

ExchangeDefender is an Internet messaging hygiene and business continuity system that keeps your users safe from email threats and keeps you in business. Your users will get much less SPAM, no viruses, they will be able to communicate if the server or network connection goes down and you will get the business reporting and control over your organizations messaging.

ExchangeDefender's core value is time savings. It started as a product to save time by eliminating SPAM. It has evolved into a product that saves management hours and puts the system control in the hands of those that your organization chooses.

ExchangeDefender can secure and save your business by:

- *Protecting you from junk mail (SPAM), viruses, trojans, malware, spyware and adware.*
- *Assuring message delivery by scanning and holding your email for up to **365** days of outage.*
- *Keeping you in business using our LiveArchive secure standby mail server with your identity.*
- *Allowing direct access to, and control of, your SPAM filter through an MS Outlook 2007 Add in.*
- *Helping you meet the regulatory compliance requirements with archiving and disclaimers.*
- *Keeping you off blacklists by enforcing SPF and Domainkeys and scanning outgoing email.*
- *Making your employees more productive by giving them control over their spam and policies.*
- *Making archival of messages possible and affordable with archives that scale with your business.*
- *Stopping identity theft by blocking phishing and adding authenticity to your mail messages.*
- *Delivering a more accountable mail infrastructure with user, network and business KPI reports.*
- *Enhancing mail server reliability by reducing the amount of mail and attacks it deals with.*
- *Leveraging global infrastructure and security to help you get your mail, faster and safer.*

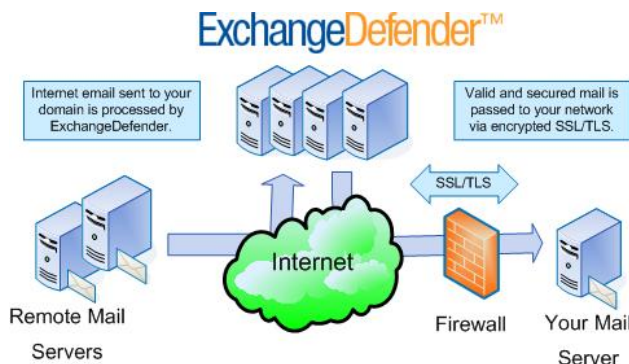
... all without any software to install or maintain. Keep your mail server running as it is and deploy ExchangeDefender in minutes at the fraction of the cost of antivirus licensing alone.

ExchangeDefender Overview

ExchangeDefender is a transparent network service designed to secure your email before it can damage your servers and workstations. It enforces your company policies, government compliance requirements and provides reporting, business continuity and even email access and collaboration when your Internet access or mail server is unavailable.

Deployment

ExchangeDefender is a transparent stateless SMTP proxy. Jargon aside, it is a security network that processes email and only delivers email you want to read down to your server. Every message going into or out of your mail infrastructure is scanned for dangerous content and the security policies you define are applied to it, along with any archiving or government compliance requirements. ExchangeDefender is a global network, spanning 2400 servers in over 14 data centers (Nov 2007) and is the fastest growing security network worldwide.



Mail for your domain is pointed to ExchangeDefender via MX records in your DNS. For outbound mail security, you use our outbound smarthost to route all outbound mail through our content protection network. Your mail server should only accept connections from ExchangeDefender and the authenticated users. For ultimate security, you can configure your firewall to only allow connections from our networks by enforcing IP restrictions.

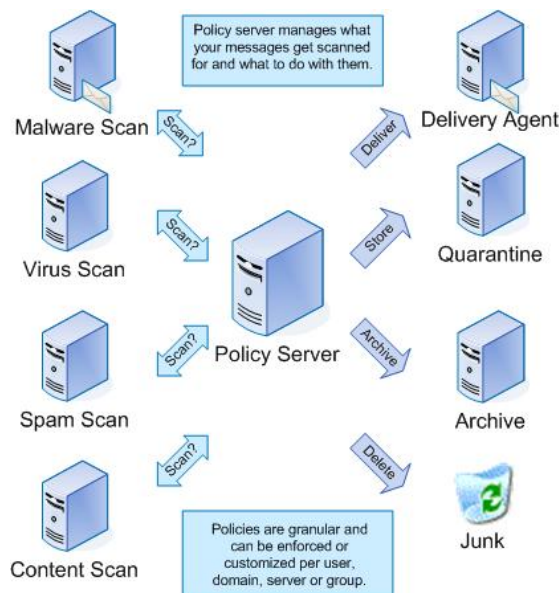
Business Continuity and LiveArchive

One of the most critical components of an external mail security solution is its reliability - you need something that will be far more reliable than your own mail infrastructure so if you ever experience an outage you have that extra layer of mail redundancy. ExchangeDefender meets and exceeds that requirement through the LiveArchive business continuity services.

LiveArchive is designed from the ground up as the core component of ExchangeDefender. It is a complete standalone email system with your users, your corporate identity and your passwords, running on highly reliable webmail system. The beauty of ExchangeDefender LiveArchive is that it is seamless; you will not even know it's there until you need it. And when you do need it you just need a web browser. Login to your account via the secure https connection, your email address and password give you access to the past **365** days of email with the ability to respond, delete, forward and essentially continue working while your main server or Internet connection to the office are down.

Security Enforcement

The brains of ExchangeDefender is its policy server, the central collection of all security directives that tell individual nodes and firewalls what to do with dangerous content, how to archive email, how to provide business continuity and implement your policies. Once your email is received by ExchangeDefender the policy server is contacted and asked what to do with the email. This is where the policies you established for your company are enforced - Should it scan it for viruses? If so, what is to be done with infected messages? What about disinfected messages? With over a thousand possible settings and policy configurations this is the core of our service:



Malware Scan - The first step in the ExchangeDefender process is a malware scan - this is where it determines if the message itself is valid and if any of the attachments are acceptable. If necessary the message is disarmed and then forwarded to the virus scanners.

Virus Scan - ExchangeDefender uses up to six different virus scanning engines to determine if any of the attachments contain viruses. If it finds a virus it will comply with your policy (delete, disinfect, quarantine), or can silently dispose of the message.

Spam Scan - Here ExchangeDefender passes the message through thousands of tests to determine if it is a SPAM or a valid/clean email. Because of the number of anti-spam techniques used in this process it averages 98% spam identification with less than 0.000004% false positive ratio (legitimate messages treated as junk mail).

Content Scan - This is the most comprehensive portion of ExchangeDefender and the most flexible because it includes the ever evolving message intelligence part of the service. It can determine if messages contain adware or spyware, if they are "phishing" with fraudulent content, if they contain adult or foreign content not suitable for your users or if they are simply things you wish not to read.

Outbound Security

ExchangeDefender provides outbound content filtering as a core component of your email infrastructure. By routing all your outbound mail through ExchangeDefender outbound servers you can restrict SMTP connections to your mail servers and offload virus and content scanning onto a server connection you can control. By scanning each message for virus content it can keep you from blacklists and minimize the chance of your server being added to a blacklist.

ExchangeDefender can also implement outbound policies that screen outgoing messages for confidential content and allow you to block quarantine or forward any suspicious information leaving your organization (accounting data, confidential contracts, etc).

Each outbound message also transparently creates a reverse trusted-sender entry (whitelist) for contacts you send mail to. Because you initiated the contact, the email address you sent mail to will be transparently added to your whitelist and their reply will bypass many SPAM filters.

Policy Enforcement

ExchangeDefender automatically applies your security policy to each message it scans, and you have a friendly web interface to properly define it. ExchangeDefender policy is very granular and easily configurable. You can establish a policy for the entire company, domain, server, and department or even allow each user to customize how their mail should be handled. There are separate control panels for the administrators and users, all easily accessible from any device with web connectivity (https).

ExchangeDefender gives you easy access to all aspects of the service including:

- antivirus** (delete, disinfect, quarantine, deliver);
- spam** (delete, bounce, quarantine, archive, forward, deliver, flag);
- attachment rules** (delete, quarantine, block, reject, deliver);
- spyware** (delete, quarantine, deliver)
- malware** (disarm, convert-to-text, quarantine)
- HIPAA compliance** (archive, deliver & store, deliver, store & forward)

Ask about InSwift's TotalCare Support

We have the expertise and tools to provide your organization with
Unlimited IT Support at a fixed price.

Let us be your guide through the technical maze that is business technology.