

# BITDEFENDER CENTRALIZED MANAGEMENT



## CENTRALIZED MANAGEMENT FOR BUSINESS SECURITY

One of the greatest challenges for any IT department is the ability to maintain control and visibility into the company's security posture. Unfortunately, many organizations do not have a dedicated resource that can develop and manage a network security strategy due to the costs involved. Small and medium businesses (SMB's) are even further limited by strict budget requirements and IT tasks are often fulfilled by someone in a dual role. This lack of business prioritization makes the implementation of an effective security program difficult to achieve within most SMB's.

As a company grows, the addition of new employees, systems, and applications to support new business initiatives also increases the number of overall attack vectors used by malware to infiltrate a company's network. To be proactive, IT departments must put controls in place to limit the impact caused by unauthorized use of rogue applications, malicious code and Internet resources - such as Web 2.0 applications - that further expose the organization to attack.

## ENDPOINT SECURITY SOLUTIONS ARE NOT ENOUGH

Antivirus deployed on a company's laptops and workstations will provide the foundation of a good security policy, but it is no longer enough to protect your workforce from today's malicious threats. Threats are constantly evolving to circumvent the security solutions put in place and can spread rapidly when not checked by a compensating control. Therefore, BitDefender's antimalware solutions have evolved beyond basic virus detection and prevention to provide a solution that can proactively install protection on unmanaged workstations and servers, remotely identify and remove unauthorized application and configure system settings - helping to minimize the effects of malware propagation throughout the network.

## SECURING YOUR BUSINESS WITH BITDEFENDER

BitDefender's Centralized Management Console allows companies to implement a unified management platform for remote installation, configuration and reporting of all BitDefender Clients, Server and Gateway products deployed throughout the network. BitDefender's Centralized Management includes:

- Network-wide visibility for IT administrators into all malware related incidents
- Proactive audits for hardware and software assets within the network
- Remote configuration and management of client and server system settings
- Malware related incident reports to identify infection rates and trends
- Tools to measure the effectiveness of an organization's antimalware security program



## KEY FEATURES AND BENEFITS

- Reduce resource costs and overhead for managing multiple endpoints and servers
- On-demand problem consolidation with one click resolution
- Allows remote configuration, auditing, installation, and application removal from any endpoint or server system in the network
- Network detection of endpoints that have no antivirus solutions installed and allows remote Client Security deployments
- Configurable Security Policies with pre-defined templates to aid policy enforcement
- Integrates with Active Directory to leverage the organizations existing Windows domain structure and group policies
- Allows remote configuration from any computer in the organization through a management console
- Scalable Master-Slave Architecture to manage gateways, servers and endpoints located in different physical locations

## ENDPOINT AUDITING AND MANAGEMENT SCRIPTS

The BitDefender's Management Server is utilizing Microsoft's Windows Management Instrumentation (WMI) Scripting Language for Endpoint and Server auditing and management. Over 30 Predefined WMI Script templates are included to automate remote management. In addition, hundreds of publically available scripts for mass; Kill applications and processes, Install and uninstall software, Restart or shutdown workstations, Enable/disable autoruns and USB removable media access.

## DEFENSE IN DEPTH

BitDefender's Centralized Management is the core 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.

## SYSTEM REQUIREMENTS

The BitDefender's Centralized Management solution contains three main components: Management Server to enable centralized management backend for all BitDefender solution, Management Console for the user interface and Update Server for downloading and distributing product and virus definition updates.

**Minimum processor:** Intel Pentium 1GHz (2GHz recommended)

**Minimum RAM memory:** 512MB (2GB recommended)

**Minimum hard disk space:** 1.5GB (2.5GB recommended), 3GB for upgrades

### Operating System:

- Windows 2000 Professional, SP4
- Windows 2000 Server, SP4
- Windows XP, SP2
- Windows Server 2003, SP2
- Windows Vista
- Windows 2008 Server
- Windows 7

### Database :

- Microsoft SQL Server 2005, 2008 or Microsoft SQL Express Edition (free)



BitDefender's Console can manage gateways, endpoints, and critical servers from a centralized location

## VISIBILITY AND REMOTE MANAGEMENT CAPABILITIES

Simple to deploy and easy to manage, BitDefender's Management Console combines both visibility into a company's security posture with remote endpoint configuration and policy enforcement via a centralized interface. The Management Console consolidates threat information and system status from across all the managed Windows and UNIX-based workstation and servers running within the organization's network. Endpoint system events and critical issues are quickly identified and easily resolved with "one click" problem resolution, minimizing administration and response times to critical incidents.



BitDefender's UNIX-based solutions utilize a separate Remote Web Administration interface for BitDefender Security for Mail Servers, or BitDefender Security for Samba File Servers. In addition to the Web Remote Administration interface, a Command Line Interface (CLI) is available for advanced users that prefer a common interface for administrating their network infrastructure.

## MANAGEMENT SERVER'S MASTER/SLAVE ARCHITECTURE

Centralized policy, product and update synchronization is controlled throughout the organization by using a Master Management Server. It ensures centralized and intelligent distribution of updates within the local network or remotely managed networks running a local Slave Management Server. The architecture ensures the updates are available to local resources to optimize network utilization.

## AUTOMATIC OR SCHEDULED UPDATE DISTRIBUTION

BitDefender Management Server enables intelligent distribution of new virus definitions and product updates from a central location. Updates can either be applied automatically once an hour when they become available, or scheduled to be applied during off-peak times to minimize performance degradation and impact to the network.

## MANAGED SECURITY POLICIES BASED ON WINDOWS DOMAIN STRUCTURE

Integration into Active Directory leverages the organizations existing Windows domain structure and group policies. Security policies can be applied directly by selecting users or user groups from the Active Directory as an alternative for managing workstation groups within the Management Server. The BitDefender's Management Server detects unmanaged workstations for easily identifying them and either making them managed by automated remote deployment, or excluding selected workstations from the common security policies.