MXTREME
MAIL FIREWALL

MXtreme™ – Spam Detection

«

Comprehensive Blended Protection Against Spam

Corporations can no longer deny the impact that spam has on their email infrastructure. As of July 2004, spam accounted for more than 80% of all inbound SMTP traffic. With these numbers, it is clear to see why email administrators are having trouble keeping up with the onslaught, and end-users are spending increasingly more valuable time deleting spam from their corporate mailboxes.

To curb the spam problem, many corporations have put anti-spam filters into place. These email filters either operate as plug-ins to an email server or are supplementary systems that require continual attention and management. If not managed properly, spam filters can grow into administrative nightmares and may become completely ineffective. This challenge is further magnified when enterprises look to spam protection as a component of large-scale email hygiene – an issue that cannot be addressed by a spam filter point solution.

The MXtreme™ Mail Firewall offers two Anti-Spam solutions. A built in Anti-Spam application uses highly effective and intuitive filters to maximize spam fighting power with minimal false positives. MXtreme also offers Symantec Brightmail® Anti-Spam as a value-added option for managed spam filtering. If you are using an existing Anti-Spam tool, MXtreme will dramatically increase your spam filtering effectiveness, while providing you with a complete mail hygiene solution.

Blended Filters

The built-in spam tools in MXtreme catch up to 98% of all spam that passes through corporate email servers and provides remarkably low ratios of 1 in 100,000 false positives. These dramatic results and comprehensive email hygiene results are achieved by using blended filters with objective and subjective filtering technology.

With MXtreme, all inbound email messages go through a set of objective filters, including blacklist/whitelist, RBL, SPF for anti-fraud and anti-phishing, DCC for bulk email, specific access patterns, and pattern-based message filters. Users can build their own personalized whitelists and manage their own quarantine areas.

The integrity of each message is then verified utilizing the high-performance Mail Transfer Agent (MTA) and mail firewall in MXtreme. Once a scan is completed the content is passed through subjec-tive filters – including Statistical Token Analysis for "Smart" lexical analysis, which catches the remaining 50% of the spam content – and other local content filters.
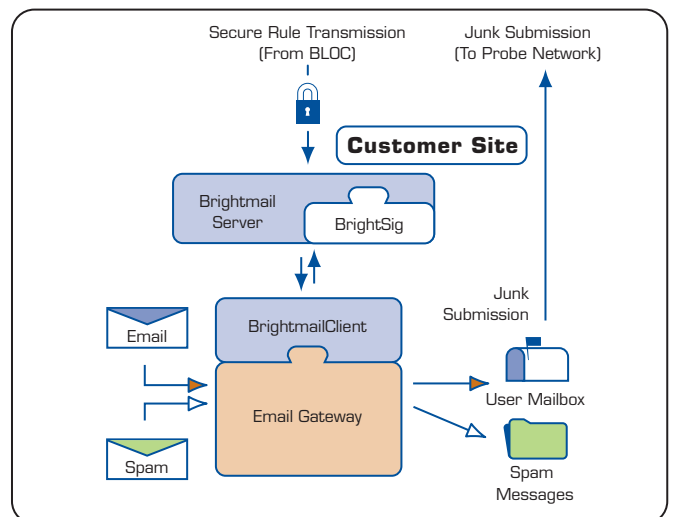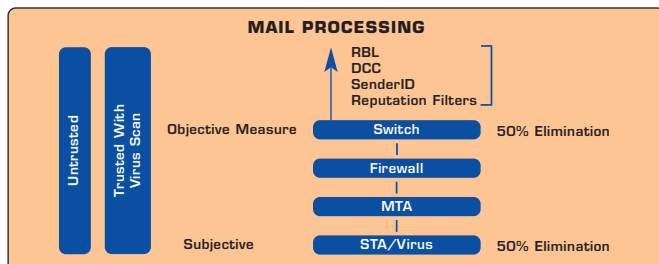
Administrators can dispose of detected spam in a variety of ways, including quarantine (enterprise and personal), rejection, redirects, subject tagging, etc.

MXtreme provides language-independent content and spam-scanning capabilities, and is used by more than 2,500 enterprises around the globe to protect more than 30 million mailboxes.

Symantec Brightmail Enterprise Edition on the MXtreme Mail Firewall

MXtreme also offers the industry-leading Symantec Brightmail® Spam Filter as a value-added option. Brightmail managed filters protect over 280 million mailboxes and 1,400 businesses from spam and unsolicited commercial email. The MXtreme Mail Firewall's S-Core™ OS and high-performance MTA work seamlessly with Brightmail to deliver a secure, high performance, and highly accurate anti-spam solution.

Once Brightmail is enabled, more than 30,000 new Brightmail rules are downloaded each day from the Brightmail Logistics and Operations Center (BLOC). This ensures spam is eliminated in real-time so users do not have to spend valuable resources managing their own spam filters, and administrators do not have to worry about updating spam signatures. With Brightmail, your organization can enjoy the benefits of 95% spam accuracy and 1 in 1,000,000 false positives.

MAIL PROCESSING

Untrusted	Trusted With Virus Scan	RBL DCC SenderID Reputation Filters
	Objective Measure	Switch — 50% Elimination
		Firewall
		MTA
	Subjective	STA/Virus — 50% Elimination

Secure Rule Transmission (From BLOC)   Junk Submission (To Probe Network)

Customer Site

Brightmail Server — BrightSig

Email

BrightmailClient

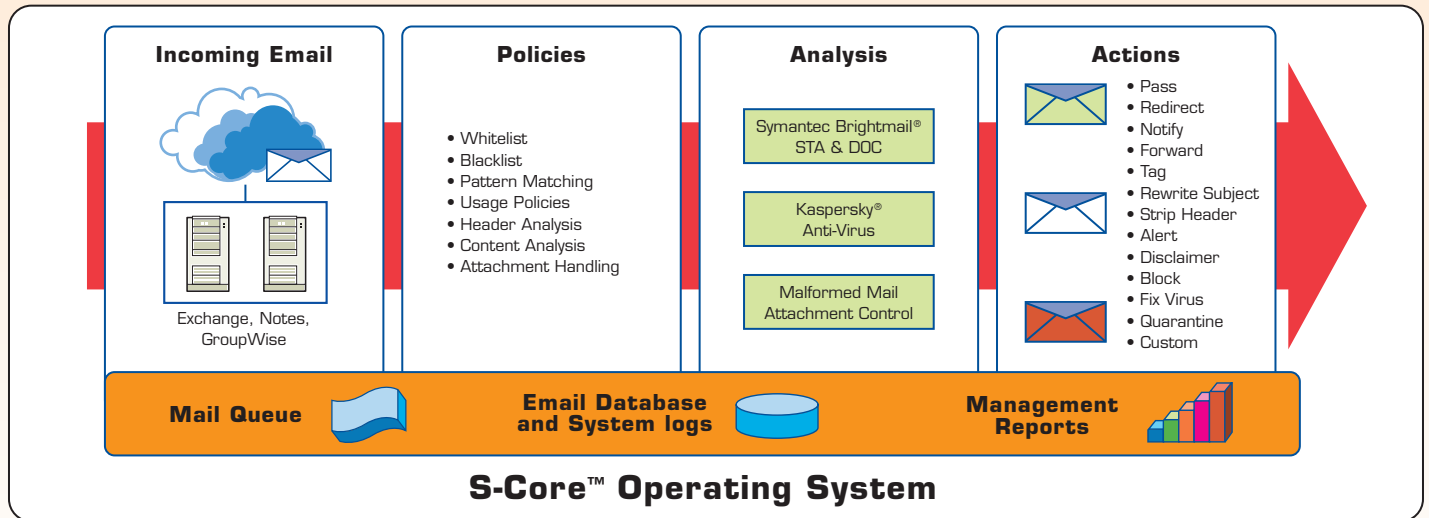Junk Submission

Spam

Email Gateway

User Mailbox

Spam Messages

◉ Rich Disposition Options

Messages tagged by the MXtreme Mail Firewall's anti-spam filters or Symantec Brightmail can be handled in a variety of ways: administrators can block or delete messages, modify subject headers, add X-headers, send messages to global or individual user quarantine, or provide any combination of these actions.

MXtreme Provides Comprehensive Email Hygiene and Spam Protection

Incoming Email

Exchange, Notes, GroupWise

Policies

- Whitelist
- Blacklist
- Pattern Matching
- Usage Policies
- Header Analysis
- Content Analysis
- Attachment Handling

Analysis

Symantec Brightmail®
STA & DOC

Kaspersky®
Anti-Virus

Malformed Mail
Attachment Control

Actions

- Pass
- Redirect
- Notify
- Forward
- Tag
- Rewrite Subject
- Strip Header
- Alert
- Disclaimer
- Block
- Fix Virus
- Quarantine
- Custom

Mail Queue

Email Database and System logs

Management Reports

S-Core™ Operating System

MXtreme Message Disposition

PARTNERS

CISCO SYSTEMS — AVVID Partner

F5 NETWORKS

Sun microsystems — iForce™ Partner

FaceTime™

symantec™

BlackBerry. — Alliance Member

KASPERSKY ANTI-VIRUS

RSA SECURITY™

Common Criteria EAL4+ CERTIFIED

Proudly Serving Enterprise and Government — 10 YEARS 1994-2004

FIVE YEARS MXTREME — Securing Enterprise & Government Email

BorderWare™

BorderWare Technologies Inc. > To learn more about MXtreme, or to register for a FREE webinar, visit www.mxtreme.com today!

Toll Free: 1.877.814.7900 • **US Federal Office:** 1.866.211.6789 • **Outside North America:** +1.905.804.1855 • **Europe:** +44.20.8538.1750

United States of America, United Kingdom, Canada, Germany, Japan, Australia, Scandinavia, Dubai