

E-Mail Hygiene Vendor Comparison

Content & Collaboration Strategies

Matt Cain

FOCAL POINT

Since 2001, the market for e-mail hygiene services has exploded, with larger vendors ramping up spending — in both R&D and via acquisitions — and with smaller vendors attracting hundreds of millions of dollars in venture capital funding. All this activity has resulted in an incredibly dynamic market, with each vendor clamoring for attention and fiercely competing for customers. This early-stage market now comprises more than 60 vendors, with each claiming competitive advantage over the others. Although most of the initial investment was related to spam filtering, vendors are rapidly expanding into peripheral areas such as secure e-mail, content filtering, regulatory compliance, and secure browser access to mail. All this adds up to a complex and confusing vendor marketplace. In this Practice, we explain some of the more salient points for evaluating e-mail hygiene vendors, including a comparative table of a dozen of the leading vendors (see the Addendum), plus the results of an extensive vendor survey broken up into three major categories: corporate comparisons, product functionality, and platform specifics (see Figures 1, 2, and 3).

CONTEXT

Threats to enterprise e-mail systems are increasing every day. Viruses are more sophisticated and have increasingly destructive payloads, and spam volume continues to rise — it now comprises up to 70% of inbound SMTP traffic at some organizations. Phishing attacks designed to lure users to disclose confidential information are accelerating, and port 25 vulnerabilities — denial-of-service attacks, dictionary harvest attacks, and mail floods — are widely used by hackers and spammers. At the same time, demand is rapidly growing for e-mail content control, whether for inbound and outbound filtering of offensive material or for unauthorized disclosure of corporate intellectual property. Increased e-mail regulations are also a growing concern: HIPAA, SEC, GLB, and other regulations variously mandate encrypted e-mail and archiving or human review of messages. All this activity means that companies must take a fresh look at e-mail hygiene to ensure that mission-critical e-mail systems are stable, secure, and in compliance with appropriate regulations.

Vendor Landscape

Results from the first part of our survey (included in the Addendum) showed the broad range of participants in this market — ranging from large antivirus vendors such as Trend Micro, Sophos (which acquired Active State), and Symantec (which recently acquired Brightmail and TurnTide), to well-funded venture capital-driven companies (e.g., Proofpoint, MessageGate, MailFrontier, IronPort). These vendors are joined by more established smaller vendors (e.g., Tumbleweed, CipherTrust, ZixCorp, BorderWare). The one participant that does not fit into an established category is firewall supplier CyberGuard. It acquired the German spam-blocking vendor WebWasher, which represents a trend we expect to continue as firewall vendors recognize the opportunity to push into the port 25 hygiene market. (BorderWare has roots in the firewall market.)

We expect vast turmoil in the vendor market as companies exhaust venture capital funding and engage in ferocious merger and acquisition activity. By 2007, we believe the vendor landscape will be quite different from its current state, with the 60+ vendors in the space winnowed down to 10 or so primary suppliers. Microsoft, with its Exchange Server Edge Services product, due for release in mid-2005, has steep ambitions here, though initially the product will be primarily an SMTP mail relay. However, buyers cannot afford to wait for market consolidation — mail hygiene issues loom large today and demand immediate resolution.

META Trend: As ad hoc electronic communication grows in importance (e.g., e-mail, instant messaging, Web conferencing), organizations will be challenged to create a hygienic and low-cost infrastructure. Through 2006, special attention will be focused on spam blocking and policy enforcement (e.g., regulatory compliance). By 2007, rising electronic communication volumes will frustrate users coping with information overload and drive organizations to employ common filters, queuing services, and categorization engines to ease communication burdens.

A quick look at the vendor channels and partner programs indicates a complex web of relationships. Some vendors, such as BorderWare and IronPort, rely on Symantec for an optional spam verdict engine. Others are engaging in technology partnerships to expand their functionality footprint (e.g., CipherTrust with Voltage, PostX for secure mail). Other vendors have more unique partnerships, such as MailFrontier's coupling with Cyveillance for additional threat, fraud, and security monitoring services. Some vendors, such as Sophos, have opted to go it alone and eschew partnerships. With the exception of the antivirus players, all vendors in the survey rely on outside help for antivirus protection. But we expect this complexity of these relationships to increase, as mail hygiene vendors consider further broadening of their footprints through forays into mail archiving, regulatory compliance, and instant messaging. Our survey also underscores the vast distribution channels at work. About half of the vendors generate most of their revenues through direct sales (e.g., Tumbleweed, IronPort, MailFrontier, Sophos, Proofpoint), with the remaining vendors relying heavily on indirect sales.

When evaluating various vendors, we established 12 criteria that we believe show the most obvious differences between suppliers. We did not include spam capture and false positive rates, because all vendors surveyed claim at least a 95% capture rate with relatively low false positive rates (see the Addendum for specific data). Our criteria follow the large-grained categories reflected in the in-depth data contained in the Addendum.

Corporate Comparisons

Company Size

Although company size is no guarantee of product quality, it does have many other implications. Typically, the larger the company, the greater the market staying power, since larger vendors have the ability to subsidize losses in one product segment with more successful product lines, therefore making them less vulnerable to market cycles. Typically, larger vendors also have more diversified distribution channels and readier access to research and development funding, as well as access to acquisition capital. In addition, these firms have the ability to tie peripheral product markets, such as Web and instant messaging filtering, for example, into one common platform. We also looked at number of employees and profitability. As suggested above, we expect this market to rapidly consolidate down to fewer than a dozen suppliers during the next several years. Therefore, we believe there is a strong correlation between the size of a vendor and the likelihood that it will be acquired (e.g., the smaller the vendor, the more likely it will be acquired).

Installed Base

Installed base becomes important for a variety of reasons. Larger installed bases typically indicate a longer presence in the market, effective distribution channels, and, in many cases (but not all), a well-received product. Larger installed bases also mean a broader supply of customer feedback, which can be parlayed into new releases that better reflect critical customer input. One growing area of interest is the volume of messages filtered by the vendor. It seems clear that vendors scanning larger volumes of mail have the opportunity to glean data that can be mined for more effective blocking of spam and viruses. For example, vendors are now correlating sending histories (e.g., always clean mail, mostly spam) with domains and IP addresses and using that data as part of the overall spam-blocking strategy. Similarly, vendors are analyzing virus outbreak patterns (e.g., unusual volumes from specific domains, common characteristics of messages) to identify (and block) viruses prior to signature downloads from antivirus suppliers. We tended to favor enterprise seats over ISP seats.

Geographic Reach

With the exception of Trend Micro (Japan), Sophos (UK), and BorderWare (Canada), all of the survey participants are American vendors. With the exception of BorderWare, Trend Micro, and CyberGuard, survey participants generate more than 50% of their revenues from North American sales. We expect these vendors to ramp up investment in Asia Pacific and EMEA as demand for mail hygiene services accelerates in these regions and as they look for new market opportunities. Most of these other vendors are rapidly opening offices in other continents and actively seeking local distribution partners. Since international sales often require local language support, many of the suppliers are actively adding additional language support, particularly for end-user controls. Many of the verdict engines, however, are language-agnostic and are able to filter spam in various languages. For scoring in this category, we factored in revenue mix across geographies, breadth of local support, and support for languages other than English. The category of geographic reach will become more important as customers consider deployment of common mail hygiene services across the globe.

Product Functionality

Spam Blocking

For most customers, the driving force behind increased mail hygiene investments is the need to combat ever-increasing volumes of spam. But as noted above, there is general parity at the blocking level, since most vendors deliver a relatively consistent set of spam-blocking services (e.g., heuristics, Bayesian filters, header analysis, signatures, URL scanning). False positive rates (i.e., numbers of legitimate messages incorrectly identified as spam) are relatively consistent, ranging from a ratio of 1:10,000 to 1:1,000,000. For this category, we also looked at connection-level checks. These are valuable, since connection with the alleged spammer is dropped before mail is delivered, resulting in a lower volume of spam that actually must be interrogated using the spam-cocktail approach. Also valuable is real-time lookup of each message against a variety of data, such as source address and DCC signatures. Our focus was not on overall accuracy rates (though that data is reported in the survey), but on completeness of the solution, since we did not establish a test bed to validate accuracy claims. In this category, we also examine the variety of disposition options available once spam is identified (e.g., quarantine, stamp as suspected spam, forward to user, delete).

Virus Blocking

Most of the vendors rely on third-party virus signature suppliers for the bulk of their virus defense. We gave higher scores to suppliers that offered multiple choices for signature vendors. But the big differences in virus-blocking capabilities come from activities not related to signatures, such as the ability to quarantine viruses based on behavior or other attributes prior to a signature download. Other elements include the ability to filter according to file, content/subject, or extension type, as well as the ability to filter outbound mail flows with the same capability of inbound services.

Message Transfer Agent/Anomaly Detection

The message transfer agent (MTA), or mail relay, has taken on increased significance as threats on the Internet increase and volume of mail rapidly accelerates. We believe the MTA will be a tremendous source of innovation as vendors strive to add scalability and SMTP connection-level logic, such as anomaly detection. Most of the vendors surveyed bundle or assume a standard SMTP engine such as postfix, sendmail, or the SMTP services of Windows. In most cases, we gave higher scores to vendors that had a proprietary MTA, due to richer feature sets, though in some cases, proprietary services resulted in lower scores due to lack of functionality. Scores were also higher for vendors that had added custom features to open-source MTAs. We purposely did not explicitly rank vendors based on MTA performance, due to extreme variability in how vendors calculate performance (e.g., differences regarding message size, differences in what interrogation features are turned on).

Anomaly detection (generally a function of the MTA) is very much like the firewall service of e-mail hygiene. Desirable features here are the ability to block common hacker denial-of-service attacks such as mail floods and buffer overload attacks as well as benign but still destabilizing events such as mail list or out-of-office loop detection. We also like to see protection against dictionary harvest attacks — where spammers bombard the relay with indiscriminate names to identify legitimate e-mail addresses at that domain. We also recommend the ability to stop any malformed messages. Furthermore, the hygiene server must be able to apply these policies during the SMTP conversation for early deletion, in addition to blocking based on IP or SMTP envelope information.

Secure Mail

The ability to encrypt messages for mailing over the Internet is become increasingly important, particularly in the healthcare (including pharmaceutical), financial services (including insurance), and government sectors. In assessing this category, we looked for a variety of services. We like to see rich, native secure mail facilities, spanning the gamut from Web delivery of the message, to S/MIME encryption, to support for server-to-server TLS encryption. We also believe it is important to give customers options to encrypt messages at the gateway based on keywords and phrases and also to allow users to declare when a message should be encrypted. Optimally, all these encryption services should be encompassed in a flexible policy engine that allows encryption by domain, sender, or groups of users. However, many vendors rely on partners to provide their secure mail capabilities, often using their native content-filtering technology to kick a message over to the third-party secure mail engine for encryption. Also in this category, we included the ability to provide a secure connection for browser users of IBM Domino and Microsoft Exchange, as well as the ability to filter messages

coming over various ports, including port 80, IMAP, and POP. We scored vendors with native secure mail capabilities higher than those with partner-supplied secure mail services.

Content Filtering

Content filtering has become increasingly important for overall mail hygiene strategies on both the inbound and the outbound side of port 25. On the inbound side, companies are routinely scanning for non-spam offensive content (offensive language, offensive images). On the outbound side, companies are scanning for proprietary intellectual property as well as offensive content. We like to see prepopulated lexicons for fast deployment, along with the ability for administrators to customize filters. Filters should be able to be applied to headers, the body, and attachments (both attachment type and attachment content). All filtering should be able to be applied to inbound and outbound streams, with different policies for each. In this category, we also included support for various e-mail regulations (e.g., SEC, GLB) and looked for specific content-filtering capabilities for each of the listed regulations. A wide range of disposition options for filtered content is also desirable.

End-User Controls

Perhaps the worst consequence of the spam blight is false positives — that is, messages that are blocked as spam but actually are legitimate e-mail. Since every spam-blocking system will generate false positives, the real issue is one of how to minimize their impact. Therefore, we advocate a system where users have access to quarantined messages, whether through a daily digest or a personal Web mailbox. In this way, users can scan the quarantine if they suspect a message may have been falsely blocked. We also advocate an end-user controlled white list, whereby users can add an address or a domain to a list, thereby allowing those messages to pass through the spam filter unmolested. This is important for volume mail that may have many characteristics of spam (e.g., newsletters) but the user nonetheless wants to receive it. We also like to see end users have some control over how policy is set and to have all services apply to any e-mail aliases the user has. Lastly, we believe administrators should have to the ability to turn on or off any of these features, and substitute a corporatewide policy for all users.

Platform Specifics

Management

Strong management capabilities result in increased control and visibility into mail hygiene services as well as reduced operational overhead. In this section, we looked at the availability of GUI and CLI interfaces, granular and delegated access to the management console, centralized administration and management across multiple machines, and the ability to export logs. Multiple directory support and automated directory update capabilities are important. We also looked for secure connections for system updates and alerts, as well as SNMP facilities for tying into larger management consoles. Finally, we looked for cluster support as well as automatic synchronization of policy and content across multiple servers plus failover and high-availability options.

Reporting

Well-run mail systems will increasingly need access to various reports on mail hygiene activities. We like to see maximum flexibility in the reporting capabilities of any product. In most cases, customers need access to raw statistics on the number of messages processed, plus the percentage of messages tagged as spam or as having viruses. Other data for troubleshooting hygiene services includes:

- Top recipients of spam and viruses
- Top virus types
- Policy compliance reports
- Top reasons for message quarantines

We also prefer to see traffic data stored in a database for flexible reporting as well as the ability to send reports via e-mail. Finally, we examined the total number of reports available as well as the ability to aggregate reports from multiple servers in addition to automatic report generation. We gave higher scores to vendors that supported multiple industry-standard databases.

Price

We made a best effort to normalize pricing across all vendors and assumed a three-year ownership period. For the rankings, we chose to look at pricing for 10,000 users (though the survey in the Addendum also

includes data on 5,000 users). Where both software load and appliance form factors were available, we chose the appliance. The lower the price, the higher the ranking. Normalization included adding, for example, the additional cost of virus signatures and spam update services. Of course, vendor pricing is subject to various factors, including competitive environment, time of year, and revenue targets. Prices are assumed to be list price. Street prices are typically 20%-30% lower than list prices.

About This Study

All the rankings in this study were compiled directly from responses to an extensive questionnaire, the results of which are included in the Addendum. Survey responses were edited by META Group for brevity. All answers from vendors were assumed to be true, though in some cases META Group asked vendors to clarify answers. Some vendors chose not to answer some questions because that data was deemed confidential. In cases where the information was not forthcoming, we made an informed estimate. Although some vendors chose to answer questions with information about future releases, we only considered answers for currently shipping products. In the spreadsheet, "NA" variably stands for "No Answer" or "Not Applicable." All vendors had an opportunity to review and comment on the study before publication, though some vendors disagree with our conclusions. Methodologies for rankings are detailed above. Vendors are listed in alphabetical order.

Pricing was exceedingly difficult to normalize due to different bundling options of management consoles, virus protection, update services, etc. The ranking represents our best estimate for volume purchases, but we encourage readers to obtain actual quotes as part of their research. Street discounts, time of year, sales compensation, etc. can all greatly impact actual pricing. We purposely did not provide a sum in the chart as an encouragement to readers to weigh categories and more closely reflect their specific needs (e.g., geographic reach may be unimportant, yet secure mail and content filtering may be essential). We also note that the survey goes far beyond the 12 categories on which the vendors were assessed. Readers should examine the actual survey results to attain a much more complete picture of the capabilities of the vendors. Vendors are comparatively ranked on a scale of 0-5, with 5 being the highest. BorderWare requested that its survey responses not be published, but it will supply the survey information upon request.

Bottom Line

Given increasing threats, users must upgrade their mail hygiene capabilities. A thorough evaluation of mail hygiene vendors — with a focus on matching business needs with supplier competencies — is critical to providing maximum e-mail protection and functionality.

Business Impact: It is essential that enterprises establish a comprehensive approach to e-mail hygiene in order to protect the overall health of corporate communications.

Figure 1 — E-Mail Hygiene Vendor Comparison 2H04: Corporate Specifics

<u>Vendor</u>	<u>Corporate Specifics</u>		
	<i>Company Size</i>	<i>Installed Base</i>	<i>Geographic Reach</i>
BorderWare	2.5	2.5	3.5
CipherTrust	3.5	3.5	3
CyberGuard	3.5	2.5	3
IronPort	3	3	3.5
MailFrontier	1.5	1.5	2.5
MessageGate	1	1	2
Proofpoint	2.5	1.5	2.5
Sophos	4	4	4
Symantec	5	4.5	5
Trend Micro	4.5	5	4.5
Tumbleweed	3	3	2
ZixCorp	2	1.5	2.5

Source: META Group

Figure 2 — E-Mail Hygiene Vendor Comparison 2H04: Product Functionality

<u>Vendor</u>	<u>Product Functionality</u>					
	<i>Spam Blocking</i>	<i>Virus Blocking</i>	<i>MTA/ Anomaly</i>	<i>Secure Mail</i>	<i>Content Filtering</i>	<i>End-User Controls</i>
BorderWare	4	4.5	4	3.5	3	5
CipherTrust	4.5	5	4	4.5	4.5	4
CyberGuard	4.0	4	3	0	4.5	2
IronPort	5	5	5	4	3.5	4
MailFrontier	5	4.5	4	1	2.5	5
MessageGate	4	4	3.5	3	5	2
Proofpoint	4.5	4.5	4	3.5	3	5
Sophos	4.5	5	4	0	3.5	5
Symantec	4.5	4.5	3.5	3.5	2.5	5
Trend Micro	4	5	3	0	3.5	1
Tumbleweed	4.5	4.5	4	5	5	4
ZixCorp	3.5	4.5	2	4.5	5	1.5

Source: META Group

Figure 3 — E-Mail Hygiene Vendor Comparison 2H04: Platform Specifics

<u>Vendor</u>	<u>Platform Specifics</u>		
	<i>Mgmt.</i>	<i>Reporting</i>	<i>Price</i>
BorderWare	4.5	4.5	5
CipherTrust	4.0	3	3.5
CyberGuard	3.5	5	4
IronPort	4.5	3.5	3
MailFrontier	4	3	3.5
MessageGate	3	4.5	4.5
Proofpoint	5	3.5	2.5
Sophos	3	2.5	3
Symantec	4	3.5	1
Trend Micro	1	1.5	1.5
Tumbleweed	4	4	3.5
ZixCorp	3	4	2.5

Source: META Group

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
	Corporate Level												
1	What is the company name?	*	Trend Micro, Inc.	CyberGuard Corp.	Zix Corporation or "ZixCorp"	Tumbleweed Communications	IronPort Systems, Inc.	MessageGate	CipherTrust, Inc.	MailFrontier, Inc.	Symantec	Sophos Plc	Proofpoint, Inc.
2	Where is the company headquartered (city, state)?	*	Tokyo, Japan	Ft. Lauderdale, FL.	Dallas, Texas	Redwood City, CA	San Bruno, CA	Bellevue, WA	Alpharetta, GA	Palo Alto, California	Cupertino, California	Abingdon, UK	Cupertino, CA
3	When was the company founded?	*	1988	1996	1988	1993	2000	2003	2000	2002	1982	1985	2002
4	How much funding has the company received to date (in \$s)?	*	NASDAQ: market cap of \$5.95B	NASDAQ market cap of \$169M	NASDAQ market cap of \$153M	NASDAQ:market cap of \$106M	\$48M	NA	\$42M	\$23M	NASDAQ market cap of \$16.2B	\$0	\$36M
5	If private, how many rounds of funding has the company been through?	*	NA	\$8.5M to build WebWasher, acquired by CyberGuard in April 2004	NA	NA	3	NA	1	3	NA	NA	NA
6	How many employees does the company have?	*	2000+	250	285	250	200	<100	170	70	5,500	848	100
7	What is the approximate 2004 revenue (mail hygiene derived revenue only)?	*	~\$70M	NA	\$15M	Total company revenue is about \$40M	NA	NA	\$60M	NA	Multi-hundred-million-dollar business.	\$13M in bookings for gateway products for y/e 31/03/2004	NA
8	What is the approximate spending on R&D for e-mail hygiene for 2004 (in \$s)?	*	~\$8.5M	NA	\$10.4M	\$9M	NA	NA	NA	NA	NA	NA	NA
9	What % of revenue is derived from professional services?	*	0%	NA	NA	\$11.5M	NA	NA	3.80%	NA	None.	<1%	NA
10	What % of total revenues are generated through:	*	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived	% Revenue derived
	Direct channels	*	5%	0%	70%	90%	70%	NA	2003: 61%; 2004 projected: 40%	65%	NA	72%	70%
	Indirect channels (VARs, distributors, resellers)	*	95%	100%	30%	10%	30%	NA	2003: 39%; 2004 projected: 60%	35%	NA	28%	30%
11	What was your total profit/loss in 2003?	*	Profit \$87.3M	\$47.8M revenues, \$7.9M pro-forma net income	Net loss of \$27.5M	Net loss of \$9.2M	NA	NA	NA	NA	FY 2004's profit was \$370M	NA	NA
12	Who are your 3 largest indirect channel partners based on volume?	*	Partner	Partner	Partner	Partner	Partner	Partner	Partner	Partner	Partner	Partner	Partner
	1	*	Software Spectrum (NA)	Network Appliance	Symquest	Zones	Milestone Systems	NA	NBG/Forsythe	CDW	NA	ACT	"8e6"
	2	*	AMPEG Technologies und Nectarine (EMEA)	Computerlinks, France	PC Solutions	Software House International (SHI)	Accudata	NA	Fishnet	GTSI	NA	Networking Technology	PlanetGov
	3	*	Softbank (JP)	Snaiso, France	Emtec Inc.	Software Spectrum	TruNorth Solutions	NA	Notch	Conquest	NA	Trebron	CPTech

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
13	What OEM partners and technology supplied by the partner exist?	*	Postini-anti-spam engine in Spam Prevention Solution	Mailshell (add'l. spam filtering method), Akonix (Instant message filtering)	Mail filters for anti-spam signatures	McAfee for virus	Symantec Brightmail Anti-Spam, Sophos Anti-Virus, PGP Secure Messaging	Verity - Document Cracking	Voltage - secure e-mail; PostX - secure e-mail; McAfee, Sophos, Authentium - anti-virus	Anti-virus - McAfee Web Data Feed - Cyveillance	None.	None	Anti-Virus – MacAfee, F-secure Secure mail – Sigaba, PGP (No release) Content filtering – Verity
14	What OEM partners resell or "private label" your product?	*	None	None	None	None	None	NA	None	None.	BorderWare, IronPort and BT Syntegra	14 AV OEMs	None
15	Who are your top 3 strategic partners	*	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>	<i>Top 3 and reason</i>
	1	*	Cisco	Network Appliance	Our top 3 partners are listed in response to Question 12.	McAfee for anti-virus (AV)	Symantec Brightmail	Sun - Strong IT Value Proposition	Equip - EMEA distribution partner	McAfee	IBM Global Solutions	Resale agreement with Sun	Sigaba – to provide anti-spam capabilities to its customers
	2	*	Microsoft	Mailshell (OEM-ing important, leading edge spam signature database from them)	—	Kaspersky for A/V	Sophos; second highest percentage of customers purchase this option	EDS - Strong Technology/Services Value Proposition	PostX - large enterprise encryption partnership	Cyveillance's threat, fraud, and security risk monitoring services for the open Internet.	Perimeter Security Value Added Reseller Channel	Sophos has certified PureMessage as Novell Yes Certified for SUSE Linux	NA
	3	*	IBM	McAfee for AV	—	Verity for attachment decomposition	Dell Computer; each IronPort product is built on this platform	MSFT - Dominant mail server & collaboration solution for large enterprise	NA	Sygate ensures MailFrontier anti-fraud software is always current and operationally sound	EDS because of its reach into high-end enterprise accounts.	Microsoft Partner Program	NA
16	Who are your 3 largest enterprise customers?	*	<i>Largest customers</i>	<i>Largest customers</i>		<i>Largest customers</i>	<i>Largest customers</i>	<i>Largest customers</i>	<i>Largest customers</i>	<i>Largest customers</i>	<i>Largest customers</i>	<i>Largest customers</i>	<i>Largest customers</i>
	1	*	400,000 seats	T-Online	Insurance - Message Inspector & Encrypted Messaging solution - 40,000 users	American Express	Cisco Systems	Boeing	Wal-Mart	AG Edwards	Several of the top Fortune 10	NA	Wells Fargo Bank
	2	*	390,000 seats	France Telecom	Insurance - Encrypted Messaging - 30,000 users	ChevronTexaco	Viacom	Lockheed Martin	Coca-Cola	NBC Universal	NA	NA	Kaiser Permanente
	3	*	119,000 seats	Large Bank	Pharma - Message Inspector - 50,000 users	Verizon, Wal Mart, DoD tied	Prudential	The Tribune Company	(virtual tie) Washington Mutual and JP Morgan Chase	SAP	NA	NA	MCI
17	What is your total number of enterprise e-mail hygiene customers?	*	In the past year 8,389 for IMSS and 3,374 for SPS. No access to data prior to Sept 2003	50+	2,300	700+ (30% of the Fortune 500)	>500	NA	>1,000	700	It is in the tens of thousands of customers.	~810	110

* BorderWare requested its survey responses not be published, but will supply the survey information upon request

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
18	What is the total number of enterprise e-mail hygiene end user seats?	*	19.6M seats sold between Q203-Q204 (ISPs and enterprise)	3,000,000+	1.5M	> 10M	>5,000,000	NA	>7M	NA	It is greater than 10M	~8.6M	1,000,000+
19	What is the total number of ISP customers?	*	Prodigy/Telmex: SPS and IMSS for 1.5M users.	10+	None	5	>10	NA	2	NA	Over 300	43	1 (not our target)
20	What is the total number of ISP end user seats?	*	NA	3,000,000	None	< 1M	> 100,000,000	NA	< 250,000	NA	Over 300M	NA	10,000
21	If appliance, what is the total units shipped?	*	NA	NA	MI does not exceed 100. Encryption exceeds 500.	NA	>1500	NA	>1850	General Availability of MailFrontier Appliance v1.2: 8/23/2004	NA	NA	Appliances comprise 45% of new Proofpoint customers
22	What percentage of total revenue is derived from the following geographies?	*	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue	% of Revenue
	North America	*	Based on IMSS/SPS revenue only: 46%	NA	90%	95%	75%	100%	91%	95%	55% (companywide)	72%	90%
	EMEA	*	Based on IMSS/SPS revenue only: 41%	NA	10%	2%	15%		9%	3%	30% (companywide)	24%	10%
	Asia Pacific	*	Based on IMSS/SPS revenue only: 13%	NA	Less than 1%	3%	10%		Opening Asia Pacific next month	2%	15% (companywide)	4%	0%
23	What is the average size (by seats) of enterprise customers?	*	90% are over 1,000 seats.	5,000 users	2,500 to 5,000 seats	10,000	8,000	50,000	7,500	NA	<1,000 seats.	~10,600	10,000
24	Where do you have sales offices outside of the US (please exclude indirect channels)?	*	Tokyo, Taipei, Shanghai, Buenos Aires, Munich, Marlow, UK, Paris, Manila	Germany, UK, France, Switzerland, Japan	Canada & EMEA	Hurst, Berkshire, England.	Canada, Mexico, Brazil, UK, France, Germany, Italy, Japan, Korea, Malaysia, China, Hong Kong, Australia, New Zealand	NA	Toronto; London; Amsterdam; Paris; opening Latin America and Asia Pacific next month	None.	Several dozen sales offices in Europe, the Middle East, Asia, Africa and the Americas.	Vancouver, Canada; Abingdon, UK; Frankfurt, Germany; Milan, Italy; Paris, France; Singapore; Sydney, Australia; Tokyo, Japan	UK, Holland
25	What version number of the product is under review? If multiple products, please list all that apply.	*	InterScan Messaging Security Suite 5.5 and Spam Prevention Solution 2.0	WebWasher Anti Spam 5.0 (software only solution), WW 1000 (appliance solution)	Message Inspector 4.3, Feb. 2004; Message Inspector 4.3.1.a, AS appliance, March 2004; ZixVPM 2.1, 2H03; ZixMail 1.8.105, Jan 2004	Email Firewall 6.0 MailGate Edge 1.0	AsynCOS 4.0	3.1	4.5	MailFrontier Enterprise Gateway™ v3.1 MailFrontier Appliance™ v1.2	Symantec Brightmail AntiSpam	Pure Message 4.6.1	2.5

* BorderWare requested its survey responses not be published, but will supply the survey information upon request

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
26	Please list the date(s) this version(s) went GA.	*	November 2003 for both	Apr-04	See above	Email Firewall 6.0 8/4/2004 MailGate Edge 1.0 9/22/2004	May-04	Apr-04	July 26, 2004 (controlled release)	MailFrontier Enterprise Gateway v3.1 (August 2004) MailFrontier Appliance v1.0 (August 2004)	June 30th, 2004	Shipped July 13, 2004	July 30th
27	When was the original version of the product first shipped?	*	IMSS 5.5 is the first version of the product that integrated with SPS. SPS 1.0 began shipping in March 03.	WebWasher Anti Spam (May 2003), WW 1000 (Sept. 2004)	Message Inspector: April 1999. Message Inspector appliance, Jan. 2004, ZixVPM, Sept. 2001, ZixMail 2H99	1997	Jul-01	Internally deployed in 2001 at Boeing	Dec-01	MailFrontier Enterprise Gateway (formerly MailFrontier Anti-Spam Gateway - February 2003)	1998	PerIMx 1.0 shipped December 2000	Spring of 2003
Technical Support & Maintenance		*											
28	What is the length of warranty/maintenance?	*	1 year	Minimum 6 months	Maintenance is for the duration of the contract for which the customer signs.	20% of list/year. Gold minimum of \$6,000/year) is 20% of list/year. Platinum (minimum of \$10,000/year) 30% of list/year.	Annual maintenance contracts	12 months	Standard is 1 year, but we sell up to 3 years	Maintenance is purchased on an annual subscription basis.	The product is per year subscription basis. This includes maintenance.	sold in yearly increments	Life of contract
29	What are the support hours?	*	8-5 telephone support, 24X7 online/e-mail support is free. 24X7 access to a technical account manager for fees.	7x24	Standard support 5x12. Emergency support for severe problems.	Bronze, Gold 12x5 Support. Platinum 24x7	24x7	24x7	24x7	Standard Support: Monday-Friday, 6 AM - 6 PM PT Premium Support: 24x7x365	Symantec has 24x7 support.	24x7	8x5 or 24x7
30	Is global on-site service available (either directly or through third party)? If Yes, through whom?	*	Yes, through Trend Micro.	On request	Yes, through ZixCorp and partners	Daily phone or e-mail status updates for severe problems. A Tumbleweed engineer may be sent on-site.	Yes, IronPort	NA	Yes, through IBM Global Services	Yes, directly from MailFrontier or indirectly via our global channel partner network.	Symantec has global on-site service directly.	Yes - available directly through Sophos or provided by partners where Sophos resources are not available.	Yes, via Proofpoint
IP/Technology		*											
31	How many patents or patent filings are there around this technology?	*	0	NA	2	18 US patents. 23 utility patent applications pending. 19 patent applications pending in foreign jurisdictions.	There are 8 patents filed for IronPort technology	10	7	16	8 mail security patents form Brightmail plus some from Symantec	NA	2

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
	Product Functionality	*											
	Spam	*											
1	What is the average spam capture rate?	*	90%-95% (+/-2%)	>95%	95%+	95%+	>95%	99.93% Effective Rate; We block 84.5 % of total e-mail in the enterprise	98%	98%	95%	98%	96%
2	What is the average false positive rate?	*	0.02% - 5%	<1%	1 in 100,000	< 0.01%	1 in 1,000,000	0.0032	Anecdotal evidence: "one in a million"	0.01%	1 in 1M	NA	0.00%
3	What types of spam detection are used? (Please mark an "X" in all appropriate boxes.)	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Header analysis	*	X	X	X	X	X	X	X	X	X	X	X
	"Reputation" filter	*		No	X	X	X	X	X	X	X	X	X
	Heuristics	*	X	X	X	X	X	X	X	X	X	X	X
	URL library	*	IMSS (Non-dedicated, eManager) + IWSS	X		X	X	X	X	We also check zip codes and phone numbers against a 20M contact point database	X	X	Partial
	Content scanning	*	X	X	X	X	X	X	X	X	X	X	X
	Black list support	*	X	X	X	X	X	X	X	X	X	X	X
	Signatures	*	X	X	X	X	X	X	X	X	X	X	X
	Custom domain level black lists	*	X	X	X	X	X	X	X	X	X	X	X
3	Custom domain level white lists	*	X	X	X	X	X	X	X	X	X	X	X
	End user white lists	*	X	X (has to be configured by administrator)	X	X	X	Evaluating feasibility	X	X	X	X	X
	End user black lists	*		X (has to be configured by administrator)	X	X	X	Evaluating feasibility	X	X	X	X	X
	Keyword and phase lexicon	*	X	X	X	X	X	X	X	X	X	X	X
	Bulk mail checking	*	X	No	X	X	X	X	X	X	X	X	X
	Spam training module	*	X (Trend Labs tools, not product-based)	X (Trained by vendor)	X		X	X	x	X		X	X
	Bayesian filtering	*	x	X	X		X	X	x	X		X	
	Automatic or self-learning filters	*	IMSS 6	No	X	x	X		x	X		X	X
	Connection-level checks	*	Non-dedicated now	X	X	X	X	X	x	X	X	X	X
	Other - please specify	*	IMSS 6 to emphasize Support Vector Machine (SVM) technology over Bayesian methods	Habeas	Sender Validation (similar to reverse DNS)	X - auto categorization and tagging for processing by the policy engine	Unique reputation based rate limiting capability keeps suspicious mail from entering the network		Anomaly detection does traffic analysis to detect outbreak or flood type events.	Our SMART Network determines "real" people's response to "real" e-mail, both spam and legitimate.	Extensive Non-English spam technology and response capability.	Spammer Asset Tracking, Campaign Tracking, Genotype Analysis	Proofpoint MLX self-learning technology uses Logistical Regression and Support Vector Machines

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
4	Does the system do a real-time look-up on each message (Yes, No, or optional)?	*	No	No	Yes	Optional	Yes	Yes	Yes	Yes	Optional	Optional	No
5	What values are "looked up"?	*	NA	NA	Reverse DNS Lookup	SPF RBLs Reverse DNS Real-time LDAP for recipient verification/DHA defense	The connection IP is checked with IronPort SenderBase	Header, connection and URL	RBL, Reverse DNS, Statistical Lookup Service (SLS), TrustedSource	Messages looked up in our thumbprint database to determine if the message has been previously identified.	Compare to a DNS-based real-time blacklist.	Known spam DNS entries in DNSBLs (DNS blackhole lists)	NA
6	Does the system use an end-user quarantine or digest option?	*	x	X	No	Yes	Yes	End user quarantine	Yes	x	x	Both	Yes
7	Typically, how often are updates sent to the customer (i.e., every X min./hours/days)?	*	Signatures 2x or more (as needed) per day; heuristic rules bi-monthly, as relevant (IMSS 6.0 will transition to weekly heuristic updates or as needed basis)	configurable, spam patterns each hour, AV patterns each 5 minutes	This is configurable (variable) out of the box.	Anti-spam updates every hour AV pattern updates as needed	Spam updates: every 4 to 7 minutes, >30,000 new rules are written a day; Virus updates every 15 minutes; SenderBase updates occur in real time for every connection	Daily	When threats, new techniques, outbreaks, etc. necessitate	Every 5 minutes	Every 10 minutes.	Updates are released as required. The service that checks for updates can be configured to run as often as desired.	Spam – Weekly Virus – as needed
8	What information is updated (e.g., spam signatures, virus signatures, white lists, etc.)?	*	Spam signatures (IMSS 6 includes added white listing)	Spam signatures, Bayesian training data, body and header rules, heuristics, URL database, AV patterns and heuristics	Spam signatures, virus signatures, w/b Lists/, Lexicons: for (Regulatory Compliance) OS updates, URL signatures	Dynamic Anti-spam Service (DAS) updates; McAfee pattern and engine updates	Spam, Virus, Virus Outbreak, Reputation Scores	Spam and virus signatures	Threat Response Updates (TRU)	Spam signatures, Adversarial Bayesian updates, contact points, reputations, and virus signatures	Spam filters every 10 minutes, virus filters every hour.	Anti-spam rules, virus signatures, known spam URIs	Spam – statistical learning files (attributes/weights) Virus – Virus definitions
9	Is the price of the update service included in the core maintenance/ subscription service, or is there an additional fee?	*	included	included	Maintenance	DAS: extra; AV: included	Bundle pricing includes all updates, service and support	Included in core maintenance	Included	Included	Included.	No additional charge.	included
10	Are major product releases included in the core maintenance/ subscription service, or is there an additional fee?	*	Included	Extra fee, minor upgrades and fixes included in maintenance	Yes	Included	Yes, included in core maintenance	Determined on customer basis	Included	Included	All releases are included.	No additional charge.	Yes, included

* BorderWare requested its survey responses not be published, but will supply the survey information upon request

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
11	Please list all languages supported for foreign language spam filtering.	*	IMSS 5: English, Hispanic, primarily (+ multiple others for false positive resolution); IMSS 6 adds Japanese, Chinese, Korean, French, Spanish, German, Russian + more in-progress	All European languages, all major languages of the rest of the world	French, Spanish, German, Italian, Russian, Japanese and Chinese.	English, German, French, Spanish, Turkish, Russian, Japanese, Korean, Chinese	English, Dutch, French, German, Italian, Chinese, Japanese, Korean, Portuguese, Russian, Spanish	English	Language independent	User controls: Arabic, Baltic, Chinese, Cyrillic, Greek, Hebrew, Japanese, Korean, Thai, Turkish, Vietnamese; Authentication/Reputation and SMART Network are language independent. The Bayesian system is English.	Many of the technologies are language agnostic (such as reputation or URL filters). Other technologies: Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian and Spanish.	Language independent	German, Spanish, Italian, French
12	Are 100% of inbound functions available for outbound mail? If not, please indicate which features are unavailable.	*	Yes	X	Yes	Yes	Yes	Header analysis	Yes	No	Yes	Yes	Yes
13	List all alternative anti-spam technologies available with the product/service?	*	TMASE engine available Now w/ ISVV targeted for IMSS 6.	Habeas, Mailshell	Automated Signature updates,	No others.	None	NA	None	Tarpitting/quality of service functionality.	NA	Extensive customization of spam filtering and message handling	Proofpoint's MLX machine learning technology
Disposition options		*											
14	What disposition options are available? (Please mark an "X" in all appropriate boxes.)	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Delete	*	x	X	X	X	X	X	X	X	X	X	X
	Quarantine	*	x	X	X	X	X	X	X	X	X	X	X
	Tag as suspected spam and forward to user	*	x	X	X	X	X	X	X	X	X	X	X
14	Reject at IP connection time	*	X (Critical errors; predefined return codes)	No	X	X	X	X	X	X	If supported by MTA	X	X
	Reject vs. discard	*		X	X	X	X	X	X	X	If supported by MTA	X	X
	Other - please specify	*		Delay, return to sender, reroute, digest	Bounce (with or without message), forward to admin (or e-mail address), Block, Log, dump to file system.	Over 23 options including Return to sender, detain, defer, route to select relay, add recipients, custom annotate body, custom notification.	Send to alternate host, alternate recipient, archive, bounce, notify, CC, BCC	Trace, Queue for Review, auto reply, re-route, remove recipient, Quarantine, Hold, Carbon Copy, Append Subject line, add disclaimer, strip attachments	Reroute; Add header		Save to disk, subject line/header markup	Copy to quarantine and deliver, forward	Annotate message body; Add footer; Add recipients; Re-route/redirect; Reply to sender; Add/modify headers

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
15	Does the system have a configurable point scoring system for spam disposition?	*	x	Yes - system does not use points but probabilities	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16	Are the dispositions configurable at a group or user level?	*	x	Yes	Yes	Both	Yes	Group level	Both	Yes	Yes	Yes	Yes
17	Can end users manage this?	*	No	No	Yes	No	No	Quarantine only	No	Yes	In an upcoming version end users will be able to manage their own actions.	Yes	Yes
Virus													
18	Please list virus signature supplier(s).	*	Trend Micro	McAfee, Computer Associates	Sophos	McAfee	Sophos, IronPort	Sophos	Sophos, McAfee	McAfee	Symantec.	Sophos Anti-Virus only.	McAfee; F-Secure
19	Is virus protection part of the base platform or optional?	*	Yes	optional	Optional	Base	Optional	Option	Sophos, McAfee and Authentium are optional	A hybrid approach is available for an extra fee	Optional	Optional.	Optional
20	Are suspected viruses quarantined prior to signature download?	*	Yes	planned for next release 5.1 in October	Yes	Can be customized	Yes	Yes	Yes	Yes	No	Optional.	Yes
21	Are virus signatures updated direct from AV vendor or from spam vendor?	*	AV vendor	CyberGuard	Direct from AV vendor	A/V vendor	IronPort by default, optionally by Sophos	MessageGate	CipherTrust	MailFrontier	AV vendor.	Sophos.	Proofpoint
22	What other types of virus detection are in use? (Please mark an "X" in all appropriate boxes.)	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Attachment type filtering by extension	*	x	X	X	X	X	X	X	X	X	X	X
	Attachment type filtering by file checking	*	x	X	X	X	X	X	X	X	X	X	X
	Message content/subject	*	x	X	X (includes attachment content)	X	X	X	X	X	X	X	X
	Anomaly detection	*	x	No	X	X	X	X	X	X	X	X	X
	Outbreak detection	*	x	No	X	X	X	X	X	X	X	X	X
23	Are all of these functions available for outbound mail? If not, please indicate which features are not.	*	x	X	Yes	Yes	Yes	Yes	Yes	(left blank)	X	Yes, all of these functions are available for outbound mail.	All available.
MTA													
24	Is there a native MTA (SMTP relay)?	*	x	X	Yes	Yes	Yes	MTA not native, solution supports Sendmail, Sun one and MS Exchange Server 2000, 2003	Yes	Proxy only-- still requires independent MTA	No but works with Windows SMTP service, Sendmail, Postfix etc.	Sendmail or Postfix.	Yes

* BorderWare requested its survey responses not be published, but will supply the survey information upon request

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
25	If so, what MTA(s) is (are) it?	*	Windows, proprietary; Postfix (or any via inline hop)	Proprietary	Sendmail for Message Inspector, and PostFix for Encrypted Messaging	Proprietary	Custom MTA	NA	Proprietary	Assumes an upstream MTA	NA	Sendmail or Postfix.	Sendmail MTA
26	Is onboard DNS caching available?	*	X (Postfix, default; No Windows support)	No	Sendmail MTA provides this.	Yes	Yes	NA	Yes	Yes	NA	Yes	No
27	Is there overlapping message delivery for high-volume sustained delivery?	*	X (Postfix, default; No Windows support)	X	Yes	Yes	Yes	NA	Yes	Yes	NA	Yes	Yes
28	Is there address rewriting to support internal and external addressing, as well as internal host name shielding and support for virtual domains?	*	X (Postfix, default; No Windows support)	No	Yes	Yes	Yes	NA	Yes	Yes, but no support for Virtual domains	NA	Yes	Yes
29	Is there support for SMTP authentication via standard directories to enable privileged users (e.g., home, traveling users) to use relay services without opening the relay to indiscriminate use?	*	X (Postfix, default; IMSS 6.0 supported for Windows)	No	Yes	Yes	Yes	NA	Yes	NA	NA	Yes	Not currently
30	Is there load balancing and failover across multiple servers?	*	x	No	Yes	Yes, via DNS/MX	Via DNS	NA	Yes	Yes	NA	Yes	Yes
31	Is there load balancing and failover for queues across multiple servers (i.e., queue replication)?	*	IMSS 6 via configuration only; not by default	No	Yes	Yes, via SQL replication or DB clustering	No	NA	No	Not applicable; no queues in MailFrontier's SMTP relay	NA	Yes	No
32	Integration with third-party load balancers?	*		No	Yes	No explicit integration, but general compatibility	Yes	NA	Yes	Yes	NA	Yes	Yes
33	What is MTA throughput with all services enabled (anti-spam, anti-virus, content filtering) in messages/hour?	*	~100K (Depends on default hardware, user policy granularity, and content filtering complexity).	9 messages/sec on a single CPU system. Additional throughput on multiprocessor systems.	72,000 msgs/per hour	40K-200K, depending on hardware	175,000 MPH @ 15KB	NA	Approximately 35,000 messages per hour	160,000 messages per hour (3 Ghz Dual CPU)	NA	20 messages/sec	Software can scale to any level. Appliance P600 = 20,000 msgs/hour, Appliance P800 = 40,000 msgs/hour

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
34	Is there a graphical user interface to manage the system or is command-line knowledge required?	*	Primarily GUI w/ additional CLI support	Both, GUI and Command Line Interface are available.	Full GUI based	All GUI-based, except for private key import tool (CLI)	Yes	NA	All functions are managed through a GUI. There is also optional CLI support for some functions.	Graphical User Interface	NA	Sendmail can be configured through the Web-based PureMessage Manager.	GUI, command line available
	Regulatory Compliance	*											
35	Is there any specific (e.g., prepopulated lexicons, standard reports) support for the following? (Please mark an "X" in all appropriate boxes.)	*	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>	<i>"X" indicates support for this function</i>
	GLB	*		Product complies with GLB	X	X		X	X				
	HIPAA	*		Product complies with HIPAA	X	X		X	X				
	SEC	*		Product complies with SEC	X	X		X					
	NASD	*		Product complies with NASD	X	X		X					
	SOX	*		Product complies with SOX	X			X	X				
	Other - please specify	*		Product supports European Data Protection Directives 95/46/EC, 2002/58/EC	Intellectual Property, HR, Personal Finance, Profanity, General Healthcare PHI, Legal				Calif. 1386		Via content filters and group-based policies.	Can create lexicons.	
36	Does the solution offer archival services?	*	x	X	Yes	Yes	Yes	Support third-party archiving solutions	Yes, third parties	NA	NA	Yes	Yes - file system based archive
37	Does solution include searchable database for e-mail auditing purposes?	*	IMSS 5, limited via traffic logging/UI; IMSS 6 (Database-driven design; centralized index across all servers)	No	Yes	Yes	Yes	Yes	No, archiving is done off IronMail. Quarantine queues are searchable but intended for short term use	Yes	NA	Yes	Yes

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
	Secure Browser Access Protection for E-Mail Services	*											
38	Is there secure browser access protection for the following e-mail services? (Please mark an "X" in all appropriate boxes.)	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Domino Web Access or iNotes	*	No	No	X			On road map	X			Yes	
	OWA	*	No	No	X			On road map	X			Yes	
	Secure WebMail	*	No	No	X			On road map	X			Yes	
	Other Mail Ports Supported for Core Virus and Spam Protection	*											
39	Is there support for core virus and spam protection for the following? (Please mark an "X" in all appropriate boxes.)	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Port 80 e-mail traffic (e.g., Hotmail)	*	IWSS	Virus protection via optional antivirus	No			On road map	No	Hotmail and MSN via Outlook Express through MailFrontier Desktop	The product includes a SDK that does allow for integration into other environments.	No	
	POP	*	X	No	No				X	Yes	Same as above.	No	
	Secure POP	*	No	No	No				X	Yes	Same as above.	No	
	IMAP	*	No	No	No			On road map	X	Yes	Same as above.	No	
	Secure IMAP	*	No	No	No			On road map	X	Yes	Same as above.	No	
40	Are all these functions available for outbound mail as well? If not, please indicate which features are unavailable.	*	POP proxy support only applicable to inbound e-mail	X	Yes			Will be	Yes		Yes	Yes	NA
	Secure Mail	*											
41	What secure mail services do you support (please mark 'x' in all appropriate boxes)?	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Web delivery (e.g., URL delivery to recipient)	*		No	X	X	X		X				Through partnerships

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
	S/MIME encryption	*		No	X	X	X		X			X	Through partnerships
	TLS server-to-server encryption	*	Via Postfix add-on; IMSS 6 via Windows SMTP Services	No	No	X	X		X		Supported by the MTA	X	Yes
	Open Group's S/MIME certificate interoperability gateway standard	*		No	No	X	X		No		NA	X	NA
	PGP encryption	*		No	No		X		X		NA	X	Yes, through partnership with PGP
	Other	*			Rabin strong encryption, Triple DES	Secure Push via Secure Envelope			PostX Secure Envelope, Voltage Encryption		NA		
42	Is a client plug-in available for local authentication for Outlook?	*	NA	No	Yes	X	Yes		Support for TLS, S/MIME, PGP in Outlook. Optional plug-in for Voltage.		NA	No	Through partnerships
43	Is a client plug-in available for local authentication for Notes?	*	NA	No	Yes	X	Yes		Support for TLS, S/MIME, PGP. Optional plug-in for Voltage.		NA	No	Through partnerships
44	Does the package have the ability to encrypt mail based on keywords/ phrases?	*	Third-party (Authentica) supported bundle, policy-based.	No	Yes, also various Labels, Masks and formats	X	Yes		Yes, as well as sender and recipient IP, address, or domain		NA	No	Via partner encryption servers
45	Does the package give users the ability to request encryption (e.g., type "secure" in header)?	*	NA	No	Yes	X	Yes		Yes		NA	No	Via partner encryption servers
46	Can the secure mail application apply different encryption methods based on the identity of the recipient or sender?	*	NA	No	Yes	X	Yes		Yes		NA	No	Yes
47	Is there support for automated digital signing of outbound mail at the gateway?	*	NA	No	Yes	X (both per domain and per sender)	Yes		No		NA	Yes	Yes, through partnerships
Authentication Support		*											
48	Does the package support SPF? If not, please specify when this is planned.	*		Not supported; planned for 2005	NA	X	Yes	Q1 - 2005	Yes	Yes	Q4 2004 release.	As soon as revised standards established.	SPF supported today as a custom module, native in Q404

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
49	When will the package support Sender ID?	*		under investigation	NA	Q4 - 2004	Sender-base in Oct. 2005. Sender-ID into reputation filters in Oct. 2004	Q1 - 2005	Fall 2004	Immediately upon finalization of the standard or mid-Q4 - whichever is sooner.	If the standard is completed in time, Q4 2004. If not, the following release.	SenderID will be supported as soon as the revised standards available	Q4 2004
50	Does the package support Domain Keys? If not, please specify when this is planned.	*		under investigation	NA	2005 Support for message signing standard per IETF/MASS	2005	Q1 - 2005	Fall 2004	Evaluating	In 2005.	No	Not currently planned
	Strong Authentication	*											
51	Does system support tokens:	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	RADIUS	*		No									
	RSA SecureID	*		No		X			X				
	Cryptocard	*		No									
	SafeWord	*		No									
	Other	*	Active Directory (IMSS 6)			End-user access to secure message store integrates with any I&AM system						PureMessage can be integrated with any authentication method.	Digital certificates are supported
52	Are these tokens supported for secure remote access?	*	NA	NA		Tokens supported for end-user access to the Web store. Admin access is via MS SQL server access control			Yes, for secure Web mail				
	Phishing protection	*											
53	Please indicate what phishing protection is available beyond core spam filtering.	*	IMSS, limited signature (IMSS 6 = full-featured phishing categorization and reporting; IWSS = currently, URL)	URL filter database contains updated phishing URLs: Detection of URLs to phishing sites /pages	A signature database specifically addressing phishing. Message Inspector has the ability to scan content (and take action) containing social security numbers and credit card information.	Anti-Fraud Service with updates, outbound S/MIME digital signatures	Brightmail Anti-Fraud is integrated into the Brightmail Anti-Spam engine. Human oversight in the Brightmail operations centers find phishing attacks and block them with rules.	NA	SPF, CipherTrust TrustedSource reputation service, CipherTrust Threat Response Updates and all the other spam detection/blocking techniques	Vulnerability exploit detection, social engineering tricks, reports of fraud in the wild, and reputation to filter phishing. Also protect corporate directory, alert security of targeted attacks, and Notify about new fraud.	Phishing filters are provided as a part of the regular spam filters.	All necessary phishing protection is performed with the spam engine.	

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
	Intrusion/ Anomaly Detection	*											
54	Does the solution offer protection against the following (please mark 'x' in all appropriate boxes)?	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	Mail floods	*		No		X	X	X	Yes, detects and blocks	X		X	X
	Buffer overload attacks	*		No		X	X		Yes, detects and blocks	X			X
	Cross-mailing list/out-of-office loop detection	*		No		X	X		Yes, detects and blocks	X		X	
	Dictionary harvest attacks	*		No		X	X	X	Yes, detects and blocks	X	Coming in the next release.	X	X
	Firewall services, which drop all Non-SMTP and irregular requests for service	*		No		X	X		Yes, detects and blocks				X
	Malformed message protection	*	X	X	X	X	X	X	Yes, detects and blocks	X		X	
	Other	*				SMTP DATA size limitations, configurable allowable number of inbound connections per host, configurable allowable number of recipients per message, detection of null sender and unspecified recipient domain, tarpitting							
55	Can policies be set at SMTP conversation time?	*	X-limited	X (a subset of the policies)	X	X	X	Yes	Yes	X		No	Yes
56	Can connections be stopped based on IP address or SMTP envelope information?	*	X-limited	X	X	X	X	Yes	Yes	X	If the MTA supports this capability.	Yes	Yes
	Content Filtering	*											
57	What prepopulated lexicons exist (please list all)?	*	Inappropriate sexual/foul language (eManager)	No	HIPAA, GLB, NASD, SEC, Intellectual Property, HR, Personal Finance, Profanity, Healthcare PHI, Legal	HIPAA, GLBA, Known Hoaxes, Resume Keywords, Sensitive Information, SPAM Disclaimers	Profanity, Proprietary Content, Sexual Content	Spam, Virus phrase, pornography, profanity	Pornography, malicious code, confidential, numerous regular expressions (SS#, phone #, account #.)		NA	Offensive words	Offensive language

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
58	Does the package have the ability for the customer to customize content filters?	*	X	X	Yes	X	Yes	Yes	Yes	Yes	X	Yes, customized lists of words or phrases can be created.	Yes
59	Are regular expressions supported?	*	X	X	Yes	X	Yes	Yes	Yes	No	NA	Yes	Yes
60	Is there support for pornography detection?	*	Language/file types Now (IMSS 6 image detection via Trend Labs filtering)	X (text only)	Yes, text only	X	No	Yes	Yes	Yes	NA	Yes	Yes
61	Are all these functions available for outbound mail as well? If not, please specify which features are unavailable.	*	X	X	Yes	X	Yes	Yes	Yes	No	X	Yes	Yes
62	What parts of an e-mail message can be inspected (e.g., header, message body, attachments)?	*	Message body, attachments	All parts, including header, body, attachments, nested archives, etc.	Header, body, attachments	All	Connection, envelope sender and recipient, LDAP group of sender/recipient, any header presence or value, body and attachment content, attachment type/file name, MIME type	Header, body, attachment, subject line, subject name	All	Header, body, attachments, contact points	Header, body and attachment.	All parts of the message can be inspected: header, body, attachments.	All, but attachments. That will be supported in next release.
63	Are attachments filtered for content, file type, or both?	*	Both	Both	Both	Both	Both	Content, type size, extension, etc.	Both; attachment filtering is based on actual file type, not extension	Both	Both.	Attachments can be filtered by both content and type.	Type today, content in next release.
64	Is attachment filtering available for outbound duties?	*	X	X	Yes	X	Yes	Yes	Yes	No	Yes	Yes, outbound attachment filtering can be performed.	Yes
Outbound services		*											
65	Does the platform support message append of disclaimer?	*	X	X	Yes	X	Yes	Yes	Yes		Q4 2004 release.	Yes	Yes
66	What other outbound services, if any, are available that have not been previously specified?	*	Encryption via Authentica-enabled bundle	Generic header adaptation		Over 23 options including Return to sender, detain, defer, route to select relay, add recipients, custom annotate body, custom Notification.	Rate limiting, Virtual Gateways (sending over multiple IP addresses), Bounce profiles per destination		None			None.	

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
Policy Controls		*											
67	Are policy control available:	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function
	by Domain	*	X (route-based support)	X	X	X	X	X	X	Yes	X	X	X
	by Group	*	X (IMSS 6 to include additional LDAP)	X	X	X	X	X	X	Yes	X	X	X
	by Individual	*	X (address group support)	X	X (also, by IP address/Node)	X	X	X	X	Yes	X	X	X
End User		*											
68	Can end users access quarantined messages?	*	Yes (anti-spam only, currently; IMSS 6 for content)	X (via digest function)	No	X	Yes	Yes	Yes	Yes	X	Yes	Yes
69	Can end users manage individual safe and block lists?	*	Safe	No	Yes (personal always/never lists)	X	No	On road map	Yes	Yes	X	Yes	Yes
70	Can end users manage their individual spam policies?	*	No (unless requested to administrator)	No	Yes, (Optional)		Yes, Via LDAP	On road map	No	Yes	X (ability to define which languages they want to accept)	Yes	Yes
71	Do you support e-mail aliases for end users (all user policies apply to all aliases)?	*	IMSS 6 (via LDAP support)	X (via LDAP)	No	X	Yes	On road map	Yes	Yes	X	Yes	Yes, and quarantines consolidate all aliases
72	Does this functionality require desktop software or plug-in?	*	No	No	No	No	No	No	No	No	X (except end user quarantine)	End User functionality requires a Web browser.	No
Platform Specifics		*											
Delivery Model		*											
1	Does the solution include an appliance?	*		Sept. 2004	Yes	Yes	Yes,	No	Yes	Yes	Via BorderWare and IronPort.	No	Yes
2	Does the solution include traditional software load?	*	Yes	Yes	Yes A desktop plug-in for e-mail encryption called ZixMail is included.	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
3	Is the solution available in a hosted fashion?	*	Yes (via third-party xSP partners)	Major ISPs offer services based on our product, e.g., T-Online in Germany	Yes The portal component, ZixMessage Center and ZixPort is hosted by ZixCorp.	No	No	No	Oct-04	No	Yes, via partners	No	No

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
4	If appliance, please list all current model numbers with approximate sizing and list price.	*		The appliance is called 'WW 1000' which supports up to 6000 users. Final pricing not yet fixed.	Additional units are deployed as necessary to achieve targeted levels of performance and availability.	Email Firewall Appliance: - 2,500 user limitation: \$15,000 (AV included) - No user limitation: \$30,000 (AV included) MailGate Edge Relay: - Edge 5G (up to 5,000 msgs/hr) \$5,000 - Edge 25G (up to 25,000 msgs/hr) \$20,000	C60 for over 1,500 users, C30 for 500 to 1,500 users, C10 for under 500 users	NA	IronMail 345 (approx. 5,001-10,000 users): \$55,000; IronMail 305 (approx. 1,001-5,000 users): \$33,500; S-Series IM-\$100 (501-1,000 users): \$19,900; S-Series IM-S50 (250-500 users): \$15,900; S-Series IM-S25 (<250 users): \$9,500	m500: \$35,000 (1,000 - 5,000 users); m1000: \$55,000 (5,000 - 10,000 users; higher user counts are supported with multiple boxes). Note: All sizing has been done based on regular mail flow being 1/3 of peak flow	NA	NA	P600, <10,000 users, \$5,750 P800, >10,000 users, \$7,750
5	If appliance, what is the OS?	*		CG Linux (CyberGuard's hardened Linux version)	ZixVPM and ZixMessage Inspector Appliance utilize Red Hat Linux.	Windows (Email Firewall) Linux (MailGate Edge)	AsyncOS	NA	Irons (based on Free BSD)	Windows 2003	NA	NA	Proofpoint's custom Linux distribution, based on Red Hat Enterprise Linux ES
6	If appliance, who is the hardware manufacturer?	*		NA	Dell	Rackable	The hardware is a custom configuration sourced from Dell.	NA	IBM	NA	NA	NA	Dell
7	Are there other hardware delivery platforms available? Specify manufacturer.	*	NA	Washing Box appliance from Exer Datacomm in France	No	NA	No	NA	Unbranded PC option also available without support	No	NA	NA	No
8	If software load, what operating systems are supported?	*	Solaris, Windows (including 2003 Server), Linux (e.g., Red Hat EL, SuSE, United Linux).	Windows 2000/2003 Server, Sun Solaris 8 and 9, Red Hat Enterprise Server 3, SUSE Linux Enterprise Server 8, Debian GNU/Linux 3.0	ZixMail: Windows 95 and higher. ZixMessage Inspector and Zix Web Inspector: Windows 2000 and higher.	Microsoft Windows 2003	N/A	Linux, Solaris Microsoft Windows 2000	NA	Windows NT/2000/2003 Server, Solaris 8/9	Windows 2000 and 2003, Solaris 8 and 9, Red Hat Linux ES and AS 3.0.	Linux, Solaris, FreeBSD, HP-UX, AIX, Windows	Solaris 8, 9 Red Hat Enterprise Linux ES 3.0

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
9	If software load, please list price per user or per processor (or whatever pricing scheme is used) for all versions.	*	IMSS + SPS = \$15.68 per seat for 10,000 users	\$10 per user/year for 1,000 users	ZixMail is \$50/year per e-mail address for a single user.	EMF- No user limit: \$20,000/cup (AV included) EMF - 2,500 user limit: \$10,000/cup (AV included) Anti-spam service: \$4,000/cup Secure Messenger (Web-based encryption module): starts at \$20,000 depending on configuration and number of users	NA	Annual Subscription or Perpetual License, price range: \$3 - \$20 depending on components purchased, discounts available	NA	Starting at \$1,980 for 100 users, MailFrontier Enterprise Gateway is priced per user. For 5,000 users, the price is \$6.15. For 10,000 users, the price is \$5.10 (both prices are based on a 2-year contract).	NA	Per user pricing.	Pricing ranges from \$20 - \$2 per user/yr. for both software and appliance, depending on user count. Additional per-user fees apply for anti-virus.
	Other Platform Specifics	*											
10	Is there a GUI-based management console?	*	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
11	What percentage of functions are available through the GUI?	*	100%	100	100%	99.90%	90%	85%	All	100%	100%	90%	100%
12	Is there a command line interface? If Yes, can all the management capabilities be exposed via CLI?	*	Yes (Limited to primary configuration updates)	Yes	No	Yes	Yes All	Yes	Yes, CLI functions are limited	No	There is a command line interface that exposes some of the functionality such as starting and stopping services.	Yes	Yes, and all are available via CLI.
13	Can the platform pull and aggregate reports from all servers?	*	Yes (TMCM)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
14	Can the platform automatically generate and distribute reports at specified time and to specified users?	*	By time, currently; w/ based on admin, IMSS 6	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
15	Is there support for auto-export of logs?	*	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Logs are made available both from the file system and the Web-based interface.	Yes	Yes
16	Is there a password-controlled and granular/delegated browser-based management interface?	*	IMSS 6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
17	Is the platform (OS and MTA) hardened? If Yes, can you provide any measure of quality (Nessus scan, third-party certification, etc.)?	*	Hardening guides only	Hardened Linux. Getting EAL4+ certified; MTA is hardened	Yes	Both FIPS 140-1 Level 1 and CC EAL2	Yes Hardened and passes a Nessus scan. Undergoing Common Criteria certification currently.	Our upcoming release will be hardened for supported OS and MTA	Yes; Nessus scan	Yes	Not applicable.	PureMessage can reside on a hardened OS and MTA.	Yes, Nessus and Qualys scans.
18	Does the package support remote and local administration with the ability to control multiple servers and administer policy from one console?	*	TMCM, Now limited; IMSS 6 for more depth	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
19	Are all centralized configuration options available from the "master" server? If Yes, is this functionality standard, or available at an extra fee?	*	TMCM, Yes, free; IMSS 6 more depth, free	Yes	ZixVPM supports native clustering.	Yes, standard	Yes The CM system is implemented as a self-healing mesh. Requires an additional fee.	Yes	Yes, no extra fee	Yes	Yes	All centralized configuration options are available on the "master" server at No extra cost.	Yes, standard functionality.
20	Is there support for load balancing (independent of DNS/MX)?	*	No, currently; IMSS 6 distributed architecture, Yes	Yes, load balancing for multiple filtering engines (via ICAP interface); No load balancing for multiple MTA.	Yes	Yes, through third party	Third-party load balancers	Yes, third parties	Yes	Yes	Depends on MTA	Third-party load balancers can be incorporated into the environment.	No
21	Is there support for failover (independent of DNS/MX)?	*	Yes	Yes, failover for multiple filtering engines (via ICAP interface); No failover for multiple MTA.	Yes	Yes, via clustering and replication	Third-party load balancers	Yes via underlying app servers, RDBMSs and third-party IP pooling.	Yes	Yes	Can failover to different filtering servers	Via third-party load balancing hardware.	Yes
22	What security certifications exist (e.g., CC EAL 4)? Please list all.	*	OPSEC, AVVID (partner only)	None. Certifications are in preparation.	The ZixSecure Data Center is SysTrust and SAS-70 certified.	Both FIPS 140-1 Level 1 and CC EAL2, in evaluation for CC EAL3	Common Criteria certification is currently in progress.	Customer internal security assessments	Common Criteria in process		Symantec Brightmail AntiSpam is in process for EAL3.	NA	None.
23	Is directory update service automated or manual?	*	IMSS 6 (Both)	Automated	The ZixSecure Data Center hosts the directory of public keys	Automated	Automatic.	Manual	Automated	Automatic	Automated.	Automatic and/or manual updates.	Yes
24	What directory support (e.g., LDAP, AD) exists? Please list all.	*	IMSS 6 (AD)	LDAP, Active Directory	Not required with ZixMail, ZixVPM and ZixMessage Center. Zix Message Inspector can be integrated with LDAP or AD	LDAP, AD, Exchange 5.5, Domino, Sun ONE	LDAP, AD	Microsoft Active Directory, Sun Directory, openLDAP, IMAP Servers, POP Servers, Microsoft NTLM	LDAP, AD	All major versions of LDAP are supported	Active Directory, Exchange 5.5 and SunOne's Directory Server.	PureMessage integrates with various forms of LDAP, including AD.	LDAP, AD

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
25	What are the top 10 reports used by customers?	*	Report Used	Report Used	Report Used	Report Used	Report Used		Report Used	Report Used	Report Used	Report Used	Report Used
	1	*	Unknown	Top recipients	Multiple message detail reports	Message Volume and Size Report	Virus Senders	Message volume by number of messages	Incoming Report	Messages Processed	Mail Summary	Top Virus Types	Summary dashboard
	2	*	Unknown	Top sender	Top groups, users, top known e-mails etc.	Spam Volume Report	Spam Senders	Message volume by size of message	Policy Configuration Report	Categories of Junk Mail	Top Sender Domains for Spam	Message Categorizations	Top Virus Types
25	3	*	Unknown	Top spam sender IPs	Top message counts by rule.	Virus Type and Volume Report	Rejected Connections	Message Dispositions (inbound/outbound/internal)	Outgoing Report	Allowed & Blocked List Population	Top Senders for Spam	Spam Range Volumes	Top Spam Dispositions
	4	*	Unknown	Top spam recipients	Amount of spam detected.	Frequently Detected Virus Report	Top Spam Recipients	Top Policies Triggered (inbound/outbound/internal)	Mail IDS Report	Top Spam Origination Domains	Top IP Sender IP for Spam	Top Virus Senders	Top Virus Receivers
	5	*	Unknown	Top media types	e-mail activity by day.	Frequent Policy Violation Report	Top Virus Recipients	Top Senders of Messages that Trigger Policies	Policy Compliance Report - Detailed	Top Spam Recipients	Top Recipients Domains for Spam	Top Spam Senders	Top Spam Receivers
	6	*	Unknown	Top top-level domains	Highest volume of encrypted E-mail senders.	Frequent Recipient Policy Violation Report	Top Virus Types	Top Recipients of Messages that Trigger Policies	Policy Compliance Report - User Based	Fraud Unjunk Recipients	Top Recipients for Spam	Policy Reporting	Top Dictionary Rules
	7	*	Unknown	Top e-mail destinations	Highest volume of encrypted e-mail recipients.	Frequent Sender Policy Violation Report	Spam Statistics	Top Senders of Messages by Message Count	Policy Compliance Report - Summary and Statistics	Messages Identified as Fraud	Specific Spam Sender	Rule Hit Rates	Top E-Mail Firewall Rules
	8	*	Unknown	Top e-mail content categories	Number of HIPAA violations avoided.	Frequent Sending Domains Report	Virus Statistics	Top Recipients of Messages by Message Count	System Defined Policies Report	Viruses Caught	Specific Spam Recipient	Quarantine Size	Top Reasons Message Quarantined
	9	*	Unknown	Top virus by name	Destination of outbound e-mail by domain.	Frequent Virus Sender Report	Message Flow Histogram	Review Queue Activity Audit Report	IronWebMail Report	Messages Filtered by Policy	Spam Summary	Spam Range Volumes - Quarantine	Top Dispositions
	10	*	Unknown	Top e-mail user groups	Origin of inbound e-mail by domain.	Attachment Volume and Size Report	Top Policy Infractions	Number of messages triggering selected policies	Vulnerability Assessment	Return on Investment	and more including 9 virus reports	Message Categorizations - Quarantine	Top Adult Spam Receivers
26	Is reporting data stored in a database for flexible reporting?	*	TMCM, Yes; IMSS 6, local level also for logs	Yes (requires WebWasher Content Reporter as extra option)	For ZixVPM and Zix Message Inspector, activity logs on the device. Activity logs for the ZixSecure Data Center	Yes	The external database uses SQL. The internal database is stored in a proprietary format accessible to customers.	Yes	Yes, flexible access via GUI and exportable	Reporting data is stored in XML files for easy report generation.	Yes	No, reporting data is stored in CSV files. Flexible export options are available for report manipulation.	Yes
27	How many reports are available?	*	At least 20 various options	90 pre-defined reports, plus unlimited customizable reports	150 plus	25 out of the box	30+	50 plus	10 standard reports	11 report groupings	19 out of the box reports.	11	37

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
28	Can reports be published or e-mailed?	*	TMCM and IMSS, published; EUQ 1.1 both	Both	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
29	What type of database is supported?	*	TMCM (MSDE); IMSS 6 (MSDE-win, PostgreSQL-Unix)	Oracle 8i, Oracle 9i, MS SQL Server 2000, MaxDB	Postgress SQL	MS SQL 2000	MySQL	MySQL, Oracle, SQL Server and DB2	Exportable as .CSV, so any relational database	No database is necessary	MySQL	PostgreSQL	Database (MySQL) is self contained, but can be backed-up and exported
30	Is there an ability to use a single database for multiple servers?	*	IMSS 6 (Distributed architecture design)	Yes	Yes	Yes	Yes	Yes	Yes	No database is necessary	Yes	Yes	Yes
31	Is there the ability to have a dedicated database machine?	*	IMSS 6 (Architecture allows separate policy, log)	Yes	Yes	Yes	The Mail Flow Controller performs analysis in an external database.	Yes	Yes	No database is necessary	Coming in the next version.	Yes	Yes, with software version. Appliance database is self-contained.
32	Is the database being used to store messages and queues, or just for reporting/logging?	*	IMSS 6 (Policy admin, scanning; logs)	Just for reporting.	Rules, configuration and log information.	All data is stored in the DB, including messages, queues, and logs.	Only statistics and logging information is handled in a database.	Message storage and reporting/logging	Yes for internal database, exports are reporting/logging	No database is necessary	The database is used for configuration, reporting, logging and spam quarantine.	Index/ message information of quarantined messages for administrative and End Users	Yes (both)
33	Please list all languages supported by the management console.	*	IMSS 5 (English, Japanese, Simplified Chinese); IMSS 6 (English, Japanese)	English	English	English by default. The UI is internationalized and has been localized into Japanese by partners	English	English	English	English; Japanese, French, German currently in beta	English	English only.	English only
34	Please give some measure of performance of the system(s) in throughput terms, assuming near-zero latency.	*	Near-zero latency; IMSS 6 (distributed architecture allows for incremental scanner scaling, as needed, w/ self-discovery for bringing online)	11 messages/sec on a single CPU system. Additional throughput on multiprocessor systems.	A single server can handle 20K messages per day in an e-mail encryption solution up to 72K messages per hour in an e-mail content scanning and anti-spam solution.	40K-200K msgs/hr depending on hardware.	An IronPort C60 is capable of 500,000 messages per hour @ 15KB message size. With all scanning enabled the system is capable of 175,000 MPH throughput.	Our production implementation at a large customer handles more than 3M e-mails a day.	Max throughput is 208,000 messages per hour at 4K message size; fully loaded (throughput is 35,000 messages per hour)	160,000 messages per hour (3 Ghz Dual CPU)	On a Intel Xeon processor based system roughly 20 messages per processor.	20 messages per second with spam, virus and policy filtering enabled on a typical dual-CPU Xeon box.	P600, 20,000 messages/hour P800, 40,000 messages/hour
35	Please list all languages supported by the end user interface.	*	NA	Default is English. Templates can be translated to other languages as needed by customer.	English	English by default. The UI is internationalized and has been localized into Japanese by partners	English	English	English	Junk Box Summary; English, French, German, Japanese, Korean, Russian and Spanish	English	The End User Web Interface supports English, French, German, Spanish and Italian languages.	English only

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
	Systems & Cluster Mgmt.	*											
36	What SNMP support is available?	*	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	"X" indicates support for this function	None		No	NA	"X" indicates support for this function	
	SNMP MIBs	*	No	None	No	NA	X	No	No	No queues in MailFrontier: SNMP MIBs support not necessary.	NA	No	X - Supported via \$syslog
	SNMP Traps	*	Yes	None	No	X	X	No	Yes	left blank	NA	No	X - Supported via \$syslog
37	Secure connection for system alerts, notifications, and updates?	*	IMSS 6	Updates via secure HTTPS	Yes via CD	X	X	Yes	Yes	SSL encryption is supported	X	No	X
38	Is clustering supported (i.e. multiple systems acting as single logical unit)?	*	IMSS 6 (Distributed architecture design)	Yes	Yes with ZixVPM	X	X	Yes, via the underlying App servers and RDBMSs.	No, our scaling model is horizontal and stateless	Yes - including shared storage clustering and geographically distributed remote analyzers	X	Yes	X
39	Can policy and content controls be automatically synchronized between systems?	*	IMSS 6 (Same as above)	Yes	Yes with ZixVPM	X	X	Yes	Yes	Yes	X	Both	X
40	Is e-mail database searchable across multiple servers?	*	IMSS 6 (Scanners store locally; database indexes)	No	Multiple servers per domain	X	X	Yes	Yes	Yes	X	Yes	X
41	Do systems added to cluster automatically notify each other?	*	IMSS 6 (Scanner self-discovery to policy server)	Yes	Yes, ZixVPM	X	X	Client filters interface with centralized management server	No, our implementation is stateless	Yes	NA	No	X
42	Do systems added to cluster automatically notify load balancer?	*	No (N/A for IMSS 6 blade reference deployment)	No	This is outside the scope of our products.	X	No	Yes	No, our implementation is stateless	No, not required. New systems coordinate through shared storage	NA	Typically systems added to the cluster are balanced using DNS/MX records.	X
	TCO/Pricing	*											
43	What is the 3-year pricing for 5,000 users (including support and maintenance)?	*	156,800 (list price \$19.60/seat) plus 2 yrs maintenance)	\$86,670 total, or \$5.78 per user/year	\$18/user/yr. Anti-spam is \$6.50/user/year and the appliance is \$7.15/user/year (includes virus).	Appliance: \$76,000 (incl. anti-spam, AV, MTA (Edge), secure mail (TLS, S/MIME), content filtering) Software: \$60,000 (incl. anti-spam, AV, MTA (Edge), secure mail (TLS, S/MIME), content filtering)	\$136,500 (includes Brightmail)	Annual Subscription or Perpetual License, price range: \$3 - \$20 depending on components purchased, discounts available, pricing starts at 10,000 users	\$53,600	Software: \$92,250 for 3 years (pre-paid) Appliance (m500): \$80,850 (includes a warm spare)	\$89,250 list.	List at \$48,300	\$72,125 (w/ platinum 24x7 support, setup, and training)

* BorderWare requested its survey responses not be published, but will supply the survey information upon request

Q#	Questions	BorderWare	Trend Micro	CyberGuard	ZixCorp	Tumbleweed Email Firewall	IronPort	MessageGate	CipherTrust	MailFrontier	Symantec	Sophos	Proofpoint
44	Antivirus pricing for above if not included?	*	Included	\$130,762 total, or \$8.71 per user/year (CA or McAfee engine, includes also Web traffic AV scanning)	Please refer to the response to Question 69 above	Included	\$10,125.00	Included in perpetual license	No	\$63,750 for 3 years	\$73,050 list.	Anti-virus and anti spam (bundle pricing) at \$101,887	\$3.68 per user/yr
45	What other options are available but not included in the above?	*	Outbreak Prevention Services (via TMCM)	SSL Scanner, Content Reporter, IM Filter, URL Filter	Optional	DAS: \$12,000 S/MIME + A/V option: \$12,800 Secure Messenger: \$78,000	Centralized Management, Mail Flow Central: \$4,000 total, three years	Perimeter Protection, Policy Enforcement (inbound, outbound & internal), anti-virus, audit, intelligent archiving	IronWebMail; Secure Delivery	Premium Support (24x7)	This is all inclusive.	extended policy available and anti-virus can be added to AS/AV bundles	Professional services
46	What is the 3-year pricing for 10,000 users (including support and maintenance)?	*	250,880 (list price plus 2 yrs maintenance)	\$115,560 total, or \$3.85 per user/year	Encrypted messaging is \$14/user per year. Anti-spam is \$5.70/user/year, appliance is \$6.00/user/year (virus included).	Appliance: \$136,000 (incl. anti-spam, AV, MTA (Edge), secure mail (TLS, S/MIME), content filtering) Software: \$120,000 (incl. anti-spam, AV, MTA (Edge), secure mail (TLS, S/MIME), content filtering)	\$176,500 (includes Brightmail)	Annual Subscription or Perpetual License, price range: \$3 - \$20 depending on components purchased, discounts available, pricing starts at 10,000 users	\$88,000	Software: \$153,000 for 3 years (pre-paid) Appliance (m1000): \$127,050 (includes a warm spare)	\$127,500 list.	\$77,220K	\$110,960 (w/ platinum 24x7 support, set-up and training)
47	Antivirus pricing for above if not included?	*	Included	\$199,785 total, or \$6.66 per user and year	\$3.80 user/year for 5,000 users \$3 user/year for 10,000 users	Included	\$15,750.00	Included in perpetual license	\$33,300	\$115,500 for 3 years	\$141,800 list.	Anti-virus and anti spam (bundle pricing) at \$163,020	\$3.08 per user/yr
48	What other options are available but not included in the above?	*	TMCM services priced separate	SSL Scanner, Content Reporter, Instant Message Filter, URL Filter, Content Protection	Available on Web site	DAS: \$24,000 S/MIME + A/V option: \$12,800 Secure Messenger: \$156,000	Centralized Management, Mail Flow Central: \$4,000 total, three years	Perimeter Protection, Policy Enforcement (inbound, outbound & internal), anti-virus, audit	IronWebMail; Secure Delivery	Premium Support (24x7)	This is all inclusive.	extended policy available and anti-virus can be added to AS/AV bundles	Professional services @ \$2,000/day