

# bitdefender® CLIENT SECURITY

## THE FOUNDATION OF BUSINESS SECURITY

The security requirements for any new or existing company – no matter how large or small - should be the same. While protecting your company's intellectual property and securing customer data are good business practices, the impact of any virus outbreak greatly affects the company's operational efficiency and can incur lost productivity from the workforce. This loss of productivity can cripple a small company and at best, hamper the company's growth.

## ANTIVIRUS IS NOT ENOUGH

Threats are constantly evolving to circumvent the security controls your organization puts in place. While antivirus is the foundation of a good security policy, it is no longer the only answer to protecting your workforce from malicious threats. Threats that cause significant business disruption can include:



**Viruses:** Transmitted by infecting executable files, hidden inside of compressed archives or as macros within legitimate documents. Virus payloads include deleting files, encrypting data, wiping the hard disk, etc.



**Adware/Spyware:** Almost as disruptive and dangerous as a virus, spyware can be difficult to identify and hard to remove. Personal and corporate data leakage is a key concern, in addition to deteriorating workstation performance, installing additional software and redirecting browser activity. Badly infected systems may require a complete system reinstall, wasting hours of IT time and resources.



**Worms:** A self replicating program that uses the network to propagate, slowing down networks and infecting systems by leveraging system and application vulnerabilities. Payloads can include the deletion or encryption of files, emailing out documents, installing backdoors, zombies and Trojans.



**Trojans and Root Kits:** Trojans and Root Kits appear to be legitimate programs but are designed to allow remote access to a computer system. Once a Trojan or Root Kit has been installed, it is possible for an attacker to access the system remotely and often can lead to data theft. Detecting and preventing these types of threats manually can be time consuming and often lead to a complete system reinstall if improperly removed.



**Email Spam and Phishing:** Unsolicited commercial advertisements distributed via email are more than just an annoyance. Spam consumes too much of peoples' personal time if not managed properly. Some Spam or phishing attacks may also include malware as attachments - leading to internal compromise if executed – or links to websites requesting personal information. Phishing uses similar techniques but directs the user to a seemingly legitimate website in order to harvest personal information, such as credit card or bank account information or dropping keyloggers onto the system that can harvest sensitive company information.

The impact of malware can be a severe disruption to everyone in the organization - however, it is the IT department that feels the after-effects the most. IT administrators that have dealt with the removal of a quickly propagating worm or virus that has infected a large number of systems knows that it is a long, time consuming task. Unfortunately, that task must take precedence over other IT projects to limit data loss and restore workforce efficiency as quickly as possible.

## SECURING YOUR ENDPOINTS WITH BITDEFENDER

The answer to data loss and lost productivity from malware is proactive protection. Companies can effectively protect their endpoints from attack by using BitDefender's ability to detect and prevent known and zero-day threats, ensure compliance to corporate security policies and manage them effectively with fewer IT resources.



## KEY FEATURES AND BENEFITS

- **Award winning virus detection, cleaning and quarantine of viruses, spyware/ adware, Trojans and rootkits**
- **Allows flexible scheduling of on-demand or immediate execution scans for up-to-date infection assessments**
- **Optimized scanning using file fingerprinting for each user session and re-scans them upon new session creation, an update, or on infection of the system**
- **Quarantine's infected or suspected files for to minimize infections and later safe analysis**
- **Policy-based configuration and management**
- **Personal firewall protection for remote and roaming users**
- **System level spam protection with constantly updated whitelists/blacklists and Bayesian learning engine to identify new spam that bypass traditional filters**
- **Customizable content filtering to identify sensitive information to minimize data leakage**
- **Reduce resource costs and overhead of managing multiple clients using a central management console.**
- **Allows remote configuration, auditing, installation, and application removal from any client or server system in the network**

## 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

### BitDefender Business Client for Windows Intel Pentium compatible processor:

- 500 MHz for Windows 2000
- 800 MHz for Windows XP
- 1 GHz for Windows Vista, Windows 7

### RAM memory:

- 512 MB for Windows 2000, Windows XP
- 1 GB RAM for Windows Vista, Windows 7

### Minimum hard disk space:

- 1 GB

### Operating system:

- Windows 7, Windows Vista SP1, Windows XP (SP2), Windows Home Server, Windows 2000 Professional (SP4 Rollup 1 v2)

### BitDefender Management Agent Intel Pentium compatible processor

### Minimum RAM memory:

- 256 MB of RAM for Windows 2000, Windows XP, Windows 2003
- 512 MB of RAM for Windows Vista, Windows 2008, Windows 7

### Minimum hard disk space: 100MB

### Operating system:

- Windows 2000 Professional with SP 4 and Update Rollup 1 Version 2
- Windows 2000 Server with Service Pack 4
- Windows XP with Service Pack 2
- Windows Server 2003 with Service Pack 2
- Windows Vista
- Windows 2008 Server
- Windows 7
- Linux 2.4.x or 2.6.x with glibc 2.3.1 or newer and libstdc++5 from gcc 3.2.2 or newer



All trademarks, trade names, and products referenced herein are property of their respective owners. All Rights Reserved.

© 2010 BitDefender.

### Proactive Protection

- Antivirus
- Antispam
- Antiphishing
- Antispyware
- Content Filtering
- Firewall

### Centralized Management

- Auto Deploy
- Auto Update
- Enforce Policy
- Restrict Control
- Reports & Alerts
- License Management

BitDefender Client Security offers multiple levels of protection and client management functionality

## ADVANCED, PROACTIVE DETECTION

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 Client Security provides multiple levels of advanced protection: Antivirus, Antispam, Antispyware, Antiphishing, Content Filtering, Trojan / Rootkit detection and a fully featured personal Firewall.



## GRANULAR SCAN CONFIGURATION AND MANAGEMENT

BitDefender Client Security provides multiple scanning methodologies to detect malicious code to safeguard the integrity of the laptops and workstations deploying within your network. Different scanning options help maintain system integrity while minimizing the impact to the user experience.

**On Access**, real-time scanning engine to detect viruses in real-time when a user adds or retrieves a document to a document library or list.

**On-Demand** scanning features allow for scheduled system scans to be performed outside of peak work hours without impacting the overall performance or availability of the system.

**Scheduled Scanning Configuration** provides configurable event scheduling for on-demand scans and update tasks, minimizing any potential server impact or system disruption during core operating hours.

**Infected or Suspected File Quarantine** suspected files are isolated in quarantine zones. The files can either be cleaned or kept in a quarantine zone for analysis, restored to its original location once validated, or sent directly to BitDefender's Antivirus Lab for assessment.

## AUTOMATIC UPDATES

Hourly updates are provided for new virus definitions and new product updates can be deployed during a scheduled maintenance window, ensuring your Client Security deployment is current with the very latest threat protection - without disrupting your network.

## INTEGRATION WITH THE BITDEFENDER CENTRALIZED MANAGEMENT PLATFORM

Large numbers of workstations can be quickly and easily managed via BitDefender's Centralized Management platform, giving IT administrators organization-wide visibility into malware threats and the ability to proactively protect their network resources. 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.