



# Whitepaper

## **iQ.Suite Watchdog**

- Central virus protection -

Intelligent server-based virus protection and file blocking  
through fingerprint technology

*Expertise matters*

## Contents

1	Executive Summary .....	2
2	Introduction.....	2
3	Computer Viruses.....	3
3.1	Types of Viruses .....	3
3.1.1	File Viruses .....	3
3.1.2	Macro Viruses.....	3
3.1.3	Trojans.....	3
3.1.4	Script Viruses.....	4
3.1.5	Worms.....	4
3.2	Cost Generated by Email Attacks.....	4
3.3	How Do Viruses Find Their Way Into the Company? .....	4
4	Virus Protection = Virus Protection? .....	5
4.1	Desktop Virus Protection.....	5
4.1.1	Insufficient Protection .....	5
4.1.2	Software Maintenance Requirements .....	5
4.1.3	Burden on the Infrastructure .....	5
4.2	Company-Wide, Server-Based Virus Protection.....	5
4.2.1	Central Administration .....	6
4.2.2	First Protect, Then Save .....	6
4.2.3	Cost-Effective Protection .....	6
4.2.4	Protecting Databases and Public Folders .....	7
4.2.5	Highest Reliability through Simultaneous Use of Multiple Virus Scanners .....	7
4.2.6	Investment Protection .....	7
4.2.7	Flexibility .....	7
4.2.8	Intelligent File Attachment Checking .....	8
4.2.9	Server-Based Content Checking of Encrypted Emails.....	8
5	Application Scenarios.....	9
5.1	Reliable Virus Protection.....	9
5.1.1	Requirements .....	9
5.1.2	Solution Approaches.....	10
5.2	Blocking Undesired File Types .....	10
5.2.1	Requirements .....	11
5.2.2	Solution Approaches.....	11
6	iQ.Suite Watchdog in a Nutshell.....	13

## 1 Executive Summary

The worldwide virus attacks launched in recent years in ever new variants have resulted in an increased awareness of the threats to existing computer systems posed by viruses, email worms and Trojans. Mail servers, networks and clients infected by viruses not only cause considerable cost but can also negatively affect a company's image and reputation.

This whitepaper shows what companies can do to protect themselves efficiently and comprehensively against the threats associated with known and newly launched viruses.

## 2 Introduction

Email and messaging have become the most important communication means in today's economic world. Many business processes are partially or entirely handled via electronic mail and the email boom is not likely to slow down in the years to come.

Let us first make a distinction between four areas related with business processes handled via email:

### Initial actions:

- Making initial contact with customers
- Direct email marketing
- Making contact with suppliers

### Negotiations:

- Exchanging requirements, product information, prices, etc.

### Customer relation management:

- Up-to-date information on products, services, etc.
- Support services

### Internal business processes:

- Workflow, e.g. holiday requests, purchasing, new staff, etc.

One thing is true for all of these areas: The availability of the communication infrastructure is a vital issue. Many company departments depend on email to such an extent that a failure of the mail system would result in a complete suspension of work as well as immense additional cost.

Computer viruses are one of the main reasons for the failure of an email system.

## 3 Computer Viruses

A computer virus is a malicious program (malware) that is able to reproduce itself and thus to infect other programs. As for “real” viruses, the computer also goes through an incubation period. Typically, the virus becomes active after a specific event or date and then executes the programmed instructions, which often cause great damage.

### 3.1 Types of Viruses

#### 3.1.1 File Viruses

File viruses usually come with COM and .EXE files. Infection takes place when the executable file is loaded, i.e. when the program is run. As their name indicates, boot sector viruses infect the floppy or hard disk boot sector (that is where the program is located that loads the operating system). As they are transmitted through infected floppy disks, they may take several weeks or months to spread. Up to the 1990s, file viruses were the predominant type of computer virus.

#### 3.1.2 Macro Viruses

Macro viruses exist since the early 1990s. One of the reasons for their great “popularity” in the years leading up to the millennium is that they are relatively easy to program. Virtually all the popular office packages come with an integrated programming language (mainly Visual BASIC for Applications – VBA), which can be used to program macros viruses and integrate them for instance in Word or Excel documents. Once distributed via email, these viruses can spread around the world within minutes. However, the number of macro viruses has strongly declined throughout the world in the last few years.

#### 3.1.3 Trojans

A Trojan (“Trojan horse”) is a program that, at first sight, appears to be harmless, but executes malicious code in the background. A typical example of a Trojan is a program that displays a faked login prompt to capture the user’s login name and password. After having sent the login data to another computer via email, the Trojan returns A “Login incorrect” message and passes control to the standard login procedure. The user may not even be aware that something wrong has happened. Trojans are unable to reproduce themselves and therefore do not spread as fast as viruses. However, Trojans can be very dangerous when combined with viruses, as is frequently the case today, because viruses are able to load Trojans, which will store keyboard sequences or steal data. Trojans are also used to infect a computer with a virus. A so-called backdoor Trojan allows the remote attacker to connect to the infected computer and misuse it for his own purposes.

### **3.1.4 Script Viruses**

Script viruses, based on Visual Basic Script (VBS), spread extremely fast. Having emerged and spread “in the wild” in recent years, this type of virus has rapidly climbed to the tops spots in virus ranking. Probably the best known example of this kind of virus is the VBS/Loveletter Virus (also called VBS/Love or VBS/ILoveYou). These viruses are very easy to program and spread, for instance by inserting them in an email body text. Some email clients run the malicious scripts as soon as the email is opened by a preview feature or simply read.

### **3.1.5 Worms**

A worm is malicious program that automatically spreads between computers in a network. The “purpose” of a worm is to infect a maximum number of computers within the network.

Once they are on the way, worms reproduce themselves and spread within and across networks or the Internet in a very short time. Internet worms exploit security gaps in the operating system or browser and “jump” back and forth between networked computers. To reproduce (they make copies of themselves), worms can generate a high amount of Internet traffic, up to a level where communication is significantly slowed down or computers crash. Typically, they use the computers’ email functionality to send themselves to whichever Internet addresses they may find. In addition to their fast-spreading capability, worms also carry malicious code that, like a traditional virus, is activated on the infected computer. Currently, worms account for nearly 100% of all computer viruses in circulation.

## **3.2 Cost Generated by Email Attacks**

Costs related to malware are enormous. There is hardly a company that has not been the victim of a virus attack at least once. Direct damages, for instance caused by the destruction of data, are much easier to estimate than losses resulting from impediments to the company communication.

Beside the loss of data and the non-availability of computers, the most severe damages mainly result from productivity losses and corrupted files.

## **3.3 How Do Viruses Find Their Way Into the Company?**

Of today’s worm viruses, nearly 100% spread via email attachments. It is hardly possible to rely on employees not to open suspicious attachments, as many viruses are spread with a faked sender address.

## **4 Virus Protection = Virus Protection?**

One result of the alarming increase of virus attacks is that virtually all companies use some sort of anti-virus software. Let us compare desktop virus protection with server-based anti-virus software.

### **4.1 Desktop Virus Protection**

#### **4.1.1 Insufficient Protection**

A great number of companies still use anti-virus products on their employees' desktop computers. The protection provided by these products against viruses spread via floppy disks is quite high, but, as mentioned above, nearly 100% of today's computer viruses are distributed via email – and here the user's PC is the last link in the transmission chain. As these viruses, in particular script viruses, usually use the e mail client's features to cause their damage, it is also the most vulnerable link. Client-based virus scanners offer only little, if any, protection against these viruses.

#### **4.1.2 Software Maintenance Requirements**

To provide full protection against attacks from the latest viruses, anti-virus software needs to be continually updated. With new viruses appearing almost daily, the update intervals for antivirus programs and in particular virus patterns are getting ever shorter. For desktop-based scan engines this means that every software update has to be distributed across all of the company's PCs.

Even with login-controlled mechanisms, central administration and maintenance of these programs is all but easy, time consuming and costly.

#### **4.1.3 Burden on the Infrastructure**

The distribution of software across a network can be quite problematic, especially when a company is being attacked by newly discovered viruses.

Even if updated virus pattern files are available, large-scale attacks can place such a heavy burden on network infrastructures that the distribution of these files to all desktop PCs becomes almost impossible.

### **4.2 Company-Wide, Server-Based Virus Protection**

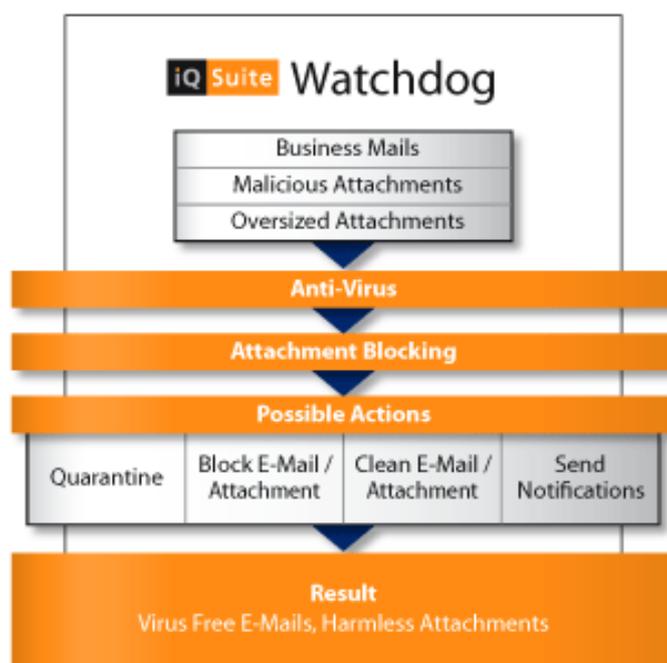
The server-based virus protection solution provided by GROUP's iQ.Suite Watchdog offers many benefits to companies.

### 4.2.1 Central Administration

iQ.Suite Watchdog can be installed and run on the existing email servers, i.e. buying a dedicated server is not necessary. Watchdog can be centrally managed through a standardized user interface. Because it is server-based, neither anti-virus software nor the latest virus pattern files have to be distributed to all of the company's workstations, which considerably reduces the cost for administration and maintenance. Also, response times are much shorter in case of attacks by new viruses.

### 4.2.2 First Protect, Then Save

iQ.Suite Watchdog scans and, where required, cleans the emails before they are saved on the mail servers. Thus, an infection of an email server can be virtually excluded. It also means that emails are definitely virus-free when delivered to their recipients.



### 4.2.3 Cost-Effective Protection

By removing the need for maintaining client-based software, iQ.Suite Watchdog helps to reduce the cost for the implementation and management of a company-wide virus protection solution.

#### 4.2.4 Protecting Databases and Public Folders

Not only inbound and outbound emails can contain viruses; other electronic documents could be infected as well and can also be saved on IBM Notes/Domino and MS Exchange servers.

iQ.Suite Watchdog not only protects the email traffic but also access to IBM Notes/Domino databases and public folders under Microsoft Exchange, thereby significantly contributing to the protection of the email and messaging infrastructure.

#### 4.2.5 Highest Reliability through Simultaneous Use of Multiple Virus Scanners

Past virus attacks have shown that recognition rates and response times may vary between virus scanners. iQ.Suite Watchdog comes with a fully integrated virus scanner, e.g. Avira and Sophos. In addition, Watchdog supports a wide variety of virus scanners from other manufacturers (please ask your sales partner).

iQ.Suite Watchdog also offers the possibility to use all virus scanners supported simultaneously, thus making a significant contribution to the overall reliability of the virus-protection solution.

#### 4.2.6 Investment Protection

Thanks to partnerships with leading manufacturers of virus scanners, iQ.Suite Watchdog enables the user to integrate any scan engine existing in the company as well as to use the advanced options provided by Watchdog. If a company plans to use further or other virus scanners in the future, these scanners can easily be integrated in Watchdog.

#### 4.2.7 Flexibility

Shifting virus scanning from the clients to the server opens up the possibility of using rule-based protection mechanisms. “Rule-based” primarily refers to a set of “if-then” conditions, where the “if” may contain multiple conditions and the “then” multiple actions to be executed.

<i>If...</i>	<i>then...</i>
an email is sent to abc@xyz.com,	check for viruses using engines 1 and 2.
an email is received by *@test.com,	check for viruses using engines 3 and 4.

## 4.2.8 Intelligent File Attachment Checking

iQ.Suite Watchdog not only recognizes viruses, worms, etc., but also allows defining and applying specific file attachment restrictions based on various criteria.

### 4.2.8.1 Restrictions Based on File Extension

One example of restrictions based on the file extension relates to script viruses (refer to Section 3.1.4). Script viruses are typically Visual Basic Script (vbs) files. With iQ.Suite Watchdog, file attachments with a file extension such as "vbs" can be reliably identified and blocked.

### 4.2.8.2 Restrictions Based on Fingerprints

Many file types have a unique binary pattern, called fingerprint, by which they can be identified. This fingerprint can be used to determine the original file type of a file that has been renamed, for instance from "execute.exe" to "execute.txt".

Watchdog is able to recognize and block many file types by their fingerprints. This feature highly improves the security aspects related to the identification of files, as it reliably protects against manipulated files.

### 4.2.8.3 Restrictions Based on the Size and Number of Attachments

Email attachments can become a serious threat to the infrastructure, when they create network bandwidth and capacity problems because of their number and their size.

With iQ.Suite Watchdog, emails can be blocked according to the following criteria:

- Number of attachments per email
- Maximum size of an attachment per email
- Maximum size of all attachments per email

## 4.2.9 Server-Based Content Checking of Encrypted Emails

Virus protection alone is not enough to ensure comprehensive, server-based security of the entire mail traffic. In many companies, email encryption, for example, plays an important role. The following should be noted in this context:

### Client-based encryption prevents comprehensive email content security

The reason is that an encrypted mail cannot be protected by antivirus programs and other email security tools on the mail servers, as encrypted messages cannot be read by these programs and the protective mechanisms implemented on the servers, therefore, do not work. This is a precarious

situation. With most companies having decided to set up email security applications on their servers in order to simplify administration, client-based encryption contradicts the need for standardized, centrally implemented and managed email infrastructures and security mechanisms.

Used in combination with iQ.Suite Crypt, iQ.Suite Watchdog also enables scanning of encrypted mails – both incoming and outgoing – for viruses and forbidden file types.

## 5 Application Scenarios

### 5.1 Reliable Virus Protection

After the successful implementation of an email infrastructure in a company, exchanges with customers and suppliers will normally increasingly shift to the electronic medium. Experience has shown that desktop virus scanners are normally unable to ensure a sufficiently high level of security: time and again, viruses manage to get onto PCs and execute their malicious code.

In the following section, we will look at suitable anti-virus solutions to provide comprehensive protection of the company's email communications.

#### 5.1.1 Requirements

1. As the maintenance of a client-based anti-virus solution has proven problematic, a server-based solution is sought. This is to reduce the cost of distributing and maintaining the anti-virus software.
2. The company seeks an anti-virus solution, where it is not tied to the products of a particular software manufacturer. The chosen product must therefore support multiple virus scanners.
3. Experience has shown that a single virus scanner will not recognize all known viruses. To increase security and reliability, several virus scanners are therefore to be used in parallel. However, only mail received from the Internet is to be scanned by more than one virus scanner; for internal mail traffic, only one virus scanner is used.
4. To protect both inbound and outbound as well as the internal mail traffic, a solution is required that will run on all email servers.
5. Beside inbound and outbound emails, the shared databases on the mail servers are also to be checked for viruses in order to provide comprehensive protection. In addition to real-time virus protection, all databases are to be scanned once every 24 hours at 1 AM.
6. In parallel with the introduction of email virus protection, the implementation of a server-based encryption and content checking solution is planned. The anti-virus solution must therefore be integrated into the overall email security concept, so that a server-based protection of encrypted emails is also possible.

### 5.1.2 Solution Approaches

1. First, the virus scanners to be used are specified.
2. The selected scan engines are then installed together with iQ.Suite Watchdog on all of the company's email servers.
3. Using the iQ.Suite server-based rule set, the rules required for scanning inbound, outbound and internal mails are defined.

<i>When...</i>	<i>then...</i>
an email is received from the Internet,	check mail with scan engines A and B
an email is sent to the Internet,	check mail with scan engine A
an email is received from the Intranet,	check mail with scan engine B
etc.	etc.

4. Protection of the selected mail server databases is also implemented through server-based rules.

<i>When...</i>	<i>then...</i>
an object is to be written to the database,	check object with scan engines A and B
the time is 01:00 AM,	check all databases with scan engine A

5. The defined rules are automatically distributed to all selected mail servers.
6. To enable server-based encryption, the encryption module – iQ.Suite Crypt – is implemented.

## 5.2 Blocking Undesired File Types

With the introduction of an email infrastructure and the transition of communications from letter and fax to the electronic medium, the mail volume is growing daily. An analysis has shown that especially the number transmitted audio files (e.g. MP3 or WMA) but also of video files, has increased rapidly. These – often large – files place a burden not only on the network bandwidth, but also the mail server resources. It can furthermore be assumed that these files do not, generally, contain information relevant to business activities, and rather tend to distract employees from their work. To preserve infrastructure resources, sending and receiving large files is to be restricted to specific departments within the company.

The company management has therefore decided to implement a solution to these problems.

### 5.2.1 Requirements

1. A facility is required for blocking the file types considered undesirable by the management.
2. A possibility of handling undesirable file types in different ways is required, i.e. moving some of the files to the quarantine on the server, while deleting others immediately.
3. Certain departments should continue to be allowed to send and receive image files.
4. A possibility of blocking messages exceeding a particular size is required, with different size limits for inbound, outbound and internal mails.
5. To prevent the spread of script viruses, Visual Basic Script and JavaScript files should be blocked.
6. The company seeks to maximize its security, and the chosen product must therefore be able to recognize a file type even if its extension has been changed. It must, for example, recognize "abc.VBS" as a Visual Basic Script file even if it has been renamed to "abc.TXT".
7. The solution must allow a quick, simple implementation of changes to the security guidelines through a central set of rules.

### 5.2.2 Solution Approaches

1. Definition of undesired file types:  
.AVI, .MPG,.MP3, .WMA, .WAV, .GIF, .JPG, .BMP and .TIF are to be systematically blocked.
2. Definition of required actions:  
.TIF, .AVI, .MPG, .MP3, .WMA and .WAV to be deleted immediately.  
.GIF, .JPG, and .BMP to be placed in quarantine.
3. Marketing can continue to send and receive .GIF, .JPG, .BMP and .TIF files.
4. Maximum size of inbound attachments: 4 MB
5. Maximum size of outgoing attachments: 2 MB
6. Maximum size in internal mail traffic: 10 MB
7. .VBS and .JS files to be blocked.
8. Installation of iQ.Suite Watchdog on all email servers.
9. Definition of the rule set.

**Rule set:**

<i>When...,</i>	<i>then...</i>
an email includes attachments of type GIF, JPG or .BMP	remove these attachments from mail and place corresponding files into Quarantine on email server. Notify sender/recipient and Administrator
an email includes attachments of type .TIF, .AVI, .MPG, .MP3, .WMA or .WAV	remove these attachments from mail and notify sender/recipient and Administrator
an email includes attachments of type GIF, .JPG, .BMP or .TIF and was sent from or to Marketing	notify data protection officer
inbound attachment from Internet > 4 MB	place attachment into Quarantine
outbound attachment to Internet > 2 MB	place attachment into Quarantine, notify sender
inbound attachment from Intranet > 10 MB	place attachment into Quarantine
outbound attachment to Intranet > 10 MB	place attachment into Quarantine, notify sender
attachment of type .JS or .VBS	place attachment into Quarantine, notify Administrator

## 6 iQ.Suite Watchdog in a Nutshell

### Highlights

- Integrated virus scanner.
- Efficient email and database scanning. All incoming, outgoing and internal messages and all databases are scanned for viruses and processed in real-time.
- Intelligent attachment checks. Checking and blocking files by type, size and structure prevents sending and receiving of messages with manipulated, undesirable or malicious file attachments.
- Flexible rule set. With its unique intelligent control mechanism for scanning emails and application databases, iQ.Suite Watchdog provides highest levels of flexibility and security. Up-to-date rule definitions are included in the package.
- Maximum virus protection. The simultaneous use of virus scanners and compression tools from various manufacturers ensures maximum protection, even from the latest or recursively packed viruses.
- Integrated, central administration. Full integration in the server platform guarantees simple administration.

### Features

- Reliable file pattern checking and blocking; also recognizes and blocks manipulated files
- Configurable rules for all scanning and protection functions
- Recursive virus scanning of all emails and file attachments in real-time, event-controlled and time-controlled
- Full support of Mail.box (IBM Domino) as well as storage groups and multiple databases (Microsoft Exchange)
- Recursive scanning of databases in real-time, event-controlled and time-controlled
- Comprehensive checking for manipulated Notes design elements / Outlook elements in emails and databases
- Automatic recognition of new mail folders and application databases or public folders
- Simultaneous use of virus scanners and compression tools from different manufacturers
- Supports automatic updates for virus signatures, control sets and file patterns
- Detailed log functions and statistics
- Configurable messages to sender, recipient and Administrator
- Optimized multi-processing and multi-threading, also for partitioned servers and clusters (IBM Domino)
- Scalable architecture
- Seamless integration with additional iQ.Suite products

## **About GBS**

GROUP Business Software is a leading vendor of solutions and services in the fields of messaging security and workflow for the IBM and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

Further information at [www.gbs.com](http://www.gbs.com)

**© 2016 GROUP Business Software Europa GmbH, All rights reserved.**

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments. The information contained in this document presents the topics from the viewpoint of GBS at the time of publishing. Since GBS needs to be able to react to changing market requirements, this is not an obligation for GBS and GBS cannot guarantee that the information presented in it is accurate after the publication date. This document is intended for information purposes only. GBS does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose. All the product and company names that appear in this document may be trademarks of their respective owners.