



Email ThreatPak

Complete Email Security from Viruses, Phishing, Spam and Content Violations

Email ThreatPak contains everything needed for email security, content filtering, quarantine and user management, and spam mitigation. The latest Spam-fighting technology is combined with a powerful Anti-Virus and content scanning engine to provide affordable, comprehensive protection from both external and internal.

Spam Filter

Email ThreatPak can be configured to automatically reject, redirect, quarantine or tag and deliver filtered e-mails. To prevent unintended filtering, SpamFilter allows you to create your own “white lists” of trusted senders, such as customers and business partners. eSoft’s proprietary SpamFilter incorporates the latest Spam fighting technologies, including Bayesian Filtering, Historical Averaging, enhanced Heuristic Analysis, and SPF technology. With the Bayesian Teaching Tool, an email plug-in created by eSoft, you can help SpamFilter learn from its experience, so that it gets better at catching Spam on its own.

Anti-Virus

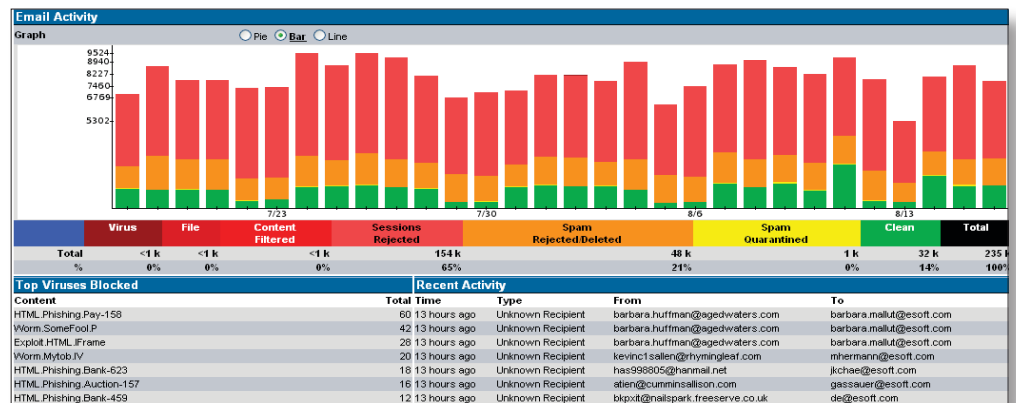
Email ThreatPak leverages a comprehensive database of frequently-updated virus signatures to scan email messages and attachments for malicious virus code. Customers create their own update schedules, and detailed reporting and graphical monitoring enables managers to see the ThreatPak in action.

Content Filter

Email ThreatPak scans all incoming and outgoing email for user-defined keywords and phrases embedded in the email body, as well as in many attachment types. The admin can quarantine email or forward it for review. ThreatPak also allows customers to create custom lists of the file types to be blocked, such as .exe, .p2p, .asp, etc.

Features at a glance:

- Automated Signature Updates
- Real Time Blackhole Lists
- Customizable White and Black Lists
- Phishing Protection
- Attachment Stripping
- Compressed/Archive Files
- Address Verification
- SPF (Sender Policy Framework)
- Bayesian Filtering
- Heuristic Analysis
- Rule-based Spam Scoring
- Historical Averaging
- Keyword Filters
- Reject, Redirect, and Tagging Email Policies
- Admin and User Quarantine
- Web-based Administration
- Reports, Statistics, and Graphs
- Simple Installation



Detailed reporting and statistics helps the organization understand its email patterns and potential risks

Simple Administration and Maintenance

Maintenance and user features of the Email ThreatPak allow IT managers to implement an e-mail security solution without extensive training and time investments. eSoft's user tools allow users to instruct the SpamFilter to better recognize junk e-mail and prevent false positives. Each week the ThreatWall quarantines fewer email and requires less administration as it learns to differentiate legitimate business communications.

Maintenance Features

- Compatible with all email servers
- Simple installation
- Automated signature updates
- Customizable white and black lists
- Reject, redirect, and tagging email policies
- Admin and user quarantine
- Web-based administration
- Reports, statistics, and graphs

User Features

- User level spam quarantine
- Outlook integration
- User learning tools
- Reject, redirect, and tagging email policies

Anti-Spam Features

- Automated signature updates
- Real time blackhole lists
- Customizable white and black lists
- Address verification
- SPF (Sender Policy Framework)
- MIME compliance checking
- Bayesian filtering
- Heuristic analysis
- Rule-based spam scoring
- Historical averaging
- SMTP protocol checking
- Keyword filters

Anti-Virus Features

- Automated signature updates
- Attachment blocking
- Compressed/Archive Files
- Administrator Notification

Part Numbers

Email ThreatPak 1 Year Subscription

InstaGate 404	IG404-ETPAK-1
InstaGate 604	IG604-ETPAK-1
InstaGate 806	IG806-ETPAK-1
ThreatWall 250	TW250-ETPAK-1
ThreatWall 450	TW450-ETPAK-1
ThreatWall 650	TW650-ETPAK-1

Need More Help?

SpamFilter: Bayesian Filtering

Bayesian Filtering

Bayesian Filtering works by examining a large number of messages to 'learn' which are spam and which are legitimate.

Bayesian Filtering Enabled

Spam Learned — 1410	Remaining —
Non-Spam Learned — 186	Remaining — 14

Still learning. Not enough messages to begin Bayesian scoring yet.

Bayesian Teaching Tool

The Teaching Tool enables users to teach the Bayesian Filter by identifying messages as Spam or not Spam.

Allow Learning via Bayesian Teaching Tool Enabled

Management Address

Platform	Add-In	Version	
Windows	SpamFilter Add-In for Outlook 2000-2003	2.0.0	Download

Bayesian Teaching Tool Access Restrictions

Allow Teaching Tool Access:

Only From Trusted Networks
 Only Approved IP Addresses
 From Anywhere

Caution: Allowing access from anywhere could allow spammers to teach your filter to allow their messages.

A sophisticated, self-learning Bayesian filter automatically learns how to treat both spam and non-spam emails for the individual organization