bitdefender®
SECURITY FOR
MAIL SERVERS

THE NEED FOR SECURE AND SPAM FREE MAILBOXES

Email has become an indispensible service that businesses need to protect – at whatever the cost. When the Email 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 accidently sending out an infected email to partners or customers. More than anything else, damage to a company's reputation can be irreversible.

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
- Dictionary Harvesting Attacks (DHA)

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 EMAIL SERVICES WITH BITDEFENDER

BitDefender Security for Mail Servers protects Windows or UNIX-based mail servers for known and unknown security threats with award winning proactive antivirus, antispyware, antispam, antiphishing, content and attachment filtering technologies. The solution secures organization's email services and provides increased productivity by blocking spam and providing common centralized management tools.

The BitDefender's Security for Mail Servers scans emails in multiple levels by checking first if the sender's mail server is suspicious or blocked, and then is 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*

- *User directory protection against harvesting attacks used by Spammers in an attempt to find legitimate email addresses by brute force techniques*

- *Allows remote configuration from any computer in the organization through BitDefender's Centralized Management Server*

- *Reduce resource costs and overhead to increase overall business productivity*

- *Minimize network downtime to increase operational efficiency*

bitdefender

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.**

SYSTEM REQUIREMENTS

Windows-based Operating Systems:

- 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
- Internet Explorer version 6.0 or higher

UNIX-based Operating Systems:

Operating System: Linux, FreeBSD, Solaris
Linux Kernel: 2.6.18 or newer
glibc: 2.3.1 or newer, libstdc++ from gcc 4 or newer
Supported Distributions:

- Debian GNU/Linux 3.1 or newer
- Fedora Core 1 or newer
- FreeBSD: 5 (or newer with compat5x)
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 or newer
- Mandrake/Mandriva 9.1 or newer
- OpenSolaris 2008 or 2009 (x86 platform)
- RedHat Enterprise Linux 3, Linux 9 or newer
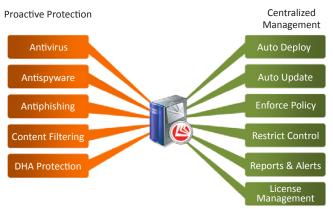- Solaris 9 or 10 (x86 platform)
- Slackware 9.x or newer

vb 100 VIRUS virusbtn.com **vb VERIFIED SPAM** virusbtn.com

bitdefender

Proactive Protection — Centralized Management

Antivirus | Auto Deploy
Antispyware | Auto Update
Antiphishing | Enforce Policy
Content Filtering | Restrict Control
DHA Protection | Reports & Alerts
License Management

BitDefender Security for Mail Servers offers proactive protection and centralized management of mail services

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 by using file scanning methods 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, thus preventing compromise.

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.

Directory Harvesting Attack (DHA) Protection – Used by spammers to find valid or existing email addresses, Directory Harvesting is more effective for finding e-mail addresses of companies as they conform to a standard. Emails can then be crafted to bypass Spam filters as they target legitimate users.

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.

SECURE, CONFIGURABLE SCANNING OPTIONS

BitDefender Security for Mail Servers provides a continuous and fully transparent scanning methodology to detect malicious code, safeguarding the integrity of the electronic mail services. Emails are scanned once and an optional footer can be amended to each message as a means to validate its security and provide end user assurance. Additional content scanning methods can be configured to avoid confidential data leakage via outbound emails to unknown external recipients.

INTEGRATION WITH THE BITDEFENDER CENTRAL MANAGEMENT PLATFORM

BitDefender Security for Mail Servers 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.