BITDEFENDER

INTEGRATED NETWORK SECURITY, AUDIT AND SYSTEM MANAGEMENT

PROACTIVE SYSTEM MANAGEMENT ENHANCES NETWORK SECURITY

IT departments are expected to operate effectively with very few resources, leaving limited time to implement proactive processes and procedures to minimise their exposure to threats. 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. With so many business and IT requirements to be met, overstretched resources find it hard to implement and maintain both security solutions and automated system auditing and management tools to automate repetitive manual tasks, help improve the overall security of the network or aid in compliance reporting.

INCREASED SECURITY AND PRODUCTIVITY WITH AUTOMATION

As a company grows, the addition of new employees, systems, and office applications also increases the complexity of an organization's network. The addition of each new desktop, laptop or server must be managed by existing IT staff, reducing the ability to maintain control and complicates efforts to visualize what is really happening in the network. To be proactive and to work smarter, IT departments must ensure they have simple and effective tools that can help automate repetitive and manual IT tasks, in addition to providing better visibility of the devices and applications needed for business operations. Automated tools can quickly expose security holes – such as unauthorized use of rogue applications or unknown devices running services that further expose an organization to potential security risks including data leakage, malware infections and virus outbreaks.

MINIMISING RISK WHILE MANAGING THE NETWORK

Simple to deploy and easy to manage, BitDefender's Business Security solutions provide visibility into an organization's network security posture, in addition to streamlining critical IT management related tasks. The Centralised Management consolidates traditional corporate antimalware functionality with wizard-driven Network Tools that simplifies mass remote configuration management and network-wide auditing of Windows-based desktops and servers.

Integrated Network Security, Audit and System Management allows companies to:
- Simplify network management and reduce manual reporting burden
- Automate network audit data collection for inventory and change reporting
- Ensure compliancy with software licenses and identify unauthorized applications
- Reduce overhead for managing a separate inventory system and agents on endpoints
- Identify easily HW/SW that is outdated or out-of-limits by using query functionality

KEY FEATURES AND BENEFITS

- Reduce resource costs and overhead by streamlining critical IT management tasks

- Automate network audit data collection for database driven inventory and change reporting

- Improve the overall security of the network and aid in compliance reporting

- Avoid overhead for managing a separate inventory system and agents on endpoints

- Simplify network management with wizard-driven Network Tasks

- Automate remote configuration, software installations and updates on Windows endpoints

- Locate unauthorized applications or processes and automate their removal from the network

- Ensure installed software within the network complies with actually licensed software

- Identify HW/SW that does not meet minimum requirements of your network

- Reduce manual reporting burden with predefined and custom reporting templates

bitdefender
CENTRALIZED MANAGEMENT
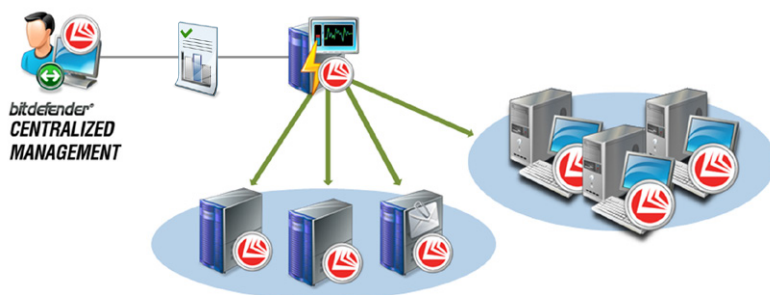
bitdefender

NETWORK AUDIT AND SYSTEM MANAGEMENT

The BitDefender's Management Server utilizes Microsoft's Windows Management Instrumentation (WMI) Scripting Language for Endpoint and Server auditing and management. More than 30 Predefined WMI Script templates are included to automate remote management; Kill applications and processes, Install and uninstall software, Restart or shutdown workstations, Enable/disable autoruns, and USB removable media access.

SYSTEM REQUIREMENTS

BitDefender's Centralised Management solution contains a Management Server which enables centralised management backend for all BitDefender solutions, Management Console for the user interface, and Agent for managing the endpoints.

BitDefender Management Server and Update Server
Processor:
- Intel Pentium 1.6 GHz

RAM memory:
- 512 MB for Windows 2000
- 756 MB for Windows XP and Windows 2003
- 1.5 GB for Windows Vista, Windows 2008, Windows 7

Hard disk space:
- 1.5 GB, 3GB for installation or upgrade

Operating system:
- Windows 2000 Professional/Server (SP4 Update 1 Ver.2), Windows XP (SP2), Windows Server 2003 (SP2), Windows Vista (SP1), Windows 2008 / 2008 SBS / 2008 R2, Windows 7

BitDefender Management Server:
- Microsoft SQL Server 2005 / Express Edition (included), Microsoft SQL Server 2008

BitDefender Update Server:
- Internet Explorer 7(+), Internet Explorer 6(+) for Windows 2000, Mozilla Firefox 2.0(+)

BitDefender Management Console:
- Internet Explorer 6.0(+)
- Microsoft Management Console (MMC) 3.0(+)
- Minimum resolution: 1024x768 / 16 bit

Software Audit

Hardware Audit

Remote Manage

Mass Configure

Audit Reports

Change Reports

BitDefender's Network Tools can remotely manage and audit organization's network from a centralised location

NETWORK AUDITING FOR COMPLIANCE AND TRACKING CHANGES

Many businesses may not have the resources to invest in a specialized asset management application, but the need to be aware of installed software within their network for compliancy to financial, governmental or industry mandates. To help address this problem, BitDefender Management Server can be configured to collect information on systems deployed within the network and scheduled for collection at daily intervals to provide IT managers with historical and up-to-date inventory via audit reports for internal as well as external audit requirements.

The Network Auditing wizard provides four standard report formats:

- **Snapshot Report Wizard**, to view the current software and hardware configurations
- **Comparison Report Wizard**, to compare installed software for two different points in time
- **Historical Report Wizard**, to view installed software details within a specified time period
- **Custom Report**, to define query based on CPU, Disk, OS, Motherboard or Software

Both software and hardware details are available on-demand for each Windows desktop or server, while historical change management reports allow for the tracking all installed or uninstalled software within the network - within a specific time period - for full visibility into the changes once a baseline has been defined. Custom reports include all the most common parameters for: CPU type and speed; disk drives, file system and remaining space; Operating System and specific Service Packs; Motherboard manufacturers, serial number and version; Virtual memory page file's size and location; Physical memory; Installed Software by name and version (e.g. Microsoft Office or Outlook).

REMOTE NETWORK MANAGEMENT, WITH MINIMUM EFFORT

The BitDefender Management Server enables IT staff to do more in less time by utilizing simple remote Network Tasks that provide over 30 ready-to-use Windows Management Instrumentation (WMI) scripting templates. A wizard-driven interface provides step-by-step configuration of all the necessary parameters, with immediate or scheduled execution on selected computers or on computer groups within the network.

The Network Tasks can manage remotely installed applications and running processes or services, the Windows Update process, or defining access to local USB removable media. These configuration management changes can be applied on-masse automatically to selected Windows systems within the network, freeing up IT staff for other, more important and less menial responsibilities.

DEFENCE IN DEPTH

BitDefender's Centralised 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.