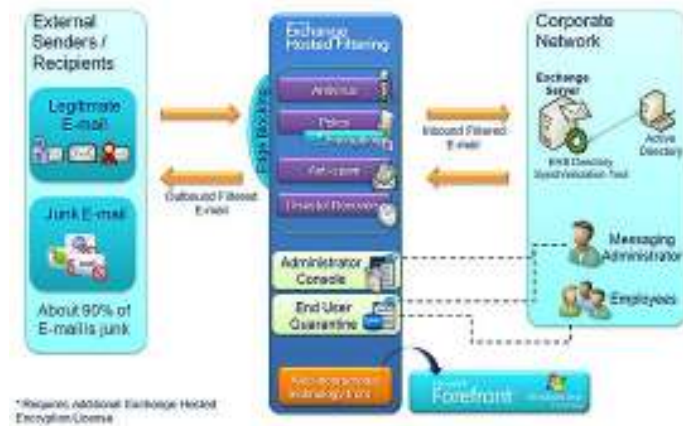


## MS Hosted Exchange Filtering

E-mail is mission-critical, but with viruses, worms, denial-of-service attacks, spam, and compliance and organizational government regulations, effective e-mail security and management is increasingly difficult. Exchange Hosted Filtering incorporates multiple filters to actively help protect businesses' inbound and outbound e-mail from spam, viruses, phishing scams, and e-mail policy violations. In addition, the service provides both rich tools for writing rules to help enforce corporate and regulatory policies governing e-mail usage and disaster recovery tools to queue mail for delivery in the event of an e-mail server outage. Exchange Hosted Filtering helps minimize capital investments, free up IT resources to focus on value-producing initiatives, and mitigate messaging risks before they reach the corporate network.



### How It Works

With just a simple mail exchange (MX) record change, e-mail will be routed to Exchange Hosted Filtering for spam, virus, and policy filtering. Exchange Hosted Filtering can be used in conjunction with any e-mail server and e-mail client. No hardware or software must be purchased or installed; and no expensive training is required for your IT staff. Administrators can customize the behavior of the service via an intuitive, web-based interface.

Exchange Hosted Filtering operates on the Exchange Hosted Services network, which is a distributed network of data centers located at key sites along the Internet backbone. Each data center contains fault-tolerant servers that are load-balanced from site to site and from server to server. Sophisticated algorithms analyze and route message traffic between data centers to help ensure secure and timely delivery. In the unlikely event that a data center is unavailable, traffic is easily routed to the other data center.

### Service Components

#### Virus Protection

Exchange Hosted Filtering uses multiple antivirus engines to remove viruses from e-mail before the malware reaches corporations. Collectively, the engines offer massive virus signature libraries and strong heuristic detection to detect both known and unknown threats. Integration with Exchange Hosted Service's e-mail security servers at the application programming interface level help ensure fast scanning and the continuous updating of antivirus definitions.

#### Spam Protection

Powered by multiple filtering engines and an around-the-clock team of anti-spam experts, Exchange Hosted Filtering virtually eliminates spam from inboxes, helping to provide bandwidth for legitimate corporate use, free precious server and storage resources, and decrease the risk of loss of sensitive information or identity theft. Captured spam is routed to the spam quarantine and can be accessed by administrators or end users at any time through an intuitive Web-based interface. An e-mail notification that lists newly quarantined spam can be configured to send to each valid e-mail address. This simplifies the end-user experience by making it simple and effective to review spam. Exchange Hosted Filtering offers the spam quarantine Web-based interface and HTML notifications in several languages.

#### Policy Enforcement

Exchange Hosted Filtering helps administrators enforce policies they set up to comply with corporate policies on e-mail usage and with government regulations such as the Gramm-Leach-Bliley Act, SEC Rule 17a, NASD Rules 3010 and 3110, and the Health Insurance Portability and Accountability Act). The intuitive policy rule writer makes it easy to monitor and manage e-mail messages based on virtually any message attribute, such as originating IP, sender, recipient, message size, file attachment, or specific text in the subject or body. Wild cards and regular expressions are supported.

**Disaster Recovery**

If the destination e-mail server becomes unavailable for any reason, Exchange Hosted Filtering helps to ensure no e-mail is lost or bounced. Exchange Hosted Filtering automatically queues e-mail for up to five days, attempting to deliver the e-mail every 20 minutes. After the customer's e-mail servers recover, all queued e-mail is automatically delivered in a flow-controlled fashion.

**Real-Time Message Trace and Reporting**

Administrators can use the powerful Message Trace tool to retrieve the status of an e-mail processed by Exchange Hosted Filtering in real-time. With basic information, such as the sender, recipient, and date, administrators can retrieve information on e-mail processed within the last 30 days. If the search yields results, administrators will have access to the exact dates and times an e-mail was processed by Exchange Hosted Filtering as well the results of the filtering (e.g., rejected, quarantined, delivered).

A comprehensive set of historical reports provide detailed statistics about customer e-mail traffic and are a valuable tool for gaining insight into any e-mail system. Reporting on an e-mail occurs within one hour of the e-mail entering the Exchange Hosted Services network. Reports can be generated by domain or entire organization and provide filtering information on spam, viruses, policy filtering, delivered e-mail, and the top virus or spam recipients.