



# Bitdefender®

## Security for Mail Servers

### THE NEED FOR SECURE AND SPAM FREE MAILBOXES

Email is an indispensable 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 malware outbreak propagated by email can practically bring a company to its knees. While many organizations consider the internal impact of email-borne malware, 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.

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
- 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 Linux and Windows mail servers against known and unknown security threats with award-winning proactive antimalware, antispam, antiphishing, content and attachment filtering technologies. The solution secures organization's email services and provides increased productivity by blocking spam and attacks.

The screenshot shows the Bitdefender Security for Mail Servers web interface. At the top, it says "Logged in as administrator" and "Logout". Below the Bitdefender logo, there are tabs: "Status", "Policies", "Quarantine", "Components", "Maintenance", "Reports", and "Logging". The "Policies" tab is selected. On the left, there is a "Mail" section. The main area shows the configuration for the "Default" group. It includes sections for "Add footer", "Antivirus", "Antispam", "Content filter", and "SMTP forward". Each section has a "Status" bar and a table of settings. The "Antivirus" section has settings for "Enabled" (yes), "On virus" (disinfect, delete, quarantine), "On suspected" (disinfect, delete, quarantine), "On riskware" (disinfect, delete, quarantine), and "On password" (ignore). The "Antispam" section has settings for "Enabled" (yes) and "Actions" (ignore). The "Content filter" section has a setting for "Enabled" (yes). The "SMTP forward" section has settings for "Enabled" (no) and "When" (before scan). Each section has a "Configure" button. At the bottom, there are "Apply" and "Cancel" buttons.

Configure group 'Default'	
<b>Add footer</b>	
<input checked="" type="checkbox"/>	
<b>Antivirus</b>	
Status	
Enabled	yes
On virus	disinfect, delete, quarantine
On suspected	disinfect, delete, quarantine
On riskware	disinfect, delete, quarantine
On password	ignore
Configure	
<b>Antispam</b>	
Status	
Enabled	yes
Actions	ignore
Configure	
<b>Content filter</b>	
Status	
Enabled	yes
Configure	
<b>SMTP forward</b>	
Status	
Enabled	no
When	before scan
Configure	
Apply Cancel	



## KEY FEATURES AND BENEFITS

- Installs in minutes
- Scans inbound email traffic to ensure real-time antimalware protection and minimize the risk of malware propagation throughout the internal network
- Scans outbound email to stop security threats spreading to your partners and customers
- High precision spam and phishing protection leveraging advanced heuristic technology, machine learning and cloud intelligence
- Content filtering for both inbound and outbound emails, identifying sensitive, unwanted or dangerous content and attachments based on administrator defined rules
- Allows for flexible filtering policies based on user groups
- Easy to manage using web-based interface
- Powerful logging and alerting module provides visibility into detected threats

## ADVANCED, PROACTIVE DETECTION AND PROTECTION

Bitdefender's award-winning technologies have been recognized by leading certification bodies - including Virus Bulletin, AV-Test, and AV-Comparatives - for their unmatched antispam and antimalware protection. Bitdefender provides multiple levels of advanced protection:

**Antivirus & Antimalware** – 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 & Antiphishing** – Besides signature based detection, URL blacklists and queries to RBL servers, Bitdefender employs advanced, proactive technologies designed to provide fast response to new and unknown attacks:

- **Advanced Pattern Matching (APM)** – powerful heuristic antispam filter detects unknown spam. Based on artificial neural networks, the APM filter is trained on large volumes of spam messages inside the Bitdefender Antispam Lab. During training, it learns to distinguish between spam and legitimate emails and to recognize new spam by perceiving its similarities, often very subtle, with messages it has already examined. This filter is highly accurate, minimizing false positives.
- **Real Time Data Analysis (RTDA)** – filter employs Global Protective Network security cloud to detect spam messages and to provide rapid protection against 0-day and advanced threats.

**Content & Attachment Filtering** – administrators can define rules to identify and block unwanted or dangerous attachments, as well as sensitive information such as credit card or account information, report names, etc.

## PROTECTED MAIL SYSTEMS

- Automatic integration with industry-leading Linux-based mail servers, including Postfix (milter), Sendmail (milter), qmail, CommuniGate Pro and Courier
- Compatible with virtually any other SMTP mail system in SMTP Proxy mode

*"Bitdefender blocked 99.98% of spam – and did so without a single false positive in either corpus of legitimate emails."*

September 2015 VBSpam comparative review



## SYSTEM REQUIREMENTS

Linux kernel 2.6.18 or newer, glibc 2.3.6 or newer

• Red Hat Enterprise Linux 4 or newer • SuSE Linux Enterprise Server 10 or newer • OpenSUSE Linux 10 or newer • Debian GNU/Linux 5 or newer • Gentoo Linux • Arch Linux • Ubuntu Server 10.04 LTS or newer • CentOS 4 or newer

**TRY THE PRODUCT AT:** <http://www.bitdefender.com/business/>  
**CONTACT U.S. Business Sales by phone:** 1-800-388-8062



Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

All Rights Reserved. © 2015 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.  
FOR MORE INFORMATION VISIT: [enterprise.bitdefender.com](http://enterprise.bitdefender.com)