

BITDEFENDER SECURITY FOR EXCHANGE

MAXIMIZE YOUR EXCHANGE SECURITY

Microsoft® Exchange has become a critical communications service that must be protected to ensure business continuity. When the Exchange server stops working, so does your workforce. The impact of lost productivity combined with a severe virus outbreak propagated by email can practically bring a company to its knees. While many organizations consider the internal impact of email-borne viruses, an even greater concern is loss of reputation and damage caused by an employee accidentally sending out an infected email to partners or customers. More than anything else, damage to a company's reputation can be irreversible.

THE NEED FOR SECURE AND SPAM FREE MAILBOXES

A company's email system provides one of the main entry and exit points within the network for malicious code propagation and data leakage. Therefore, email security solutions should be able to counter the many different threats that leverage a company's email system in order to propagate - these include;

- Sending or receiving malicious code through email attachments
- Unsolicited communication in the form of Spam
- Phishing attempts to acquire confidential information
- Legitimate users leaking confidential information by email

Because of the mechanisms used to propagate email threats are becoming more virulent, stopping them at the desktop may be too late. Therefore, a solution deployed at the edge of the network and on the mail server itself can minimize the impact of malware by cleaning infected documents and ensuring the protection of your organization's most critical business asset - a communicating workforce.

SECURING EXCHANGE SERVERS WITH BITDEFENDER

BitDefender Security for Exchange safeguard's your organizations critical messaging services to protect against email-borne viruses, spyware and spam. Integrating seamlessly with Microsoft® Exchange Server, BitDefender Security for Exchange combines malware protection, antispam, antiphishing, and content filtering technologies to increase productivity and ensure the overall integrity of your email platforms.

The BitDefender's Security for Exchange scans emails in multiple levels by checking first if the sender's mail server is suspicious or blocked, and then if the content or attachments contains malicious code or match with spam related rules.



KEY FEATURES AND BENEFITS

- Scans inbound email traffic to ensure real-time antimalware protection and minimize the risk of virus propagation throughout the internal network
- Scan outbound email to stop security threats spreading to your partners and customers
- Scans each email just once by using selected scanning method to minimize the server load
- Content filtering for both inbound and outbound emails, identifying specific administrator defined keyword content such as credit card data
- High Precision Antispam and Antiphishing filters with Heuristic NeuNet technology
- Reduce resource costs and overhead to increase overall business productivity
- Minimize network downtime to increase operational efficiency
- Integration with Microsoft's Virus Scanning API to optimize and accelerate the scanning process

BITDEFENDER TECHNOLOGIES

b-have All BitDefender solutions include B-HAVE, a patent-pending technology which analyzes the behavior of potentially malicious codes inside a virtual computer, eliminating false positives and significantly increasing detection rates for new and unknown malware.

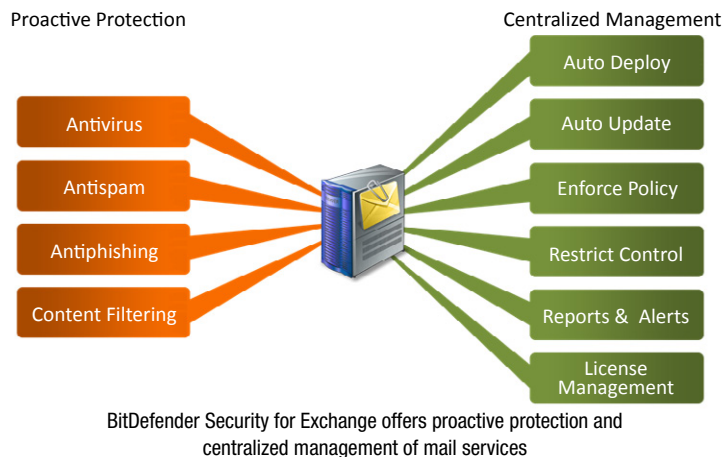
NeuNet To better deal with new spam, the BitDefender Lab has created NeuNet, a powerful antispam filter. Inside the Antispam Lab, NeuNet is pretrained on a series of spam messages so that it learns to recognize new spam by perceiving its similarities with the messages it has already examined.

INTEGRATION WITH THE BITDEFENDER CENTRAL MANAGEMENT PLATFORM

BitDefender Security for Exchange provides integration with the Management Server's Security Dashboard, giving Administrators enterprise-wide visibility into their network resources and overall security posture. The BitDefender Management Server provides a centralized point for remote installation, configuration and reporting of all BitDefender Clients, Server and Gateway products deployed within the enterprise and notifies administrators of scan performance, infections and update tasks through its comprehensive alert module.

SYSTEM REQUIREMENTS

- Windows Server 2000 SP4 + Update Rollup 1
- Windows Server 2003 with SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server (SBS) 2008
- Windows Exchange Server 2003, 2007, 2010
- Internet Explorer version 6.0 or higher



ADVANCED, PROACTIVE DETECTION AND PROTECTION

BitDefender's award-winning scan engines have been recognized by leading certification bodies, - including ICSA Labs, Virus Bulletin, and West Coast Labs - for their unmatched proactive antimalware protection. BitDefender provides multiple levels of advanced protection;

Antivirus – In addition to signature based detection, BitDefender provides heuristic detection that emulates a virtual computer-within-a-computer, checking all files and code for malicious behavior. This technique produces fewer false positives and significantly higher detection rates for zero-day and unknown threats.

Antispam – Using constantly updated blacklists and whitelists of known Spam sites, Bayesian learning provides another layer of detection that adapts to the changes made by Spammers to bypass static Spam filters.

Antispyware – BitDefender detects and prevents known spyware and adware to prevent infections by spyware leading to outbound data leakage.

Antiphishing – While considered more of personal than a corporate threat, phishing sites could also harvest information from your company's employees. Using a combination of constantly updated blacklists and configurable content inspection rules, BitDefender blocks messages requesting users to access phishing sites.

Content Filtering – Content filtering allows for the detection of predefined information such as credit card or account information, report names, client databases, etc. from passing outside the company's control.

White List/Black List – for excluding particular mail servers or implicitly allowing specific mail servers as trusted with option to validate their IP addresses to match with the sender's domain.

MULTIPLE HIGHLY CONFIGURABLE SCANNING METHODS

BitDefender Security for Exchange provides Continuous, On-Request, Transport and Full scanning methodologies to detect malicious code to safeguard the integrity of the electronic mail services. Each email will be scanned only once in any selected scanning method and fully configurable email footer can be included into each scanned email. Additional content scanning methods can be configured to avoid confidential information being sent across by selected user groups.

DEFENSE IN DEPTH

BitDefender Security for Exchange is just one element in a comprehensive suite of solutions providing end-to-end network protection from the gateway to the desktop. BitDefender's proactive, multi-platform products detect and stop viruses, spyware, adware and Trojan threats that can compromise your network integrity.

