

# BITDEFENDER SECURITY FOR SHAREPOINT



## DOCUMENT COLLABORATION BECOMES MAINSTREAM

Document collaboration is quickly becoming a key initiative to help boost corporate productivity and effectiveness. Organizations deploying web-based collaboration technologies such as Microsoft® SharePoint® allow departments to create unlimited individual SharePoint websites in order to easily create, share and manage group project documentation. Each site is accessible from a standard web browser and SharePoint's permits document version control through a standard check-in and check-out procedure.

Organizations can easily consolidate individual SharePoint websites across an entire enterprise by using a Windows SharePoint Portal Server. The Portal Server extends the capabilities of Windows SharePoint Services by providing management tools for SharePoint sites, enabling different departments to publish information accessible to the entire organization.

## THE NEED FOR SECURE DOCUMENT COLLABORATION

Collaboration systems have allowed employees and partners to greatly increase productivity; however, they have also become an easy access point for malicious code that can cripple a company's infrastructure and waste an enormous amount of time, money and resources when an infection strikes. As Microsoft SharePoint becomes a central repository for many organizations, protection against the propagation of malicious code via SharePoint resources should be high on the list of IT priorities.

Unfortunately, many network administrators incorrectly assume that their desktop and file server antivirus solutions will detect SharePoint-related viruses and malicious code. If undetected, viruses have the potential of remaining stored in the SQL based document libraries for months, sometimes even years at a time. Some collaboration systems even allow users to check out and alter documents without ever saving the file to their local system, therefore bypassing desktop antivirus solution. If infected, these documents can propagate viruses and worms throughout the organization.

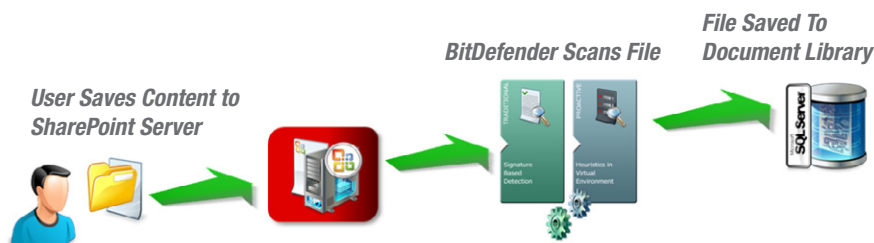
Viruses can be easily introduced into SharePoint sites in a number of different ways, including saving infected document files to the document library, saving HTML web pages with malicious macro's, embedded viruses, and Trojans, or via an infection propagated through a mapped network drive.

## SECURING SHAREPOINT WITH BITDEFENDER

Companies can protect their SharePoint deployments from attack by using BitDefender's ability to scan for content within a document to help ensure compliance to corporate security policies and prevent sensitive data from being distributed outside of the organization.

## KEY FEATURES AND BENEFITS


- Award winning virus detection, cleaning and quarantine
- Minimize network downtime to increase operational efficiency
- Reduce resource costs and overhead
- Scans file traffic ensuring real-time antimalware protection to minimize the risk of malware propagation throughout the network
- Scans and fingerprints "read-only" files just once during the same session and only re-scans them if there is a new session, an update or an infection in the system
- Allows flexible scheduling of on-demand or immediate execution scans for possible infection assessment
- Quarantine's infected or suspected files, minimizing risk of propagation
- Allows remote configuration from any computer in the organization through a web configuration console
- Mail archive support for Dbx, Mbx, Pst, Mime, Mbox, Hqx, Uudecode, and Tnef file formats



## ADVANCED FEATURES

- Integration with BitDefender's Management Server
- Centralized dashboard providing deployment status overview with alert thresholds
- Custom antivirus scanning profiles (high, medium, low, create your own) to allow improved flexibility
- Safely quarantine suspicious files, with optional restore to original location feature
- Integration with Microsoft's Virus Scanning API to optimize and accelerate the scanning process

## BITDEFENDER TECHNOLOGIES

 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.

## DEFENSE IN DEPTH

BitDefender Security for SharePoint is just one 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

- Windows Server 2003 with SP1
- Windows Server 2008, Windows Server 2008 R2
- Microsoft SharePoint Portal Server 2003
- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Services 2.0, 3.0
- Internet Explorer version 6.0 or higher

SharePoint  
Repository  
Protection

Antivirus

Antispyware

Rootkit Detection



Centralized  
Management

Auto Deploy

Auto Update

Enforce Policy

Reports & Alerts

License  
Management

BitDefender's antimalware detection, management and reporting features ensures safe document sharing throughout the organization

## GRANULAR SCAN CONFIGURATION AND MANAGEMENT

BitDefender Security for SharePoint provides on access, on-demand and scheduled scanning methodologies to detect malicious code and use quarantine zones to safeguard the integrity of the SharePoint repository. 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.

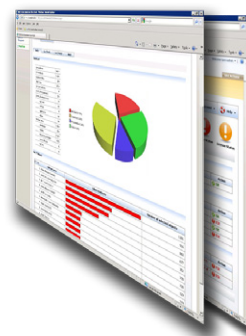
**Antivirus** In addition to signature based detection, BitDefender provides heuristic detection that emulates a virtual computer-within-a-computer, checking all files and code for malicious behavior. This technique produces fewer false positives and significantly higher detection rates for zero-day and unknown threats.

**Antispyware** BitDefender detects and prevents known spyware and adware to prevent infections by spyware leading to outbound data leakage.

**Trojans and Root Kits** that are designed to allow remote access to a computer system can be detected by BitDefender's scanning engine. Detecting and preventing these types of threats manually can be time consuming and often lead to a complete system reinstall if improperly removed.

## REPORTING AND ALERTING

Integrated directly into the SharePoint Central Administration interface, BitDefender Security for SharePoint provides predefined reports on infections, quarantined files, cleaned files and update status. Email alerts can be customized to inform administrators or create help desk tickets



## INTEGRATION WITH THE BITDEFENDER CENTRAL MANAGEMENT PLATFORM

BitDefender Security for SharePoint provides integration with the Management Server's Security Dashboard, giving Administrators enterprise-wide visibility into their network resources and overall security posture. 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.

