



McAfee System Protection Solutions

# McAfee Outbreak Manager for McAfee GroupShield and WebShield SMTP

Proactively Prevent Virus, Mass-Mailer,  
and E-Mail Denial of Service Outbreaks

## Table of Contents

---

|  |          |
|--|----------|
| <b>Executive Summary</b>                               | <b>3</b> |
| <hr/>  |          |
| <b>Overview</b>  | <b>3</b> |
| <hr/>  |          |
| <b>The Outbreak Detection Challenge</b>                | <b>3</b> |
| <hr/>  |          |
| <b>Introducing Outbreak Manager</b>                    | <b>3</b> |
| Resident Scanners                                      | 4        |
| <hr/>  |          |
| <b>Understanding Rules</b>                             | <b>4</b> |
| Rule Status and Logging                                | 5        |
| <hr/>  |          |
| <b>Trigger Types and Thresholds</b>                    | <b>5</b> |
| Trigger Examples                                       | 5        |
| <hr/>  |          |
| <b>Real World Example of Outbreak Manager Rules</b>    | <b>5</b> |
| Example of a Rule Not Taking Action                    | 5        |
| Example of a Rule Taking Action                        | 6        |
| <hr/>  |          |
| <b>Understanding Your Mail Protection Requirements</b> | <b>6</b> |
| Profiling Your Company's E-Mail Habits                 | 6        |
| File Attachment Risk Assessment                        | 6        |
| <hr/>  |          |
| <b>Methods of Profiling E-Mail Activity</b>            | <b>8</b> |
| <hr/>  |          |

## Executive Summary

This white paper provides information on the configuration and custom tuning of McAfee® Outbreak Manager for customer environments. It is intended for use by administrators using McAfee GroupShield® for Microsoft® Windows® environments and WebShield® SMTP, both of which include the McAfee Outbreak Manager utility.

## Overview

Companies face increasing numbers of virus incidents every year. Not only are these attacks increasing, but the severity of the incidents and their associated recovery costs are also on the rise. According to Computer Economics, in 2001, the Nimda virus cost companies \$635 million in cleanup costs and lost productivity. E-mail, Internet downloads, and Web browsing are major sources of this unprecedented growth in viral activity and increased severity of attacks. According to the 2002 ICSA Computer Virus Prevalence Survey, e-mail, Internet downloads, and Web browsing were the source of over 90 percent of all virus and worm infections.

Viruses and worms that spread via e-mail can infect your entire network in minutes, disrupting communications with your customers and partners, and interrupting intra-corporate collaboration. These viruses exploit the automated scripting capabilities of flexible, feature-rich e-mail applications to generate floods of server-hogging, inbox-clogging e-mail messages. However, the earlier a virus outbreak is detected, the easier the cleanup and the less severe the resulting damage.

## The Outbreak Detection Challenge

Historically, signature-based scanning has been the most reliable method of detecting and removing known viruses. However, with more than 200 new viruses appearing every month, keeping virus signature files up to date is a difficult task for anti-virus administrators and virus solution vendors alike. Even the strongest signature-based scanning is only as reliable as your last update, and your entire network can be compromised by just one unprotected or out-of-date desktop. These new e-mail viruses can spread incredibly fast, so by the time the outbreak is obvious, your entire network could be infected—costing you hundreds of thousands of dollars in damages, lost productivity, and missed opportunities.

Many experts contend that behavioral analysis is the future of virus detection. Behavioral analysis techniques watch for activity that seems viral in nature. For example, actions

committed automatically by scripting technology can be an indicator of viral activity. The problem with using this technique alone is that it can detect only viruses in action and won't reliably pick up dormant viruses waiting to drop their payload, the way that signature-based scans can. More importantly, predefined behavioral analysis rules are not customized for your network and e-mail systems, and can generate large numbers of false alarms.

Although operating systems provide tools to profile and monitor themselves, and solutions like Microsoft Exchange offer performance counters, their use is limited because they are essentially reactive and serve mainly as forensic tools. The administrator has to be aware of the problem and then utilize these tools to find the cause.

If you could sit around all day and monitor your e-mail server, chances are you would be able to spot a virus outbreak in progress. You are familiar with the day-to-day operations of your e-mail system and know what a normal day's traffic looks like. You know whether or not large mailing lists are in use and how common it is for certain types of files or numbers of files to be sent as attachments to e-mail messages. However, you probably have more important things to do at work. Plus, you have the added drawback of being human. You go out for lunch, occasionally sleep, and sometimes you even take a vacation!

## Introducing Outbreak Manager

Detecting an outbreak before it affects your business has never been an easy task. In the past, identifying and responding to a malicious code outbreak was largely a manual process. Security administrators would receive notification of a potential outbreak from end users via e-mail, phone, or pager and rush to respond to the situation manually.

There are multiple points in the network where an outbreak can be detected and controlled. Given the nature of recent threats, Internet gateways and e-mail servers are a good place to focus. It is estimated that over 86 percent of all virus activity enters the network through the Internet gateway or e-mail server. McAfee is the first to provide a solution to the outbreak management challenge described in this document. Outbreak Manager is a component of McAfee's e-mail-based, anti-virus scanners: WebShield SMTP, GroupShield for Exchange, and GroupShield for Domino.

The Outbreak Manager utility is specifically designed to detect and react to virus outbreaks. It provides proactive protection before virus definitions are available and can take action based on rules that you specify. Outbreak Manager can be configured to respond automatically to a detected

outbreak or can notify you and allow you to respond. You can teach Outbreak Manager all the things you know about your company's e-mail habits and relax while Outbreak Manager watches for suspicious activity.

Depending on the anti-virus software that you have installed, there may be an additional option of specifying your office hours, which allows Outbreak Manager to react automatically to outbreaks if they occur when you are out of the office but to notify you and allow you to respond manually during your office hours.

The Outbreak Manager component of WebShield SMTP, GroupShield for Exchange, and GroupShield for Domino adds the flexibility and rapid response capabilities of behavioral analysis tools to the reliability of McAfee's award-winning, signature-based virus detection.

### **Resident Scanners**

Outbreak Manager works in concert with the McAfee solutions listed below.

- WebShield SMTP
- GroupShield for Microsoft Exchange
- GroupShield for Lotus Domino (AIX version not supported)

WebShield SMTP is an in-line Internet mail scanner—meaning that all SMTP-compliant mail is forwarded to the scanner from a source, scanned for mail, then passed to a destination based on the forwarding rules configured in the software. Since WebShield SMTP does not scan x400 or POP3 mail, it is usually installed behind the firewall as the primary Internet mail connector. After scanning e-mail messages for viruses, WebShield SMTP forwards the mail to the internal e-mail system.

This is in contrast to GroupShield for Microsoft Exchange and Lotus Domino. GroupShield is installed directly into the Groupware application and scans either the information store on Microsoft Exchange servers or the mailbox database areas on Lotus Domino servers, therefore protecting more than just SMTP mail. Products in the GroupShield family also have additional capabilities, such as performing on-demand scans for the entire e-mail system.

### **Understanding Rules**

Outbreak Manager allows administrators to create a rule-based outbreak management system by setting up multiple rules specific to their individual environments.

A rule has four components.

- Trigger—A virus event or events
- Threshold—The number of times the event occurs
- Reaction—Whether Outbreak Manager should act without administrator intervention (automatic) or wait to be instructed how to proceed (manual)
- Response—The action to be taken if automatic reaction is chosen

Using rules, McAfee Outbreak Manager can automate the typical administrator responses to outbreak situations but with two important differences.

- Outbreak Manager witnesses the trigger happening and reacts immediately as instructed, thereby preventing the outbreak
- Outbreak Manager is always on the job 24/7

Outbreak Manager can also enforce sets of escalating rules, allowing you to create very flexible rules that increase in severity of actions over a period of time if the rule continues to trigger. For example, you can create a rule that automatically updates the virus signature files when triggered and progresses to blocking all attachments in later stages if the outbreak behavior continues beyond a certain time period.

You can configure escalation times for the separate actions, so that they are only performed if the rule continues to detect virus outbreaks after the escalation time period has elapsed. An e-mail is sent to the administrator to inform him or her of the situation and of any action taken by the Outbreak Manager. Various actions are listed below.

- Updating the resident, e-mail-based, anti-virus scanners
- Increasing the level of anti-virus scanning
- Temporarily shutting down the resident mail server or anti-virus product

**Rule Status and Logging**

You can view the status of your outbreak rules instantly at the click of a button. This allows you to view the current state of the rule and escalate its actions if it has triggered. Viewing a rule's status can help you gauge how accurately you have specified its thresholds, allowing you to fine-tune them for your organization.

By default, Outbreak Manager continually records the status of each virus outbreak rule with a Log Manager utility, allowing you to view the rule's status and virus outbreak activity as often or as infrequently as you like.

**Trigger Types and Thresholds****Trigger Examples**

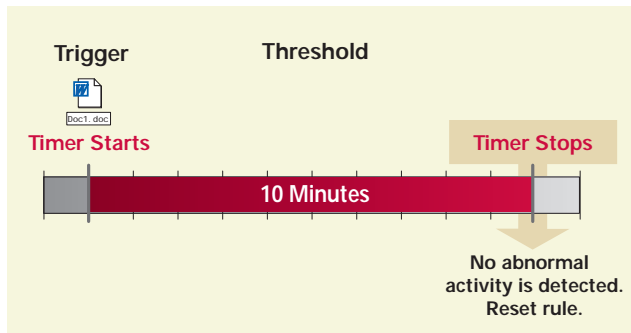
The Outbreak Manager utility can identify virus outbreaks or suspected outbreaks based on the triggers that you specify for the outbreak rules. Depending on your anti-virus software, some of the occurrences for which you can monitor are listed below.

- Number of viruses detected in a time period
  - You select the number of incidents and a time period within which to count the number of events
  - The first instance of a virus event starts an event counter and a timer counter
  - Thereafter each virus alert results in the event counter increasing by one until reaching the limit set in the rule
  - If the trigger limit is reached, the first reaction begins, and these counters are disregarded (since they are no longer relevant)
  - If the time counter has reached its limit set within the rule, then the counters are disregarded, and any subsequent virus alerts will restart the event counter and timer counter
- Number of identical viruses detected in a time period
  - Same as above, although each virus starts its own counters
- Number of identical attachments detected in a time period
  - This is certainly the most useful of all triggers within Outbreak Manager, as it allows you to select the number of identical files detected and a time period within which to count the number of files
- Every file attachment that is detected starts its own event counter and time counter
- Thereafter each identical attachment results in the event counter increasing by one until reaching the limit set in the rule
- If the trigger limit is reached, the first reaction begins, and these counters are disregarded (since they are no longer relevant)
- If the time counter has reached its limit set within the rule, the counters are disregarded, and any subsequent attachments will restart the event counter and timer counter
- Number of identical attachment types detected in a time period
  - Same as above, although instead of monitoring the number of individual attachments, this trigger monitors the number of attachment types over a given time period
  - You select the number of identical attachment types detected and a time period within which to count the number of events
  - Every file attachment type that is detected starts its own event counter and time counter
  - Thereafter each identical attachment type results in the event counter increasing by one until reaching the limit set in the rule
  - If the trigger limit is reached, the first reaction begins, and these counters are disregarded (since they are no longer relevant)
  - If the time counter has reached its limit set within the rule, the counters are disregarded, and any subsequent attachments will restart the event counter and timer counter for that attachment
  - This trigger is a little more difficult to set and is the one most likely to provide you with false alarms if not configured correctly

**Real World Example of Outbreak Manager Rules****Example of a Rule Not Taking Action**

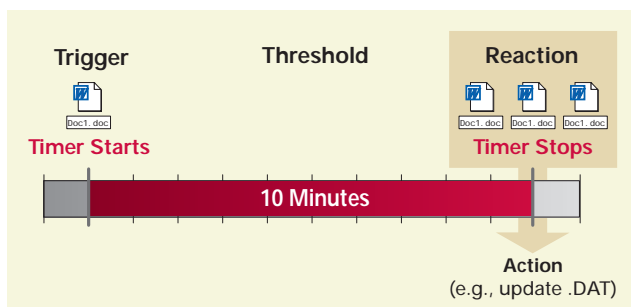
- Trigger—Rule is set to identify an identical attachment received in a ten-minute time period
- Threshold—The clock starts ticking when the trigger occurs; the threshold for this rule looks for multiple occurrences of " doc1.doc" in a ten-minute time period

- **Reaction**—As no other “doc1.doc” is received during threshold period, no action is automatically invoked and no alert is sent to administrator
- **Action**—As there is no automatic response, no action is taken, and the rule is reset



### Example of a Rule Taking Action

- **Trigger**—Rule is set to identify an identical attachment received in a ten-minute time period
- **Threshold**—The clock starts ticking when the trigger occurs; the threshold for this rule looks for multiple occurrences of “doc1.doc” in a ten-minute time period
- **Reaction**—Several occurrences of “doc1.doc” are received during the threshold period; action is invoked automatically and alert is sent to administrator
- **Action**—Outbreak Manager takes action defined by administrator (e.g., update .DAT)



## Understanding Your Mail Protection Requirements

It is important to remember that triggers are the events for which Outbreak Manager monitors, and a threshold is the number of times that an event can occur before Outbreak Manager springs into action. Therefore, it is critical that you carefully construct your rules so that real threats to your organization can be identified. Setting thresholds too low can result in too many false alarms, while setting thresholds too high may allow real threats into your organization.

Every organization's e-mail content is different, depending on policies, business type, and size. One company's potential outbreak is another company's normal e-mail traffic. In order to create rules that accurately detect and stop an outbreak in progress, it is good practice to analyze the type of mail your organization receives.

Once you have a better understanding of what your e-mail looks like on a normal business day, you can best instruct Outbreak Manager to watch for aberrations.

### Profiling Your Company's E-Mail Habits

One of the first steps in analyzing your e-mail traffic is determining what an average day's e-mail volume looks like. To accomplish that, consider the following questions.

- Are large mailing lists commonly in use, or is mail typically sent to individuals in your organization?
- What types of file attachments are common in your organization?
  - Depending on your business and the applications in use, some file attachment types will be commonly used, while others appearing in your e-mail traffic could indicate a threat.
  - For example, if your company uses Visio software to manage organizational charts or to create process diagrams, Visio attachments might be an everyday occurrence. But an organization that is not using Visio should consider a sudden increase in Visio attachments as a symptom of a virus.
- What types of attachments does your organization consider a threat?
  - Use the file attachment risk assessment table to identify the highest-risk file attachments classified as unsafe.
  - You should determine which of these are in use in your organization and set rules that identify when an unusual number of this attachment type is detected in your e-mail traffic.

### File Attachment Risk Assessment

As a general e-mail best practice, it is a good idea to prevent many of the file attachments listed on next page from being received into your organization. However, depending on your e-mail behavior, it may be necessary to receive some high-risk attachments. Outbreak Manager can be used in these instances to apply a rule to a particular high-risk attachment if its behavior constitutes unusual activity in your environment.

| Extension | Description                          | Risk Assessment | Additional Notes on Attachment   |
|-----------|--------------------------------------|-----------------|--|
| ADE       | Microsoft Access Project Extension   | Medium          | No known threat but potentially dangerous  |
| ADP       | Microsoft Access Project             | Medium          | No known threat but potentially dangerous  |
| ASP       | MS Active Server Page                | High            | Known destructive code   |
| BAS       | Visual Basic Module                  | Medium          | Potentially dangerous  |
| BAT       | MS-DOS Batch File                    | Medium          | DOS-based scripting has some business validity, not a very strong delivery method for destructive code |
| CHM       | Compiled HTML Help File              | High            | Common method of delivery of destructive code, very dangerous  |
| CMD       | Windows NT Command Script            | Medium          | Known destructive code   |
| COM       | MS-DOS Application                   | Medium          | Known destructive code   |
| CPL       | Control Panel Extension              | High            | Known destructive code   |
| CRT       | Security Certificate                 | Medium          | No known threat but potentially dangerous  |
| EXE       | Application                          | High            | Common method of delivery of destructive code, very dangerous  |
| HLP       | Windows Help File                    | Medium          | Known destructive code   |
| HTA       | HTML Application                     | High            | Known destructive code   |
| HXS       | Windows Help File V2                 | High            | Known destructive code   |
| HTM       | HTML Page                            | High            | Known destructive code   |
| INF       | Setup Information File               | High            | Used in installation of applications, known destructive code   |
| INS       | Internet Communication Settings      | Medium          | No known threat but potentially dangerous  |
| ISP       | Internet Communication Settings      | Medium          | No known threat but potentially dangerous  |
| JS        | JScript File                         | High            | Sometimes blocked, as there are a number of "childs" to this type                                      |
| JSE       | JScript Encoded Script File          | High            | Known destructive code   |
| LNK       | Shortcut                             | High            | Known destructive code   |
| MACRO     | Office Applications Excel and Word   | High            | Embedded macros, known virus activity associated with macros, very common method of delivery           |
| MDB       | Microsoft Access Application         | Medium          | Database with scripting capabilities, no known destructive code  |
| MDE       | Microsoft Access MDE Database        | Medium          | Database with scripting capabilities, no known destructive code  |
| MSC       | Microsoft Common Console Document    | High            | No known threat but potentially dangerous  |
| MSI       | Windows Installer Package            | High            | No known threat but potentially dangerous  |
| MSP       | Windows Installer Patch              | High            | No known threat but potentially dangerous  |
| MST       | Visual Test Source File              | Medium          | No known threat but potentially dangerous  |
| PCD       | Photo CD Image                       | Medium          | No known threat but potentially dangerous  |
| PDF       | Adobe File                           | Medium          | Known virus, must have full install of Adobe to become an impact                                       |
| PI        |                                      | High            | Known destructive code   |
| PIF       | Shortcut Link                        | High            | Known destructive code   |
| REG       | Registration Entries                 | High            | Changes registry entries when clicked, not a very good way to deliver destructive code                 |
| SCR       | Screen Saver                         | High            | Common method of delivery of destructive code, very dangerous  |
| SCT       | Windows Script Component             | Medium          | No known threat but potentially dangerous  |
| SH        |                                      | High            | Sometimes blocked, as there are a number of "childs" to this type                                      |
| SHB       | Document Shortcut File               | High            | Potentially very dangerous   |
| SHS       | Shell Scrap Object                   | High            | Common method of destructive code delivery, very dangerous   |
| URL       | Internet Locator                     | High            | Potentially very dangerous   |
| VB        | Typical VBScript File Type           | High            | Sometimes blocked, as there are a number of "childs" to this type                                      |
| VBE       | VBScript Encoded Script File         | High            | Common method of destructive code delivery, very dangerous   |
| VBS       | VBScript Script File                 | High            | Common method of destructive code delivery, very dangerous   |
| VSD       | Microsoft Visio File Type            | Medium          | Visio file, no known virus but potential is there  |
| VSS       | Visio File Type                      | Medium          | Visio file, no known virus but potential is there  |
| VST       | Visio File Type                      | Medium          | Visio file, no known virus but potential is there  |
| VSW       | Visio File Type                      | Medium          | Visio file, no known virus but potential is there  |
| WMV       | Windows Media Viewer                 | High            | Known virus vulnerabilities  |
| WS        | Typically a Windows Script Component | Medium          | No known threat but potentially dangerous  |
| WSC       | Windows Script Component             | Medium          | No known threat but potentially dangerous  |
| WSF       | Windows Script File                  | Medium          | No known threat but potentially dangerous  |
| WSH       | Windows Script Host Settings File    | Medium          | No known threat but potentially dangerous  |

### Methods of Profiling E-Mail Activity

Some of the resources and tools you can use to gather the information you need to start creating your Outbreak Manager rules are discussed in this section.

- McAfee GroupShield by Network Associates®—Analyzing average virus activity over time while an outbreak is not occurring can help you construct rules that can trigger if a certain number of viruses are detected in a time period
- AppAnalyzer by NETIQ for Exchange version 2.0—A Web-based reporting and analysis solution that helps messaging administrators and IT managers monitor and understand Microsoft Exchange Server usage
- OmniAnalyser by Hypersoft Information Systems—Delivers metrics on all messaging traffic, server availability, and information store contents statistics in Microsoft Exchange and Lotus Domino organizations

**McAfee Security** 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766)

---

Network Associates® products denote years of experience and commitment to customer satisfaction. The PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects—all with service levels to meet the needs of every customer organization. McAfee® Research, a world leader in information systems and security, continues to spearhead innovation in the development and refinement of all our technologies.

Network Associates, McAfee, GroupShield, WebShield, and PrimeSupport are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Sniffer® brand products are made only by Network Associates, Inc. All other registered and unregistered trademarks herein are the sole property of their respective owners. ©2004 Networks Associates Technology, Inc. All Rights Reserved. 6-sps-obm-001-0104