

# Onion Shell Security

Securing Your Business with  
BitDefender Corporate Defensive Tools



## Disclaimer

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible post-release information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide. Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

*Copyright © 2009 BitDefender. All rights reserved.*

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.

# Table of Contents

Onion Shell Security.....	1
Disclaimer.....	2
Table of Contents.....	3
About This Document.....	4
We Would Like to Hear from You .....	4
Onion Shell Security.....	5
<i>Knowing your enemy – discovering the current landscape of e-threats .....</i>	<i>5</i>
<i>Mitigating risks and dangers – appropriate defensive technology .....</i>	<i>6</i>
<i>Strategic layers for effective defense .....</i>	<i>7</i>
Perimeter.....	8
Network.....	8
Workstation .....	8
Applications and Data.....	8
<b>Core components of BitDefender Business Security .....</b>	<b>9</b>
Security for ISA Servers.....	9
Security for Mail Servers .....	10
Security for Exchange .....	10
Management Server.....	10
Security for File Servers.....	11
Security for Samba Shares.....	11
Client Security.....	11
BitDefender for Unices .....	12
Security for SharePoint Servers .....	12

## About This Document

This document is primarily intended for IT&C System's Security Managers, System and Network Administrators, Security Technology Developers, Analysts, and Researchers, but it also addresses issues pertaining to a broader audience, like small organizations or individual users concerned about the safety and integrity of their networks and systems.

## We Would Like to Hear from You

As the reader of this document, you are our most important critic and commentator. We value your opinion and want to know what you like about our work, what you dislike, what we could do better, what topics you would like to see us cover, but also any other comments and suggestions you wish to share with BitDefender's Team.

You can e-mail or write us directly to let us know what you did or did not find useful and interesting about this document, as well as what elements and details we should add to make our work stronger.

When you write, please be sure to include this document's title and author, as well as your name and phone or e-mail address. We will carefully review your comments and share them with the authors and contributors who worked on this document.

*E-mail:*

[documentation@bitdefender.com](mailto:documentation@bitdefender.com)

*Mail:*

BitDefender Headquarters

West Gate Park

24<sup>th</sup>, Preciziei Street

Building H2, Ground Floor

6<sup>th</sup> district, 062204, Bucharest

ROMANIA

# Onion Shell Security

Răzvan Livintz  
Communication Specialist

The advent and wide scale implementation of Local Area Networks and Wide Area Networks in the past twenty years facilitated the migration from standalone workstation to collaborative environments, offering both average users and corporations an ideal and easy to use platform for their daily assignments and tasks.

With the proliferation of high-speed Internet access in the last decade, the communication media have embraced new various forms, such as e-mail, rapid file transfers, instant and mobile messaging, online Web conferences, etc, that became a standard of day to day business interaction in the 2000s.

All these technologies and their rapid development opened the way to a new type of connection between individuals while also creating another bridge from companies to their customers.

But in addition to narrowing and bringing together in a virtual environment people with common interests and activities located inside the same building or scattered around several continents, LANs and WANs also need to face the dangers and risks revolving around the same collaborative principles networking implies.

## Knowing your enemy – discovering the current landscape of e-threats

E-criminals seek to take advantage of users' and systems' vulnerabilities employing different types of complex behavioral- and technological-based tactics and strategies. In the current malicious environment, the one fifth of the globe population connected to the Internet has to cope with approximate 2,000 new and mutated viruses per day, almost 50,000 phishing attempts per month and more than 1,000,000 hijacked computers that spread bots, rootkits and other malware during one year.

E-threats are to be held accountable for the significant increase of:

- *infrastructure costs* – ISPs' and other organizations' network management, antimalware solutions deployment and maintenance (at desktop, server, and Internet level), help desk assistance, etc.
- *productivity loss* – slowed networks due to the bandwidth waste, reduced e-mail processing and storage capabilities, time spent to sort and discard the unwanted messages, resource consuming collateral damages, such as detection and removal of malware, etc.

For instance, in 2005, organizations across the world have had to support a financial burden of \$ 50 billion for the e-mail spam only<sup>1</sup>. For 2007, estimations for the price to be paid for the junk mail and its subsequent damages revolved around \$ 198 billion<sup>2</sup>.

<sup>1</sup> David Ferris, Richi Jennings, Chris Williams, "The Global Economic Impact of Spam, 2005. Report #409. Ferris Analyzer Information Service", published 24 February 2005, on *Ferris Research*, <http://www.ferris.com/2005/02/24/the-global-economic-impact-of-spam-2005/>.

<sup>2</sup> As quoted by Robert Jaques, "Spam will cost business \$20.5bn this year", published 10 June 2003, on *Incisive Media's www.vnunet.com*, <http://www.vnunet.com/vnunet/news/2122506/spam-cost-business-5bn>.

In this context, securing networks should become a priority in terms of:

- protecting assets, ideas and sensitive data
- assessing and reinforcing standards, regulations and Governance, Risk Management and Compliance, such as Sarbanes-Oxley, Basel II and other relevant EU directives<sup>3</sup>
- defending investments and reducing TCO.

## Mitigating risks and dangers – appropriate defensive technology

To prevent and protect companies and organizations around the globe, BitDefender® develops and maintains a suite of security technologies. The acknowledged efficiency and added value of the safety layers complementing millions of platforms, systems, data and users worldwide also brings our customers the several key advantages:

- *Highly customizable defense solutions* – easy to integrate and corroborate with the organization essential software and applications.
- *Effective malware shield* – first class detection, accurate recognition and annihilation of viruses, worms, Trojan horses, adware, spyware, bots, etc.
- *Watchful antispam technology* – several associated e-mail protection tools forged together in an intelligent and trainable module.
- *Dedicated solutions* – for server, desktop, laptop, and mobile computing & communication real time protection.
- *Fast response time* to new electronic threats – between 2 and 4 hours.

In order to suit the clients' needs BitDefender searches, analyzes and keeps track of new methods of crafting e-threats and develops new filters to block the arising attacks. It also focuses on improving proactive detection and reaction speed.

It is much easier to prevent and save a great deal of time and money, rather than to disinfect. Also, there is a lot of research concentrating in the e-threat analysis process automation since the number of e-threats has grown exponentially in the past years. For instance, BitDefender has already implemented B-HAVE, Active Virus Control (AVC) and NeuNet as significant components of its antimalware and antispam integrated solutions.

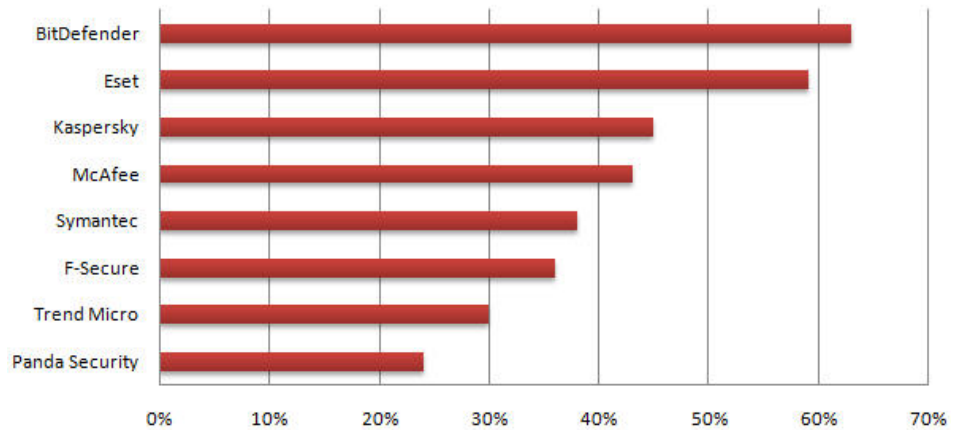
B-HAVE and AVC are dynamic heuristic scanners designed to augment the current security technology and provide proactive protection, while NeuNet is an "intelligent" spam filter, using a neural network that is pre-trained on a series of bulk messages.

New or mutated breeds of malware can be detected and annihilated based on architectural or behavioral pattern, rather than using a list of known e-threats. This led to a drastic decrease of the time elapse between the launching of malware and the issuing of an antimalware signature update (also known as window of exposure). The independent tests carried out in January 2008 by

<sup>3</sup> The European Union's Financial Services Action Plan (FSAP), The 4th directive Annual Accounts of specific type of companies (78/660/EEC), The 7th directive Consolidated accounts (83/349/EEC), The 8th directive of Company Law 1984 (84/253/EEC) and 2006 (2006/43/EC), The Consolidated Admissions and Reporting directive (CARD) (2001/34/EC), The Transparency directive (2004/109/EC), The Insider Dealing directive (1989/592/EEC) & The Market Abuse directive (2003/6/EC).

Anti-Malware Test Lab already proved that BitDefender’s B-HAVE heuristics detect 63% of e-threats, without needing a signature<sup>4</sup>.

**Proactive antivirus protection test**



Active Virus Control (AVC) is an advanced heuristic scanner engineered to perform a real-time check of the active processes running on a particular system, monitoring them since their start. Its crucial mission is to analyze and compare against various potentially malicious actions any suspicious activity. If any potentially malicious process is identified, Active Virus Control neutralizes it to safeguard the integrity of the system. The tests conducted by BitDefender in April 2009 on a collection of malware samples available in the wild demonstrated that the detection rate of Active Virus Control is 95.5%.

As spam requires more and more attention due to its variety and emergence speed, detection methods must adapt to this pattern- shifting reality. More complex spam types require more intelligent detection engines. To better deal with new spam, BitDefender has created NeuNet<sup>5</sup> (short for Neural Network), a powerful antispam filter. NeuNet is pre-trained by the BitDefender Antispam Lab 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. Freshly-trained versions of the network are shipped regularly to clients as part of the regular update process.

**Strategic layers for effective defense**

The BitDefender Business Security package can be tailored for different computer networks defensive needs. It is a fully-automated security suite that allows network administrators to implement security policies, to manage the entire network from one computer. The Business Security Suite is able to detect the newly-added workstations into the network and automatically installs the security software to keep them safe.

The different components of BitDefender Business Security can be deployed to ensure the safety of various network layers:

<sup>4</sup> See "Testing of proactive antivirus protection: Key results from the proactive antivirus protection test", published 14 January 2008, in *Anti-Malware Test Lab*, <http://www.anti-malwaretest.com/?q=node/39>.

<sup>5</sup> For a thorough description of the NeuNet filter, please see the whitepaper, "BitDefender Antispam NeuNet", available on *BitDefender*, [http://www.bitdefender.com/files/Main/file/BitDefender\\_Antispam\\_NeuNet.pdf](http://www.bitdefender.com/files/Main/file/BitDefender_Antispam_NeuNet.pdf).

## Perimeter

The perimeter is the first line of defense. It could be understood as the first and last point of contact for the security tools that protect corporate network, or the border between the local network and the Internet.

The network perimeter also translates as the gateway to the outside world. Once it is compromised, it could inflict corporate ability to conduct business. Probably the best example is to be found in companies that run Web-based business and which obtain revenue from visitors via on-line purchases or transactions. Breaching such a network perimeter ultimately means that business servers will also be exposed and orders or sales affected.

The following BitDefender solutions provide security at the network perimeter:

- BitDefender Security for ISA Servers
- BitDefender Security for Mail Servers
- BitDefender Security Exchange Servers

## Network

The network level represents the LAN and/or WAN. Usually, a network consists of clients and servers, desktops and laptops, and even more complex remote connections for telecommuters, teleworkers and road warriors.

Network level security is crucial especially in terms of productivity loss and infrastructure costs. Without the appropriate defensive solution, it is sufficient to compromise a single machine in order to disrupt the entire network's operation.

The following BitDefender solutions provide security at the network level:

- BitDefender Management Server
- BitDefender Security for File Servers
- BitDefender Security for Samba Shares

## Workstation

Unlike servers, which gather most of the focus of network administrators, especially in terms of security and defensive measures, clients are not scrutinized with the same intensity. There are more of them which make maintenance more laborious and their flexibility makes even small company infrastructure, highly complex.

Client computers are technically the access gate to different types of sensitive content that normally resides on the server and cannot be otherwise retrieved. Even if it is almost impossible for one to connect a mobile HDD to a server and to start copying information, it is nonetheless very likely that one access the data stored on the server from a client machine and copies it on a USB stick, bypassing and breaking thus an entire set of policies.

The following technologies provide security at the workstation level:

- BitDefender Client Security
- BitDefender for Unices

## Applications and Data

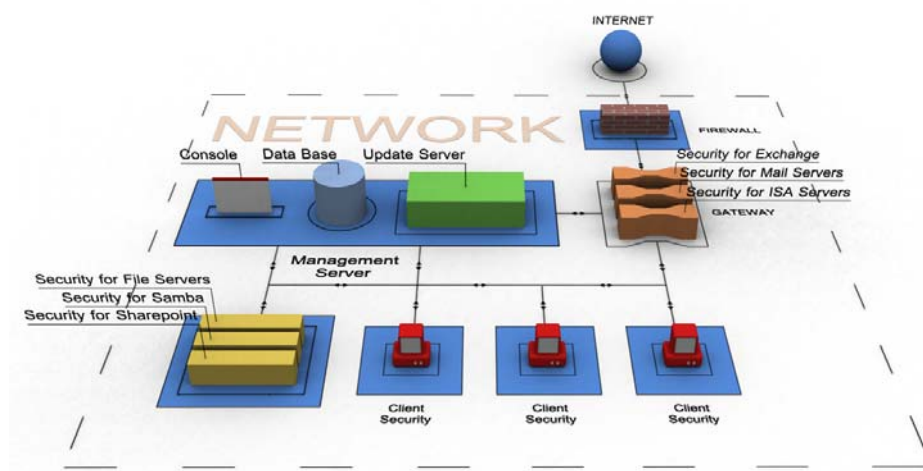
Insufficiently protected applications can provide easy access to confidential data and records. Applications that are being deployed over the Web for the ease of access by customers or remote employees are another risk to be considered.

Classified and sensitive data are the core of every business and they should be considered by every security strategy. In the absence of a strong access policies management they are extremely easy to grasp.

The following technologies provide security at the application and data level:

- BitDefender Security for File Servers
- BitDefender Security for Exchange Servers
- BitDefender Security for SharePoint Server
- BitDefender Security for Samba Shares

The diagram below describes the different components that Business Security package could integrate:



## Core components of BitDefender Business Security

### Security for ISA Servers

BitDefender Security for ISA Servers offers antivirus and antispyware protection for Web traffic, including protection for data received through webmail. BitDefender Security for ISA Servers integrates with the Microsoft Internet Security and Acceleration (ISA) Servers through two application filters (ISAPI), offering antivirus and antispyware protection for HTTP, FTP, and FTP through HTTP traffic.

BitDefender Security for ISA Servers fights Internet-borne malware by filtering and blocking the HTTP and FTP traffic that carries potentially dangerous active codes and protects arrays that run on Microsoft ISA Server Enterprise Edition. It also isolates dangerous or restricted files in a quarantine zone for later actions to be pursued.

BitDefender Security for ISA Servers eliminates the risk of browser blocking and timeouts associated with large file downloads because it gradually scans and sends parts of the requested data to the browser, while the download is in progress. It can also integrate with BitDefender Security for Mail Servers to protect SMTP traffic against viruses and spam.

## Security for Mail Servers

Designed for mail servers running on Windows or UNIX-based platforms, BitDefender Security for Mail Servers brings together antivirus, antispyware, antispam, antiphishing, and content/attachment filtering engines that secure the mail traffic of companies and Service Providers. Compatible with most e-mail platforms, the product offers advanced malware protection.

BitDefender Security for Mail Servers offers anti-phishing protection by proactively detecting forged messages intended to trick their recipient into disclosing confidential data.

It includes dedicated agents for automatic integration with several of the most popular mail transfer agents, such as Sendmail (milter), Postfix, Courier, qmail and CommuniGate Pro, and can act as a multiple mail server proxy through interfaces capable of filtering the traffic routed to different mail servers.

Through its optimized scanning process, BitDefender Security for Mail Servers increases mail delivery speed and reduces server workload, thus improving productivity and preventing the loss of confidential information.

BitDefender Security for Mail Servers provides a highly efficient multi-layered antispam protection system which reduces mail traffic by accurately classifying messages as spam, phishing or legitimate and blocking unsolicited mail based on several filters, such as Black/White Lists, trainable Bayesian Filter and proactive NeuNet filter. Supplementary, the Directory Harvesting filter protects against attempts to steal valid mail addresses from the mail server.

BitDefender Security for Mail Servers also offers the possibility of separately handling riskware (applications that pose a potential threat, but which certain user groups might still need).

## Security for Exchange

BitDefender Security for Exchange brings together antivirus, antispyware, antispam, antiphishing, and content/attachment filtering. It seamlessly integrates with the MS Exchange Server to create a malware-free messaging environment.

## Management Server

The Management Server automatically detects any newly connected computers. It can then deploy client security to the new endpoint, utilizing pre-set security policies that can be configured down to the group level.

It also enables Windows Management Instrumentation (WMI) scripting on groups of network workstations and provides scheduling capabilities to reduce the administration effort and centralize results. Thus, IT administrators can perform network audit (gathering of hardware and system information from workstations) and administrative actions remotely.

Management Servers provide enterprise-wide network visibility, throughout its centralized Security Dashboard, detailed reporting capabilities and network auditing potential. The Dashboard monitors the network status and displays key security information, including areas of concern, being also the centralized point to delve deeper into system administration and configuration.

The enhanced reporting tool enables the administrator to generate statistics on network issues, updates, installation, etc., using predefined templates or customized reports based on Crystal reports.

The same WMI administration scripts previously mentioned gather hardware and system information about the workstations, hardware properties, startup programs, installed software, hot fixes, and service packs, etc.

## Security for File Servers

BitDefender Security for Windows-based File Servers protects file traffic from viruses, spyware, rootkits, and other malware utilizing proactive protection. Security for File Servers lowers the administrative burden through its integration with BitDefender's Management Server, allowing centralized visibility and control of server security enterprise wide.

It helps increasing productivity by scanning and fingerprinting as "read-only" the files just once during the same session; it only re-scans them if there is a new session, an update or an infection in the system.

It gives fast and secure file access, thanks to its advanced multithread scanning functionality and optimizes the number of scan instances by automatically detecting the number of processors used.

BitDefender Security for File Servers has the ability to scan each accessed or copied file in real-time with no impact upon file server performance and offers a configurable scheduler for on-demand antivirus scans and update tasks. Supplementary, it has an increased scanning speed because it allows preventing safe processes from being scanned.

## Security for Samba Shares

BitDefender Security for Samba provides antivirus and antispysware protection for Samba network shares. By scanning all accessed files for known and unknown malware it keeps network users safe and it helps comply with data protection regulations. The open source BitDefender vfs module provides flexibility, allowing it to be compiled against any Samba version, making it the best choice for your favorite Unix-based system.

## Client Security

BitDefender Client Security provides protection from viruses, spyware, rootkits, spam, phishing, and other malware. BitDefender's proactive protection provides best-in-the-business protection from even zero-day threats. The centralized management server can auto-detect new endpoints and deploy client security to any workstation in your enterprise.

BitDefender Client Security is a robust and easy to use business security and management solution based on two major components:

- BitDefender Business Client once installed on the company's workstations, it provides industry leading proactive protection against viruses, spyware, rootkits, spam, phishing and other malware.
- BitDefender Management Server
  - automatically performs routine and recurrent activities for a more efficient network management
  - ensures security compliance by applying consistent policies throughout the network
  - manages and controls BitDefender Business Client and other BitDefender server solutions.

## BitDefender for Unices

BitDefender Antivirus Scanner for Unices is a versatile on-demand scanner built for Linux and FreeBSD systems. It provides antivirus and antispymware scanning for both UNIX and Windows-based partitions.

BitDefender Antivirus Scanner for Unices has script and extension-based integration with various applications and services, such as e-mail clients (Pine, Evolution), mail server services and scheduling services (Cron), ensuring scan and update automation.

Its classic command line scanner is complemented with a graphical user interface for better integration with desktop environments. BitDefender Antivirus Scanner for Unices includes three popular file manager plug-ins from the GUI package: Konqueror (KDE), Nautilus (GNOME) and Thunar (Xfce).

## Security for SharePoint Servers

BitDefender Security for SharePoint provides antivirus and antispymware protection for Microsoft SharePoint Server. BitDefender Security for SharePoint scans files uploaded into and downloaded from document libraries and lists, in real-time, with excellent cleanup rates and an option to quarantine infected files. This solution allows safe team collaboration inside business networks, while preventing infected files from compromising the confidentiality of business activities.

BitDefender Security for SharePoint ensures fast, secure collaboration, thanks to its advanced and tight integration with Microsoft Virus Scanning API and offers a configurable scheduler for on-demand antivirus scans and update tasks. It also notifies administrators about the performance of scan and update tasks through its efficient alerts module.

BitDefender® is the creator of one of the industry's fastest and most effective lines of internationally [certified security software](#). Since our inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe – giving them the peace of mind of knowing that their digital experiences are secure. BitDefender solutions are distributed by a global network of value added distribution and reseller partners in more than 100 countries worldwide. For more details about BitDefender's security solutions, please check [www.bitdefender.com](http://www.bitdefender.com).