



StandGuard Anti-Virus—Technical Packet

BYTWARE, INC.

Monitoring & Securing a Connected World.™



StandGuard Anti-Virus® Technical Packet

Revision July 2008

StandGuard® and StandGuard Anti-Virus® are registered trademarks of Bytware, Inc.

© 2008 Bytware, Inc. All Rights Reserved.

Table of Contents

Introduction to StandGuard Anti-Virus	5
Solution Overview: The Threats and the Risk to IBM Power Systems	
Do I need to scan the IBM Power System?	7
Why is the IBM Power System the Perfect Host?	7
What are the threats?	8
What's at risk?	8
What puts the IBM Power System and your data at risk?	9
How to Protect Your IBM Power System: Key Features of StandGuard Anti-Virus	
You'll never know unless you scan	11
How the native McAfee scanning engine for IBM Protects You	12
Support for IBM i scanning features	13
On-Access Scanning	13
On-Demand Scanning	13
Scanning IBM i SMTP Mail	13
Object Integrity Scanning	14
Scanning guest operating systems	14
Scanning Lotus Domino	15
Automatic updates	15
Scheduling features	16
Network-enablement	16
Reporting and logging	16
Monitoring and alerts	17

How StandGuard Anti-Virus Detects Viruses and Protects Your IBM Power System

Only the best scanning engine for IBM Power Systems	19
Identifying the type of object	19
Decoding the object	19
Looking for viruses	19
Encryption	20
Polymorphism	20
Using heuristic analysis	20
Calculating the checksum	20
Cleaning	20

Satisfying Compliance Regulations, Corporate Executives, and Auditors

COBIT Objective DS5.17: Protection of Security Functions	21
COBIT Objective DS5.19: Malicious Software Prevention, Detection, and Correction	21
COBIT Objective DS9.5: Unauthorized Software	21

StandGuard Anti-Virus for Lotus Domino

Mail scanning	23
Database scanning	23
Quarantine	23
Real-time alerts	23
Automatic updating	24
Scheduling	24
Logging	24
Ease of management	24

Contacting Bytware	25
--------------------	----

StandGuard Anti-Virus is the award-winning, native scanning solution for IBM Power Systems (aka AS/400, iSeries, System i) running IBM i (aka OS/400 or i5/OS), AIX*, Linux*, and Domino*. In this document we will use the terms “IBM Power Systems” and “IBM i” to represent all past and present versions of the server and the operating system.

Developed with the unique features of IBM Power Systems in mind, StandGuard Anti-Virus offers all the power and protection of the industry-leading McAfee scanning engine found on other platforms while meeting the specific needs of IBM i. With StandGuard Anti-Virus you have the essential tools to ensure that your IBM Power System meets compliance and security requirements, protects your data from viruses, worms, and malware threats, and gives you peace of mind.



The Threats and the Risk to IBM Power Systems

First off, let's answer the most common questions we are asked about StandGuard Anti-Virus:

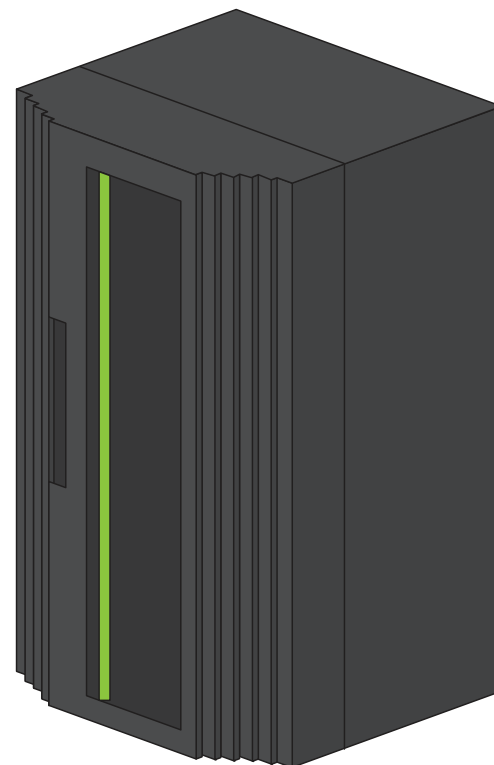
Do I need to scan the IBM Power System?

Yes. IBM Power Systems have always been able to host infected stream files (PC files) and share them with remote PCs and other servers. IBM marketing has been very clever to call IBM Power Systems “virus resistant.” They have never claimed it is “virus proof.” What they mean by “virus resistant” is that the traditional file system and programs—CLP, RPG, and COBOL programs—are resistant to viruses because they need to be compiled before they become executable. Once they are compiled, they cannot be easily changed.

IBM's evolution of the server has made it vulnerable to viruses. Today's IBM Power Systems run UNIX binary code, complies with POSIX and X/Open standards, has a traditional UNIX-like file system, and runs remote commands, shell scripts and Java. It includes a web server that can host infected HTML and PHP files. It's the perfect environment for today's viruses and malicious code.

Why is the IBM Power System the perfect host?

In most cases, IBM Power Systems can be ‘seen’ by every computer on the network. If an infected file is executed by any of these computers, that computer becomes infected and in turn can launch new attacks against the rest of the network—even back to the IBM Power System itself. These attacks can render computers and the network inoperable. A running virus has access to all of the same resources as the user whose machine launched the virus. Viruses can alter, copy, delete, and run commands against IBM i files, programs, and libraries. With respect to an IBM Power System, a virus starting there can spread to other systems and partitions through the use of network shares and the Integrated File System (IFS).



What are the threats?

Modern threats and malicious code (e.g. viruses, spyware, bombs, malware, network password sniffers, adware, suspicious programs, rootkits) present a major risk to your corporate data and security. There are more than 432,000 known threats floating around today, 100+ new threats occurring each week, and evidence that new threats are being designed to target corporate enterprises. Today's threats are no longer simply nuisances. Internet worms, Trojans, and backdoors are now a significant and growing threat, alongside EXE infectors and macro viruses. These blended threats are the viruses of the new millennium.

Recent trends in computer usage have increased the likelihood that your system has programs from untrusted sources or programs that perform unknown functions that can take up system resources and steal or destroy data.

What's at risk?

The Integrated File System (IFS) is an important area that, unfortunately, most IBM i businesses overlook. More and more operating system functions depend on information and code stored in the files in the root file system of the IFS. Unfortunately, there is still a misconception that the IFS is not used. Nothing could be farther from the truth. There is more operating system code and data in the IFS than in QSYS.LIB. Much of the system's critical data is stored in the IFS, including the TCP/IP configuration files, web server configuration files, terminal services configuration files, and much more.

WebSphere Application Server (WAS), IBM Portal Server, and the Apache Web server store extensive amounts of executables and data in the root file system; as does PHP. Exposures in these applications on any system—including IBM Power Systems—which is based on the ability to read or alter application programs or data, are often no less an exposure if the application is hosted on a system running IBM i.

PC data or applications stored in the IFS that are not scanned put your IBM i systems at risk! An infected file that resides in the IFS—but is never scanned and cleaned—will continue to reinfect, at a minimum, your PC clients and will remain on your IFS. Conceivably, the applications mentioned above could be attacked by using a Windows virus to read or alter the application programs and/or data associated with WAS, Portal Server, Apache, or PHP.

Without protection, the security and integrity of the IFS—as well as the stability and integrity of the entire system—are vulnerable.

What puts the IBM Power System and my data at risk?

Viruses and malicious code use a variety of tools (e.g. rootkits, Trojans, sniffers) and take advantage of many common technologies in an effort to compromise hosts to infect and steal data. These technologies include FTP, Telnet, and ODBC, all used every day in the typical IBM i environment. Through these technologies, viruses, and malicious code may be used as part of other types of assaults such as Denial of Service (DoS) attacks, Man-In-The-Middle (MIM) attacks, Flooding, Sniffing, Spoofing, ARP & DHCP attacks, and buffer overflows to name a few. A running virus can execute the DEL command and other dangerous system commands against a network drive mapped to the IBM Power System, causing serious damage. Some of these attacks have taken down the system TCP/IP stack, requiring an IPL to recover.

The domain name resolution function (BIND program) in IBM i is really an AIX executable that runs in the Portable Application System Environment (PASE). Many different types of systems use the exact same code because it is in the public domain. This particular program has had several security exposures, at least one of which allowed the attacker to execute arbitrary code as superuser in AIX and as QTCP in IBM i. This is just one example of how rogue, virus-like code inserted in the root file system can be used to attack other IFS files and even native IBM i resources.

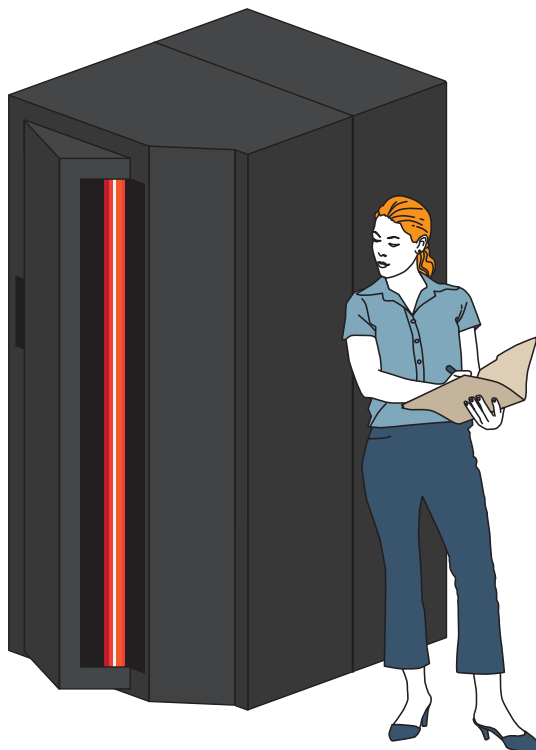
Regulatory legislation places serious challenges on your security efforts. Software solutions play a key role in building and implementing a plan to bring your organization into compliance. With specific directions about combating the threat of malicious code, COBIT guidelines can be used in an effort to comply with SOX and other regulatory legislation.

How to Protect Your IBM Power System

You'll never know unless you scan

There is no way for you to know if threats reside on your IBM Power System unless you are scanning the system with a native solution designed to detect and clean threats. And because threats are continually evolving—and systems have evolved into more than just file servers—scanning must be done on a regular basis with a reliable scanning solution. StandGuard Anti-Virus incorporates the latest generation of McAfee's scanning engine, in turn making StandGuard Anti-Virus a mature product backed by battle-tested technology, advanced heuristic analysis, and generic detection and cleaning. Unless you are scanning your IBM Power System with StandGuard Anti-Virus, you will never know if your system is threat-free. Take control of and eliminate potential threats with these power features:

- Detects and cleans macro and script viruses.
- Detects and cleans encrypted and polymorphic viruses.
- Detects unknown viruses using heuristic analysis.



- Detects and removes Trojans, worms, malware.
- Scans within compressed, packed, and OLE files.
- Supports the built-in scanning enablement in IBM i.



How the Native McAfee scanning engine for IBM i Protects You

By partnering with McAfee, the leading provider of commercially-backed scanning engines, Bytware brings the only native scanning solution to IBM i. The McAfee engine is superior in the industry for many reasons.

- **Detects and cleans macro and script viruses.**

A macro virus is a malicious macro. Macro viruses are written in a macro programming language and attached to a document that supports macros, such as a Word or an Excel file. When a document or template containing the macro virus is opened in the target application, the virus runs, does its damage, and copies itself into other documents. Continuing use of the program results in the spread of the virus.

- **Detects and cleans encrypted and polymorphic viruses.**

An encrypted virus's code begins with a decryption algorithm and continues with scrambled or encrypted code for the remainder of the virus. Each time it infects, it automatically encodes itself differently, so its code is never the same. Through this method, the virus tries to avoid detection by anti-virus software.

Polymorphic viruses create varied (though fully functional) copies of themselves as a way to avoid detection by anti-virus software. Some polymorphic viruses use different encryption schemes and require different decryption routines. Thus, the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands in an attempt to thwart anti-virus software. One of the most advanced polymorphic viruses uses a mutation engine and random-number generators to change the virus code and its decryption routine.

- **Detects new/unknown and generic viruses using advanced heuristic analysis.**

Heuristic analysis is behavior-based analysis of a computer program by anti-virus software to identify a potential virus.

- **Detects and removes “Trojan horses,” worms, and many other types of malicious software.**

A Trojan horse is a malicious program that pretends to be a benign application. It purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive. Trojans are often dropped onto systems by hackers as a prelude to an attack and can be very useful in remotely opening pathways into a system.

Worms are parasitic computer programs that replicate, but unlike viruses they do not infect other program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread through Internet Relay Chat (IRC).

- **Scans within compressed, packed, and OLE files.**

A ZIP file is an archive containing a collection of compressed files. ZIP files are popular on the Internet because users can deliver multiple files in a single container, and the compressed files save disk space and download time. A ZIP file can contain viruses if any of the files packaged in it contain viruses, but the ZIP file itself is not directly dangerous. Other archival file types include RAR, SIT, and LHA files.

- **Supports IBM i scanning features**

Starting with V5R3, IBM integrated virus scanning support into the operating system. StandGuard Anti-Virus fully supports these features. The result is better security and substantially lower overhead compared to other platforms and file systems.

- **On-Access Scanning**

StandGuard Anti-Virus provides real-time protection against virus threats by scanning files dynamically as they are opened. You can enable on-access scanning separately for file server accesses (NetServer mapped drives, FTP) and 5250 environments (host-based applications, like Java, Websphere, etc).

- **On-Demand Scanning**

StandGuard Anti-Virus provides on-demand scanning, which allows you to scan all or part of the system at scheduled times. You can configure which directories to scan and the schedules at which to run the scan. This allows you to run scans during off-peak times to reduce the CPU impact on other applications.

- **Scans IBM i SMTP Mail**

StandGuard Anti-Virus can scan inbound and outbound mail passing through the IBM i Mail Server Framework. If you are using the IBM Power System to send or receive e-mail, StandGuard Anti-Virus can perform virus scanning on e-mail before it reaches your PC clients, other servers in your network, or customers.

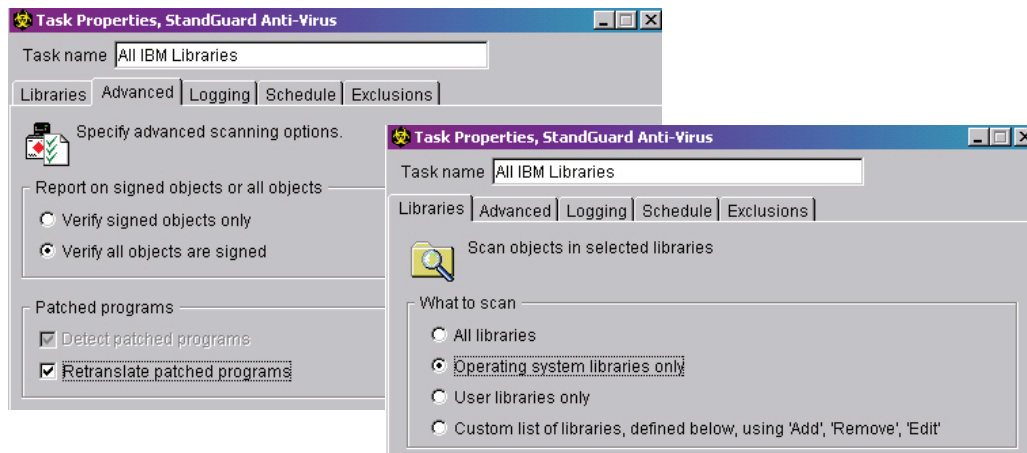


Object Integrity Scanning to detect changed objects, patched programs, etc.

Unique to IBM i and not found in any other product today, StandGuard Anti-Virus scans the operating system (and user libraries) for objects that have been tampered with and have the potential to cause serious harm to the operating system or bypass all security entirely.

The system security administrator needs to be concerned about programs that perform unauthorized functions. As new server functions become available to participate in the open environment, some of the object-based protection functions of servers no longer apply. For example, with the IFS, users can directly manipulate some objects in directories, such as stream files. As a file server, the server can store programs that many PC users share. Since hackers and other malicious users are able to quickly catch up with advances in technology, the only effective security policies are those that are constantly updated to help you detect attempts to introduce a virus-type program into your system.

It is for this reason that IBM and many other vendors digitally sign their objects, and why scanning is so critical on all servers. But unless you are scanning objects, you can't know for sure if they have been changed. StandGuard Anti-Virus will scan and detect changed objects, patched programs, etc.



StandGuard Anti-Virus makes it easy for you to protect IBM i from unwanted changes. By scanning IBM's digital signatures you can determine when objects have been modified.

- **Scans guest operating systems in partitions**

StandGuard Anti-Virus supports scanning and cleaning of Linux and AIX guest partitions using the Network File System (NFS). By creating scheduled scan tasks to scan NFS mountable volumes on guest partitions, you can reduce the time, effort, and cost associated with installing and configuring multiple stand-alone anti-virus applications on each partition. A single installation of StandGuard Anti-Virus on the host partition can be used to ensure that all of your Linux and AIX partitions are free of viruses, Trojans, worms, malware, and spyware (extra licenses may be required).

- **Scans Lotus Domino**

If you are running Domino servers on your IBM Power System, StandGuard Anti-Virus has an add-on feature to expand scanning to Domino. StandGuard Anti-Virus will scan Domino mail and databases for viruses and let you configure and manage remote Domino servers from a central administration server. See the section on Anti-Virus for Domino, beginning on page 22 for more information.

- **Automatic download of virus definitions (DAT files)**

StandGuard Anti-Virus ensures that you always have the latest protection against current virus threats by automatically downloading virus definitions from McAfee. By keeping virus definitions up-to-date automatically, StandGuard Anti-Virus protects you from the 100+ new virus threats that occur each week. You can use the supplied menu/commands to download the files interactively as well as integrate within your own nightly batch processes, or use the IBM Systems Director Navigator for i plug-in and let StandGuard Anti-Virus handle the updating for you automatically.

- **Automatic download of software updates and fixes**

StandGuard Anti-Virus keeps itself up-to-date by downloading new features, fixes, and enhancements from Bytware.

```

Change AVUPDATE Attributes (AVCHGUPDA)

Type choices, press Enter.

Transfer method . . . . . *FTP      *PATH, *FTP
FTP Location . . . . . *DFT
_____

FTP Password . . . . . _____
_____

Schedule . . . . . *DAILY      *DAILY, *WEEKLY, *MONTHLY...
Days . . . . . *ALL          *SAME, *ALL, *SUN, *MON...
+ for more values _____

Time . . . . . 053100        Time, *SAME
Output . . . . . *LOGFILE    *LOGFILE, *PRINT
Back up files before update . . *YES      *NO, *YES
Retrieve files only . . . . . *NO      *NO, *YES

More...

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

```

Keep your protection up-to-date easily with automatic updating of both the product and virus definitions. You can update either directly from McAfee and Bytware servers, or from local systems on your network to which you have downloaded updates and DATs.

- **Built-in scheduling features for scanning and updating**

StandGuard Anti-Virus integrates with the IBM i Job Scheduler—and other job schedulers—to schedule automatic updating of virus definitions, product enhancements, and scanning tasks that you create. By automating these tasks using the IBM i tools that you know and trust, you can rest assured that StandGuard Anti-Virus is providing reliable, around-the-clock protection.

- **Network-enabled**

StandGuard Anti-Virus can retrieve virus definitions and program updates from either an FTP server, or a shared local network path. The path can be located on another IBM Power System or partition, a Windows file server, or any supported network path of your choice. This allows you to use one server or partition to download the virus definitions (from McAfee's FTP server) and have the remaining servers or partitions retrieve their virus definition files from the shared network folder. The same networking features can be used to keep the StandGuard Anti-Virus product up-to-date for all your servers or partitions. Use one server or partition to download the updates and the remaining servers or partitions can retrieve their updates from the shared network folder.

- **Extensive reporting and logging**

StandGuard Anti-Virus provides several logging features that you can use to monitor and report:

- Scan reports provide detailed information about the directories scanned, infections found, and cleaning/quarantining activity.
- Virus scanning activity is recorded in the system audit journal, providing a secure audit trail of virus activity within the system.
- All changes made to StandGuard Anti-Virus's automation files are recorded in the AVJRN journal, recording all changes made to the product, who made them, and when they were made.
- Scan-related messages are logged to the message queue AVMSGQ. You can view the message queue manually as needed, or use third-party monitoring tools (such as Bytware's Messenger™) to automate the monitoring of this queue and alert you to viruses and failed downloads via e-mail, cell phone, or pager.

- **Green screen and IBM i Navigator plug-ins provided.**



Monitoring and alerts

Bytware strongly recommends that you monitor the StandGuard Anti-Virus messages logged to the AVMSGQ to ensure an ongoing problem is noticed and remedied as soon as possible.

StandGuard Anti-Virus can keep you and your staff up-to-date at all times regarding the status of your system. By combining the virus protection capabilities of StandGuard Anti-Virus with your automated monitoring and notification solution, you can know immediately when critical events have taken place and respond promptly to avoid disruption of operations, minimize damage, and meet the requirements of regulatory legislation.

For example, you can:

- Monitor the AVMSGQ message queue manually
- Automate the monitoring with one of the Bytware Messenger™ products
- Ensure timely notification by e-mail, pager, cell phone, smart phone or other device

As important as it is to install anti-virus protection on your server, it is equally important to know when problems occur. Important events that you need to monitor are:

- When StandGuard Anti-Virus detected and removed a virus
- If virus definition files could not be retrieved
- If the AVSVR job is ended or not running
- If a scan ended abnormally
- If a scan did not run at all

StandGuard Anti-Virus does more than just scan for viruses; it allows you to keep your IBM Power System healthy at all times, prevent the spread of viruses to other areas of your network or outside systems, and meet the requirements of regulatory legislation.



How StandGuard Anti-Virus Detects Viruses and Protects Your IBM Power System



Only the Best Scanning Engine for IBM Power Systems

Open source, non-commercially backed scanning engines like ClamAV are not viable solutions for business. The McAfee scanning engine and Bytware's StandGuard Anti-Virus are commercially-backed, fully supported solutions.

Wrapped by StandGuard Anti-Virus, McAfee's scanning engine is a complex data analyzer. The exact process of analysis depends on the object (often a file) being scanned and the type of viruses being sought.

- **Identifying the type of object**

This stage determines which type of object is being scanned. Files that contain executable code, for example, need to be scanned. Different types of files in the Microsoft Windows operating system, for example, are distinguished by their file extensions, such as .EXE and .TXT. However, any file can given a false extension to hide its true identity, so the contents of the file must first be determined. Each type of object requires its own special processing. If the type cannot be infected with a virus, no further scanning needs to be done. For example, a picture stored in bitmap format (a .BMP file) cannot be infected.

- **Decoding the object**

This stage decodes the contents of the object, so that the virus scanner “understands” what it is looking at. For example, a compressed WinZip file cannot be interpreted until it has been expanded back to its original contents. The same applies to non-compressed files, too. For example, the engine must decode a Microsoft Word document (.DOC) file in order to find a macro virus. File decoding can become quite complex when a file contains further encoded files. For example, a WinZip archive file might contain a mixture of other archives and document files. After the engine decodes the original WinZip file, the engine must also decode and separately scan the files inside.

- **Looking for the virus**

This complex stage of virus scanning is controlled by the virus definition (DAT) files. The scan.dat file contains thousands of different drivers. Each driver has detailed instructions on how to find a particular virus or type of virus. The engine can find a simple virus by starting from a known place in the file, then searching for its virus signature. Often, the engine needs to search only a small part of a file to determine that the file is free from viruses. A virus signature is a sequence of characters that uniquely identify the virus, such as a message that the virus may display on the screen, or a fragment of computer code. We take care when choosing these signatures to avoid falsely detecting viruses inside clean files. More complex viruses avoid detection with simple signature scanning by using two popular techniques:

- **Encryption**

The data inside the virus is encrypted so that anti-virus scanners cannot see the messages or computer code of the virus. When the virus is activated, it converts itself into a working version and then executes.

- **Polymorphism**

This process is similar to encryption, except that when the virus replicates itself it changes its appearance.

To counteract such viruses, the engine uses a technique called *emulation*. If the engine suspects that a file contains such a virus, the engine creates an artificial environment in which the virus can run harmlessly until it has decoded itself and its true form becomes visible. The engine can then identify the virus as usual by scanning for a virus signature.

- **Using heuristic analysis**

Using only virus signatures, the engine cannot detect a new, previously unknown virus because its signature is not yet known. Therefore, the engine can use an additional technique called *heuristic analysis*. Programs, documents, or e-mail messages that carry a virus often have distinctive features. They might attempt unprompted modification of files, invoke mail clients, or use other means to replicate themselves. The engine analyzes the program code to detect these kinds of computer instructions. The engine also searches for “legitimate” non-virus-like behavior, such as prompting the user before taking action, and thereby avoids raising false alarms.

By using these techniques, the engine can detect many new viruses.

- **Calculating the checksum**

This stage exactly identifies the virus. The engine performs a mathematical calculation over the virus data to produce a unique number—the *checksum*. The engine compares this checksum against previously calculated values in one of the DAT files (scan.dat) to identify the exact virus.

- **Cleaning**

This stage cleans the object. Usually, the engine can clean an infected file satisfactorily. However, some viruses can alter or destroy data to such an extent that the file cannot be fixed. The engine can easily clean macro viruses by erasing the macro from the infected document; but executable viruses are more complex. The engine must restore the original path of execution through the program so that the virus does not become active. For example, a virus might append itself to the end of an executable program file. To run, the virus must divert the path of execution away from the original code to itself. After becoming active, the virus redirects the path of execution to the original code

to avoid suspicion. The engine can disable this virus by removing the diversion to the virus code. To clean the file, the engine then erases the virus code.

Satisfying Compliance Regulations, Corporate Executives and Auditors

A plethora of security regulations have been passed over the years, including the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, the Gramm-Leach-Bliley Act (GLBA), FISMA, and PCI DSS, with still more in legislation draft that stipulates the protection of data. All of these place the responsibility and accountability on the shoulders of the IT professional. Some useful guidelines include:

- **COBIT Objective DS5.17: Protection of Security Functions**

Most compelling is the COBIT objectives regarding Protection of Security Functions. This objective directs that all security-related hardware and software should be protected against tampering to maintain their integrity and to guard against the disclosure of secret keys. StandGuard Anti-Virus can detect, prevent, and remove viruses and malicious code, allowing you meet this directive natively on IBM Power Systems.

- **COBIT Objective DS5.19: Malicious Software Prevention, Detection, and Correction**

This objective states that, regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective, and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response, and reporting. StandGuard Anti-Virus can detect, prevent, and remove viruses and malicious code.

- **COBIT Objective DS9.5: Unauthorized Software**

The COBIT objective regarding Unauthorized Software specifies that clear policies restricting the use of personal and unlicensed software should be developed and enforced. The organization should use virus detection and remedy software. Business and IT management should periodically check the organization's personal computers for unauthorized software. Compliance with the requirements of software and hardware license agreements should be reviewed on a periodic basis. StandGuard Anti-Virus can detect, prevent, and remove viruses and malicious code.



StandGuard Anti-Virus for Lotus Domino

Bringing the Power of McAfee and StandGuard Anti-Virus to Domino on IBM Power Systems

The StandGuard Anti-Virus Domino add-on feature expands your scanning protection to Lotus Domino mail and databases residing on IBM Power Systems. Providing all the features of StandGuard Anti-Virus, the Domino add-on gives you the following extras:

- **Mail scanning**

The application dynamically scans e-mail messages for viruses and other types of malicious code, protecting Domino mail users from receiving infected and potentially harmful messages.

- **Database scanning**


The application provides on-demand scanning of Domino databases, detecting viruses and malicious code embedded within document attachments and OLE objects.

- **Quarantine**

StandGuard Anti-Virus provides a secure area to where infected files are moved out of harm's way. When a file is quarantined, the file is not been deleted but access to the file is prevented. An administrator can then further investigate the origin of the virus and the integrity of the file by submitting a sample to McAfee's AVERT Labs threat center.

- **Real-time alerts**

Alerts can be configured to notify you when various events occur, such as when infected messages and documents are detected or when automatic activities occur. With these alerts administrators will be continually aware of the health and status of the system.



STANDGUARD ANTI-VIRUS FOR DOMINO FROM BYTWARE, INC. POWERED BY MCAFEE

On-Demand Scanning - Task Configuration

Server: test/support
 Task Name: ALL
 Description: All Databases
 Last Result: 0 virus(es) found.
 Last Run: 07/22/2008 09:56 AM

What to Scan

Starting directory or database name: *

Scan subdirectories below directory: ☒ Yes ☐ No

Databases to omit from scan: (separate multiple values by commas)

Skip files larger than: 0 kilobytes (0=Scan all files regardless of size)

Options

Scan options:

- ☒ Scan compressed files
- ☒ Enable file heuristics
- ☒ Find suspicious programs
- ☒ Scan archive files
- ☐ Incremental scan
- ☒ Macro analysis

File types to scan:

- ☒ Scan all files
- ☐ Scan commonly infected files only

Run priority: 50

Timeout: ☐ Yes ☒ No

Actions

When an infection is found:

- ☐ Log and continue
- ☐ Clean attachment
- ☒ Quarantine attachment
- ☐ Delete attachment

Schedule

Scheduled? ☐ Yes ☒ No

Logging

Options:

- ☒ All files

- **Automatic updating**

McAfee updates virus definitions daily and StandGuard Anti-Virus can automatically update itself by downloading DAT files directly from McAfee's Internet servers or by using DAT files that you have downloaded to a specified computers on the local network.

- **Scheduling**

The administrator can schedule automatic database scanning and automatic updating to occur at user-configurable time periods when system activity is low, such as nights and weekends.

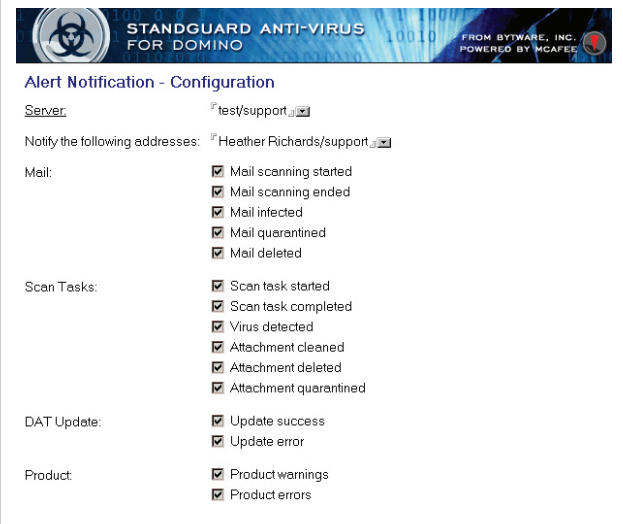
- **Logging**

All product activities are logged to a central database. The Log database provides information such as when scans start, finish, and any infections that were found. You can specify the number of days the Log database will retain information.

- **Ease of management**

Remote Domino servers can be configured and managed from a central administration server, reducing the time and effort normally required to manage remote servers. The log database is presented as a consolidated view of all events occurring across multiple servers. In addition to the traditional Notes user interface, the product also provides a web browser interface for viewing and managing all activities across multiple remote servers.

The Domino add-on requires StandGuard Anti-Virus for IBM i, Bytware's native IBM i anti-virus solution designed to scan IFS directories and perform advanced cleaning and notification functions.



Alert Notification - Configuration

Server: test/support

Notify the following addresses: Heather.Richards/support

Mail:

- ☒ Mail scanning started
- ☒ Mail scanning ended
- ☒ Mail infected
- ☒ Mail quarantined
- ☒ Mail deleted

Scan Tasks:

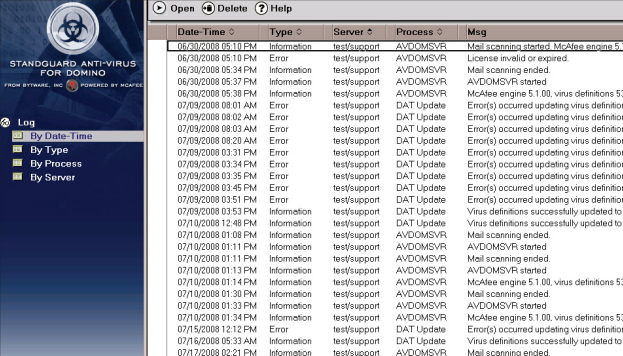
- ☒ Scan task started
- ☒ Scan task completed
- ☒ Virus detected
- ☒ Attachment cleaned
- ☒ Attachment deleted
- ☒ Attachment quarantined

DAT Update:

- ☒ Update success
- ☒ Update error

Product:

- ☒ Product warnings
- ☒ Product errors



Date-Time	Type	Server	Process	Msg
06/30/2008 05:10 PM	Information	test/support	AVDOMSVR	Mail scanning started. McAfee engine 5.1.00
06/30/2008 05:10 PM	Error	test/support	AVDOMSVR	License invalid or expired.
06/30/2008 05:34 PM	Information	test/support	AVDOMSVR	Mail scanning ended.
06/30/2008 05:37 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
06/30/2008 05:38 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
07/09/2008 08:01 AM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:02 AM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:03 AM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:28 AM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:31 PM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:34 PM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:35 PM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 08:45 PM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 03:51 PM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/09/2008 03:53 PM	Information	test/support	DAT Update	Virus definitions successfully updated to version 5.1.00
07/10/2008 12:48 PM	Information	test/support	DAT Update	Virus definitions successfully updated to version 5.1.00
07/10/2008 01:08 PM	Information	test/support	AVDOMSVR	Mail scanning ended.
07/10/2008 01:11 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
07/10/2008 01:11 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
07/10/2008 01:13 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
07/10/2008 01:14 PM	Information	test/support	AVDOMSVR	McAfee engine 5.1.00, virus definitions 53304
07/10/2008 01:30 PM	Information	test/support	AVDOMSVR	Mail scanning ended.
07/10/2008 01:33 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
07/10/2008 01:34 PM	Information	test/support	AVDOMSVR	AVDOMSVR started
07/15/2008 12:12 PM	Error	test/support	DAT Update	Error(s) occurred updating virus definitions: 53204
07/16/2008 05:33 AM	Information	test/support	DAT Update	Virus definitions successfully updated to version 5.1.00
07/16/2008 06:21 PM	Information	test/support	AVDOMSVR	Mail scanning ended.
07/17/2008 02:24 PM	Information	test/support	AVDOMSVR	AVDOMSVR started



For more information about StandGuard Anti-Virus or to arrange a technical walkthrough, please contact us at 800.932.5557. Additional information about and a free trial of StandGuard Anti-Virus is also available on our website by visiting www.bytware.com/products/av/

Bytware, Inc. 9440 Double R. Blvd, Suite b, Reno, Nevada 89521 USA

StandGuard® and StandGuard Anti-Virus® are registered trademarks of Bytware, Inc. © 2008 Bytware, Inc. All Rights Reserved. [AVTP080729]