

Hosted Email Security and Continuity

Northeast Computer Services is proud to announce its partnership with GFI to bring you the best in hosted email security and continuity. GFI MAX MailProtection's industry-leading technology ensures the optimal filtering of unwanted or harmful messages.

GFI MAX MailProtection stops spam, viruses, and other email threats before they reach your network or mail server; incoming email is redirected to its fully redundant network and application architecture, which processes messages in real-time via both traditional spam filtering techniques and leading-edge approaches to message analysis including authenticity checks, message fingerprinting, heuristic rule sets, extensive URI databases, real-time message source analysis, and customizable whitelists and blacklists.

Key Benefits:

- ✓ Comprehensive and highly accurate spam filtering.
- ✓ Zero-hour antivirus protection.
- ✓ Business continuity with integrated queuing and on-demand mail service.
- ✓ One click whitelisting.
- ✓ Simple management interface.
- ✓ Compatibility with any email system or operating systems.
- ✓ Minimized risks of incorrectly classified messages.
- ✓ Substantially greater scalability and reliability than a software or hardware solution dependent on a single device.
- ✓ Message logging and search capabilities.

Feature Summary:

Network Defense

Almost all spam and email threats can be blocked before they reach your network - reducing risk, freeing up network bandwidth and easing mail server load.

Continuity

You can continue accessing, responding to, and sending email messages, even in the event of an on-premise mail server or network outage; mail is queued by the service, and you can continue accessing or responding to those messages via the GFI MAX MailProtection control panel, even while your own mail server is off-line.

Zero-Hour Virus Protection

Block new or emerging "zero hour" virus threats before those threats can be detected by traditional signature-based AV solutions.

Inbound Spam Filtering

Improve productivity of servers and employees by reducing the volume of junk mail getting through an existing anti-spam solution.

Outbound Spam Filtering

Prevent inappropriate messages or attachments from being sent from your network or from a specific user, thereby protecting your company's reputation and alerting administrators as to the presence of any infected workstations or 'zombie' machines, so that those systems can be handled appropriately.

Directory Harvest Attack Prevention

Defend against spammers who attempt to deliver messages to a large number of valid and invalid email addresses at your domain.

Intuitive Web-Based Control Panel

The control panel allows administrators and users to control the service, while providing access to quarantined messages as well as to queued mail in the event of an on-premise mail server failure.

Denial of Service Attack (DoS) Prevention

Prevent email-based DoS attacks by limiting and controlling inbound SMTP traffic from one or more given source IP addresses.

Hosted Individual Junk Mail Quarantines

The service can retain detected spam messages in the control panel outside of the company's network, while allowing each user to access these messages at any time to check for any genuine mail that may have been caught by the spam filters.

Individual Junk Mail Digests

Users can view a convenient, automatically emailed summary of detected spam messages, with a link next to each message to allow the user to identify and release from the quarantine any potential false positives. The digest messages can be scheduled as infrequently as once per week or as frequently as three times per day.

Configurable User Preferences

Administrators can set the spam filtering configuration for a given user, or can delegate the ability to do so to the individual users so that the service works for their specific needs.

Message Logging and Search

Determine the delivery status of an inbound or outbound message, via a message search tool that includes full delivery logs for all messages in the last 10 days.

Platform-Neutral

Works with any operating systems or mail infrastructure including Exchange, Lotus Notes, GroupWise, Zimbra, qmail, postfix, sendmail and any other SMTP server.

Pricing:

Contact Northeast Computer Services today for additional information and pricing.