marshal also provides an on-the-fly URL categorization engine based on keyword scanning and content analysis and user-defined criteria.
- Malware filtering is included via dynamic-link library (DLL) integration supporting a number of popular antivirus or anti-spyware signature databases.

- Directory-based (for example, group and user) application control allows the blocking of known HTTP applications identified by URLs, and it has a number of policy control parameters, such as bandwidth quota, domain, time of day, browsing time and file attributes.
- WebMarshal shares the same content inspection capability as MailMarshal to filter and manage in/outbound content.
- WebMarshal is a natural shortlist vendor for MailMarshal clients and prospects.

#### Cautions

- Marshal must expand its brand recognition in North America and launch an appliance product that enhances the capabilities of the current software product. To that end, the company plans to launch an appliance product in late 2007, and it is also considering a managed services offering for 2008.
- One of the primary advantages of an e-mail security vendor in the Web gateway is the coordination of content policy across all communications channels; however, WebMarshal doesn't share a management interface or policies with MailMarshal yet, but this is due later in 2007.
- Marshal has also neglected to integrate IM security product into the WebMarshal product.
- The dynamic URL filtering is ineffective with flash or Java-based content.
- Some customers commented that overall maturity and stability, as well as management, reporting, and scalability features, are not yet as strong as in MailMarshal.
- Malware detection capabilities are mostly dependent on the strength of the third-party antivirus.

#### McAfee

##### Strengths

- McAfee revamped its Web security appliance product line in 2005, added the Secure Computing list and increased functionality.
- Its recent line of secure Internet gateway appliances encompass HTTP and SMTP, which are targeted mostly at SMBs and midtier enterprises, and are not priced per node.
- The largest, the SWG appliance, can be used for companies with 5,000 users.
- McAfee has made some strides in rounding out its product strategy, adding URL reputation (via its SiteAdvisor acquisition) in a release in May 2007.
- McAfee does have some e-mail security functionality, and DLP functionality is expected to ship later this year, leveraging technology the company acquired from Onigma.
- For existing McAfee customers, especially SMBs, McAfee may be a suitable option, especially for those with an existing suite license.

#### Cautions

- Like other desktop antivirus vendors in the SWG market (for example, CA, Sophos, Trend Micro), the primary challenge is demonstrating significant diversity between client and gateway

malware detection techniques, such that malware detection rates are increased, rather than malware simply being caught in a different location.

- McAfee has not yet cracked the performance "nut," and it does not have a product suitable for large enterprises (more than 5,000 seats) without clustering multiple appliances.
- McAfee also has only rudimentary IM and application control capabilities.
- While McAfee's channel and installed base remain strong with its desktop anti-spyware base, the company has not delivered a best-of-breed product suitable for larger enterprises.

#### MessageLabs

##### Strengths

- MessageLabs is a privately held managed service provider, headquartered in the U.K. MessageLabs has a long history (since 1999) of providing e-mail-security-managed services. The company has invested in growth in the United States during the past four years and has reselling partnerships with IBM and Verizon Business.
- After initially acting as a reseller of ScanSafe, the company launched its own SWG service in late 2006.
- The company has expanded its inbound scanning services outside e-mail via an acquisition of Omnipod, an IM security provider.
- MessageLabs has begun to expand its Skeptic heuristics malware detection engine for HTTP and combines it with traditional antivirus signatures to provide malware protection.
- The URL database is licensed from SurfControl.
- MessageLabs is particularly attractive to existing customers that are looking to invest in SWG functionality using an management service provider (MSP) and synchronize acceptable-use policies for HTTP and IM with their e-mail security policies.

#### Cautions

- The market for managed Web security services is nascent, much more so than for e-mail security. MessageLabs is still very new in this market, and well over 90% of the company's revenue currently comes from e-mail security and compliance offerings.
- Like many other SWG vendors, reporting and capabilities for nested/hierarchical policies are still a challenge for MessageLabs.
- Application control and URL reputation and dynamic classification are rudimentary.
- The company needs to invest in DLP for what will become an important expansion of acceptable-use policy enforcement, which is monitoring blogs and consumer Web mail for compliance with company policies.

#### Mi5

##### Strengths

- Mi5 is a very promising startup company that launched its line of five Mi5 Webgate appliances at Mi5 Webgate Appliances in February 2006.

- Mi5 developed its own streaming inspection architecture, which enables bidirectional malware scanning of all ports and protocols with low latency.
- The Webgate appliance uses Sophos and Sunbelt scan engines, along with its own network behavior heuristics that detect a wide range of malware – including an innovative Botnet traffic detection function.
- A major advantage of Webgate is its ability to identify infected PCs by name, provide a severity indicator and dispatch a dynamic cleanup agent (obtained from Sunbelt).
- Mi5 recently licensed a URL categorization database from IBM.
- The URL and malware filtering subscriptions are very competitively priced to fit comfortably in most companies' existing URL-only filtering budgets.
- Application control is limited to directory and policy application URLs and file type blocking.
- For multinode deployments, the central management device distributes policy and configuration settings and provides central reporting.
- Webgates are typically deployed in-line, or off a spanning port, which has fewer clustering options; however, Mi5's highest-end platform (Dual Xeon) supports up to 1 Gbps of traffic with very low latency.
- Redundant hardware, active standby configuration and fail-open features provide additional reliability.

#### Cautions

- Mi5 faces stiff competition from much-larger established vendors, and it is not clear that other vendors cannot achieve the same scalability results with a different architecture.
- Building a strong channel organization will be a key step to gain access to the enterprise market.
- The company has only a limited history of producing fast, accurate signatures or proactive rules for zero-day threats.
- Mi5 should include application programming interfaces (APIs) for more URL, anti-spyware and anti-spyware engines.
- Application control, such as IM and P2P blocking, is not yet available.
- SSL decryption will require Mi5 to add a proxy engine.
- Although it is very good for an early release product, the management and reporting capability also needs to mature to provide finer levels of detail.
- The company's road map includes adding support for additional detection engines, application control and SSL later this year.

#### ScanSafe Strengths

- ScanSafe was the first company to launch a managed service for URL filtering and malware scanning of Web traffic.
- It recently added IM application control.
- Although it is still a relatively small vendor, the company has quickly garnered a relatively significant installed base of customers and a network of traditional value-added resellers (VARs)/resellers as well as more-strategic OEM relationships

with larger service providers, such as AT&T and Postini.

- ScanSafe has invested in its own capabilities for filtering malware from Web traffic and analyzing URL reputation (in other words, where the Web server is generated, the traffic pattern and so on).
- ScanSafe offers SearchAhead and Scandoo services, which warn users of the services of the "riskiness" of a URL before it is clicked.
- Early user feedback on malware scanning and URL filtering has been positive, and latency issues have not been reported by the majority of clients.
- ScanSafe stores all the log data in its data center, which can be a benefit to company struggling to keep up with large amounts of log data and the associated database management tasks.

#### Cautions

- Customers comment that ScanSafe's reporting capabilities are limited compared with traditional solutions.
- ScanSafe has provided a mechanism to port authentication information from a company's existing proxy and to transfer company Active Directory information; these decisions can be challenging for larger companies.
- Currently, ScanSafe does not have DLP capabilities, although it launched IM filtering last year.
- We expect competition to increase for ScanSafe in 2008, from both existing service provider players (for example, MessageLabs and SurfControl/BlackSpider, which have recently launched similar services) and appliance and software vendors expanding into the service provider business.

#### Secure Computing Strengths

- Secure Computing has strong offerings in the three main components of a SWG and launched three new proxy appliances in November 2006.
- It owns the SmartFilter URL filtering database, which it deploys on its own appliances and also distributes via OEM agreements to nearly 30 network security appliances.
- Secure's Webwasher proxy appliances also enable malware protection and application control.
- The acquisition of e-mail and messaging security vendor CipherTrust (in 2006) has strengthened Secure's management team and has enhanced its product portfolio.
- Secure uses CipherTrust's TrustedSource reputation system to dynamically classify unknown URLs and assign a reputation score to each URL.
- All three appliances offer anti-malware protection on-box via internally developed proactive malware detection technologies (similar to Finjan's techniques), supplemented by partnerships with antivirus vendors.
- The anti-malware protection is enhanced by the proxies' ability to decrypt and inspect SSL traffic.
- The Webwasher appliance also provides granular application control over IM and other P2P applications. The company plans to further enhance these capabilities by integrating CipherTrust's IronIM IM hygiene solution into the Webwasher appliance, but IronIM presently remains a separate product.

- Secure acquired DLP technology via CipherTrust and has integrated some of this DLP functionality into its Webwasher appliances.

#### Cautions

- Secure has a sizable revenue stream (\$264 million revenue for its 2006 fiscal year) from a broad array of products; however, it lacks significant brand recognition.
- Secure is busy integrating and rationalizing its product portfolio obtained through numerous acquisitions and dropping numerous subbrands to eliminate confusion.
- The SmartFilter URL database is a distant third behind Websense and SurfControl in terms of revenue-based market share. Gartner estimates that SmartFilter garnered approximately 15% of worldwide revenue for URL filtering in 2006, although it has a larger seat market share because of the revenue impact of its OEM strategy.
- Integration of e-mail/IM and SWG products into a common management interface is still lacking, although it is scheduled for deployment in 2007.
- Secure needs to demonstrate in production deployments that its new Webwasher appliances meet the scalability and performance demands of very large data centers.

#### Sophos Strengths

- Sophos, an experienced anti-malware vendor, recently (February 2007) launched its proxy-based WS1000 Web Security (WS) appliance.
- Sophos has deep malware experience and a host of techniques to detect new threats early in their life cycle, thereby providing broad threat family signatures. Sophos also provides behavioral analysis, which is effective at intercepting some new threats without the need for an update.
- Sophos has a unique Managed Appliance offering, which provides automatic software updates, proactive system health monitoring and on-demand remote assistance, reducing the administration burden for clients.
- The WS1000 can block application URLs that run over HTTP through URL categorization, controlling streaming media and block the download of known unwanted client applications.
- The company's own URL analysis, which classifies URLs into five trust categories, ranging from "high risk" to "trusted," is augmented with SurfControl's URL categorization database.

#### Cautions

- Like other desktop antivirus vendors in the SWG market (for example, CA, McAfee, Trend Micro), the primary challenge is demonstrating significant diversity between client and gateway malware detection techniques, such that malware detection rates are increased, rather than malware simply being caught in a different location.
- The WS1000 is limited to a maximum of 2,000 users per box. Although there are a number of clustering options, there are no role-based administration options, automatic methods to synchronize policy, or consolidated management/reporting yet. It needs to rapidly improve its capability and scalability to gain broader enterprise market share.

- Sophos needs to expand the number of ports and protocols (including HTTPs) it inspects and/or proxies to manage more-evasive spyware traffic and applications, such as Skype and non-HTTP P2P traffic.
- The WS1000 management console uses the same graphical user interface (GUI) as the company's e-mail security appliances; however, they are distinct products today, and shared content inspection policy is notably lacking.
- Some users comment that reporting capabilities are still immature.

#### St. Bernard Software Strengths

- St. Bernard Software offers a family of three iPrism appliances as well as LivePrism, an SaaS service (similar to MessageLabs and ScanSafe).
- St. Bernard's primary market is the SMB URL filtering market, and the company does not claim its appliances have significant malware filtering or application control; however, the LivePrism service offers HTTP antivirus scanning, e-mail filtering and basic IM security.
- The company has improved its reporting capabilities by adding a new appliance dedicated to reporting (its Enterprise Reporting Server, the ERS M6200).
- St. Bernard has implemented a limited form of a reputation service by mapping known URLs to registered IP addresses (which it positions as an anti-Domain Name System [DNS] spoofing solution).
- The St. Bernard appliances and URL filtering subscriptions are inexpensive and will appeal to many SMBs that focus primarily on URL filtering.

#### Cautions

- St. Bernard's appliances do not offer anti-malware protection, and they have limited ability to provide application control.
- While the appliances are commonly deployed in-band (in-line), they are optimized to analyze outbound traffic rather than inbound filtering.
- The iPrism appliances offer limited control over IM services – they use signatures to block them, but the appliances cannot offer granular control, such as allowing the service but stripping off inbound attachments.
- The iPrism appliances lack the ability to dynamically classify unknown URL addresses in real time.
- The LivePrism service faces stiff competition from more-established providers, such as ScanSafe and MessageLabs.
- St. Bernard needs to raise its market visibility.

#### SurfControl Strengths

- SurfControl has been a stalwart in the URL filtering market since the mid-1990s and continues to deliver an enterprise-class URL categorization database with granular reporting capabilities, including superior Active Directory integration.
- Reporting and directory integration continues to set the company apart from the majority of the other SWG vendors.

- Since the commencement of new management in 2006, SurfControl has improved its channel operations and increased the licensing of its URL list, particularly to UTM vendors, such as Check Point Software Technologies and Juniper Networks.
- The company acquired BlackSpider, a small EU-focused e-mail and Web security MSP in 2006 that SurfControl can leverage to provide multiple delivery options as well as a hybrid delivery model.

### Cautions

- As with Websense, enterprises do complain about false positives associated with URL categorization and the length of time (sometimes several days) it takes the company to recognize new sites.
- With malicious sites, such delays challenge the value of traditional URL categorization.
- The company has been slow to deliver a full-fledged SWG strategy.
- It finally announced anti-spyware partners (Kaspersky Lab and McAfee) in late 2006, but their anti-spyware scanning and IM and application control are rudimentary.
- SurfControl has been using dynamic classification, but this has led to reports of false positives. SurfControl has not yet incorporated URL reputation, although it has some of that capability in early form from the BlackSpider Technologies' Web security service.
- SurfControl has expanded its coverage of delivery models, but its Windows appliance caters to the SMB market, and BlackSpider has struggled to gain traction in the United States.
- SurfControl does not have cross-protocol outbound DLP capability, although its outbound e-mail content functionality is mature and feature-rich.
- The proposed acquisition of SurfControl by Websense will give SurfControl DLP functionality. However, there are significant risks posed by the proposed acquisition.

### Trend Micro Strengths

- Trend Micro historically has had a strong reputation for scalable gateway anti-spyware protection; the InterScan Web Security Suite (IWSS) has been used for several years by enterprises for anti-spyware protection.
- Trend Micro has made improvements in the quality of its URL filtering database, and it has recently added URL reputation data and more IM and application control functionality.
- Trend Micro also has active content inspection and database capabilities.
- Trend Micro does have some outbound content filtering functionality with its eManager and InterScan Messaging Security e-mail security products.
- IWSS currently addresses much of the SWG functionality required by enterprises, even if it is not best-of-breed for each category, especially for existing customers that can take advantage of a suite license.

### Cautions

- Like other desktop antivirus vendors in the SWG market (for example, CA, Sophos, McAfee), the primary challenge is demonstrating significant diversity between client and gateway malware detection techniques, such that malware detection rates are increased, rather than malware simply being caught in a different location.
- Despite its early lead in the gateway market, Trend Micro has also been slow at adapting to changing customer requirements for new delivery models, such as appliances, leaving room for SWG specialists to steal market share.
- Although Trend Micro is one of the few anti-spyware vendors to scale to enterprise requirements, users report it requires significant hardware investments.
- Despite having an e-mail security solution, Trend Micro does not have cross-protocol DLP capabilities for enterprise customers, which will become a more important functionality for this market.

### Websense Strengths

- Websense is a standout leader in the traditional URL filtering market, with approximately 50% (by revenue) enterprise market share in 2005, but the company has been frustratingly slow to respond to the converging requirements of the SWG market.
- Websense Security Labs, which is responsible for detecting numerous zero-day threats, is a significant resource that is not well-known, even by Websense customers.
- Websense is finally poised to break into the SWG Leaders quadrant with its recent licensing of Inktomi's proxy software, which will form the nucleus of a new, appliance-based SWG solution.
- Websense has ported the Inktomi code to a Crossbeam appliance and will market the solution (named the Content Gateway) initially to organizations with up to 5,000 Internet users. Scalability will be improved in the third quarter of 2007, when Websense ports to a blade chassis Crossbeam appliance.
- The proxy functionality is a prerequisite for Websense to get the ability to control the inbound inspection of content for malware and richer application control.
- We expect that Websense will add capabilities developed by its Security Labs for real-time inspection of malicious Web content to detect zero-day threats.
- Websense is also making an aggressive attempt to move beyond its Web focus with its acquisition of PortAuthority and its intent to acquire SurfControl. The acquisition of PortAuthority gives Websense best-of-breed DLP technology. The planned acquisition of SurfControl will give Websense an e-mail security product (although one that is not generally considered best-of-breed) and e-mail and SWG managed services capabilities from BlackSpider. The SurfControl acquisition will effectively double the Websense installed base, providing a rich target market for its new SWG appliance.

## Cautions

- Websense faces a number of business challenges and execution; the next 12 months will be critical.
- The SurfControl acquisition, which is still subject to regulatory and stockholder approvals, is risky and could prove distracting. Converting SurfControl's URL filtering customers will likely be a challenge for Websense. SurfControl won many of its customer deals because it offered similar functionality at lower cost. With low switching barriers and increasing embedded URL filtering in SWG products, it is not clear that these customers will automatically renew with Websense.
- The PortAuthority acquisition puts Websense in a new, unfamiliar market with new enterprise buyers. While there are significant advantages to converging DLP with e-mail and Web gateways, realizing them will require considerable integration work across three different product lines from three different development groups.
- Websense's plans for the Inktomi proxy software are good on paper but yet to be proved in a demanding enterprise market. Although the Inktomi proxy was a proven product in terms of performance and scalability – it was at the core of AOL's and

other large ISP networks – it was never a big hit in the enterprise market and has seen little feature development in the past five years. Websense will have to rapidly mature this product and add new capability to move into the SWG Leaders quadrant.

## Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

## Evaluation Criteria Definitions

### Ability to Execute

**Product/Service:** Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

**Overall Viability (Business Unit, Financial, Strategy, Organization):** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

**Market Responsiveness and Track Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

### Completeness of Vision

**Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

**Offering (Product) Strategy:** The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

**Business Model:** The soundness and logic of the vendor's underlying business proposition.

**Vertical/Industry Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

**Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

**Geographic Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.