Worry Free Business Security Services

Outbreak Prevention Policy

Outbreak Prevention Policy

Outbreak Defense is a key component of the WFBS-SVC solution and protects your business during a worldwide threat outbreak.
The Outbreak Defense Strategy is based on the idea of an Internet-wide outbreak life cycle. The life of an outbreak is divided into three stages — **Threat Prevention**, **Threat Protection**, and **Threat Cleanup**. Trend Micro counters each stage of the cycle with a defense strategy called Outbreak Defense.

Outbreak Defense Response to the Outbreak Life Cycle Stages.

Outbreak Stage	Outbreak Defense Stage
In the first stage of an outbreak cycle, the experts at Trend Micro observe a threat that is actively circulating on the Internet. At this time, there is no known solution for the threat.	Threat Prevention Outbreak Defense prevents the threat from attacking your devices and network by taking actions according to the Outbreak Policy downloaded from Trend Micro update servers. These actions include sending alerts, blocking ports and denying access to folders and files.
In the second stage of the outbreak, computers that have been affected by the threat pass the threat along to other devices. The threat begins to rapidly spread through local networks causing business interruptions and damaging devices.	Threat Protection Outbreak Defense protects at-risk devices by notifying them to download the latest components and patches.
In the third and final stage of an outbreak, the threat subsides with fewer reported incidents.	Threat Cleanup Outbreak Defense repairs damage by running Cleanup services. Other scans provide information that Administrators can use to prepare for future threats.

Outbreak Defense Actions

The Outbreak Defense Strategy was designed to manage outbreaks at every point along the outbreak life cycle. Based on the Outbreak Prevention Policy, Automatic Threat Response typically takes preemptive steps such as:

- Blocking shared folders to help prevent virus/malware from infecting files in shared folders
- Blocking ports to help prevent virus/malware from using vulnerable ports to spread the infection on the network and clients
- Outbreak Defense never blocks the port used by the WFBS-SVC Server to communicate with clients.
- Denying write access to files and folders to help prevent virus/malware from modifying files
- Assessing clients on your network for vulnerabilities that make it prone to the current outbreak
- Deploying the latest components such as the virus pattern file and virus cleanup engine
- Performing a **Cleanup** on all the clients affected by the outbreak
- If enabled, scanning your clients and networks and takes action against detected threats

✔ ***Note:*** *When Trend Labs creates an OPP, the same OPP can apply not only to WFBS-SVC , but also to other Trend Micro products that provide client protection.*

Automatic Outbreak Defense Detail

The Automatic Outbreak Defense Detail section displays information about the virus/malware that is currently on the Internet and could potentially affect your network and clients. Based on threat information, the Outbreak Prevention Policy (OPP) takes steps to protect the network and clients while Trend Micro develops a solution (See Trend Micro Outbreak Prevention Policy).
This section provides the following information:

- **Alert Type:** Red or Yellow
- **Risk Level:** The level of risk the threat poses to clients and networks based on the number and severity of the virus/malware incident.
- **Delivery method:** How the threat is spread
- **Automatic Response:** Click to enable/disable the Automatic Response
- **Automatic Response Details:** Click **More info** to view the specific actions Outbreak Defense is using to protect your clients from the current threat.

Status of Devices within Outbreak Prevention Enforcement

The section displays the total for the number of clients with and without automatic alert enabled. Click the number link under the **Enabled** and **Not Enabled** columns to view more information about specific clients.

Vulnerable Devices

The Vulnerable Devices section displays a list of clients that have vulnerabilities. A vulnerable device has weaknesses in its operating system or applications. Many threats exploit these vulnerabilities to cause damage or gain unauthorized control. Therefore, vulnerabilities represent risks not only to each individual device where they are located, but also to the other devices on your network.

Scan For Vulnerabilities Now

Clicking **Scan for Vulnerabilities Now** sends a notification to all the Security Agents to perform a vulnerability scan on the Clients. After clicking Scan for Vulnerabilities Now, The Scan Notifying Progress screen appears temporarily to show you the progress of the notification and then is replaced with the Scan Notifying Results screen.
The Scan Notifying Results screen displays whether or not the WFBS-SVC Server has successfully notified a Client. Unsuccessful results occur when a Client is offline or in unexpected situations such as when there are network interruptions.

Enable/Disable OPP

Clicking this takes you to the **Administration > Global Settings** page. Here you can enable/disable red and yellow alerts issued by Trend Micro.

Red Alerts

Several infection reports from each business unit reporting rapidly spreading malware, where gateways and email servers may need to be patched.
The industry's first 45-minute Red Alert solution process is started: An official pattern release (OPR) is deployed with notification of its availability, any other relevant notifications are sent out, and fix tools and information regarding vulnerabilities are posted on the download pages.

Yellow Alerts

Infection reports are received from several business units as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download. In case of an email-spreading malware, content filtering rules, called Outbreak Prevention Policies (OPP), are sent out to automatically block related attachments on servers equipped with the product functionality.

Trend Micro Outbreak Prevention Policy

The Trend Micro Outbreak Prevention Policy is a set of Trend Micro recommended default security configuration settings that are applied in response to an outbreak on the network.
The Outbreak Prevention Policy is downloaded from Trend Micro to the WFBS-SVC Server.
When the WFBS-SVC Server detects an outbreak, it determines the degree of the outbreak and immediately implements the appropriate security measures as stated in the Outbreak Prevention Policy.
Based on the Outbreak Prevention Policy, Automatic Threat Response takes the following preemptive steps to secure your network in the event of an outbreak:

- Blocks shared folders to help prevent virus/malware from infecting files in shared folders
- Blocks ports to help prevent virus/malware from using vulnerable ports to infect files on the network and clients
- Denies write access to files and folders to help prevent virus/malware from modifying files
- Displays an alert message on clients when an outbreak detected
-

Situations of OPP Notification

Outbreak Prevention notifications can be received by the client in the following situations:

- Client restart
- Client reconnection to the network
- When Update Now is performed
- When a client scheduled update is performed

OPP Configurations

OPP Functions in the Agents

OPPs are applied to non-pattern file functions in both the Client/Server Security Agent. In an outbreak, an OPP will be applied as a temporary measure, while TrendLabs create a pattern for more permanent protection.

Applying OPP Configurations in the Agents

The OPP configurations is in the form of XML files (OppActive.xml and OppBackup.xml) to the agents.

The agents analyze and use the OPP settings in the configuration file.

The following steps take place:

1. OppActive.xml contains the OPP configuration for each agent.
2. If the agents use existing protection settings, such as port blocking in the Client/Server Security Agent the settings are written to OppBackup.xml.
3. OppActive.xml is parsed by the agents.
4. If the existing settings in the agents are the same as those applied by the OPP, there is no need to take any further action on the OPP.
5. If the existing settings are different from the OPP, the new OPP settings are applied.

OPP Functions for a Client/Server Security Agent

An OPP incorporates the following functions in a Client/Server Security Agent. Port blocking rules are applied to the

- Shared folder blocking
- Port blocking
- Write Access Denial to Files and Folders

Shared Folder Blocking

Shared folder blocking is applied to all shared folders on selected computers. Two blocking levels are provided:

- Read only (Deny write)
- Deny read and write

Port Blocking

The OPP can block specify ports by the following way:

- Blocking ports which Trend Micro advises as vulnerable to trojans
- Specifying the ports by individual port numbers or a range of port numbers.
- Block specific ports for incoming traffic and outgoing traffic
- Block traffic on ports that follow a specific protocol for example TCP and/or UDP.

Port blocking in an OPP is implemented through port-blocking rules that are added to the existing rules by the firewall driver.

1. When invoked the OPP module sends the outbreak prevention policy (TmOpp.ini) to the ECF component on the Client/Server Security Agent, through tmlisten.exe
2. The Communicator receives the outbreak prevention settings that relate to port blocking and sends these to the Rule Set Generator.
3. This loads the outbreak prevention settings to memory and then notifies the Common Firewall adapter, which, in turn, notifies the Common Firewall API.
4. This informs the CFWD that the Client Firewall settings have been updated.
5. This reads the settings in memory.

More information on these port blocking rules is provided in the OPP Module section of the Client/Server Security Agent chapter on 109. The following steps occur during port blocking:

Blocking Trojan Ports

Trojan ports are port numbers that are known to be used by Trojans to gain access to computers.

✔ ***Note:*** *Different Trojan variants of the Trojan can use different ports. The administrator can manually add other ports to block after blocking all advised Trojan ports.*

Denying write access to files and folders

Viruses can modify or delete files and folders on their host computers. When a virus outbreak occurs, the administrator can prevent viruses from modifying or deleting files and folders on clients using the deny write function of Outbreak Prevention. When configuring the deny write function of Outbreak Prevention, the administrator can deny write access to:

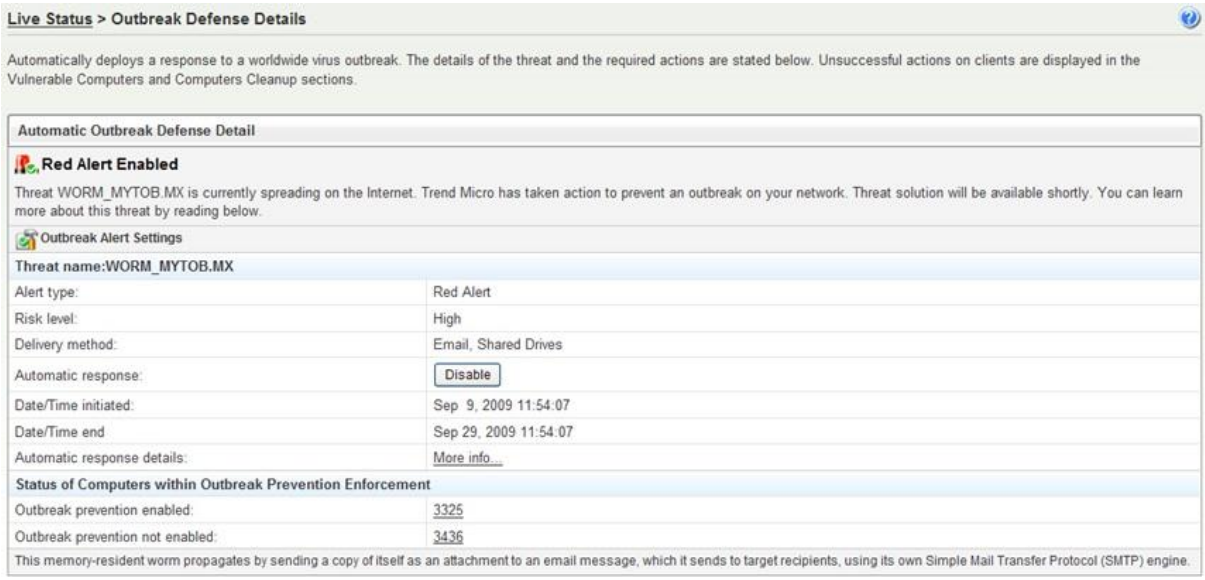
- All file name extensions in specific folders
- Specific file name extensions in specific folders
- Specific file names in all folders

Deny write access to specific file name extensions in specific folders

To deny write access to specific files names in specific folders, the administrator first needs to specify the folders to protect. Then select Files in the protected directories with the following extensions and then specify the file name extensions to protect. File extensions that are not protected can still be written to. For example, if the administrator adds c:\DWFolder to the list of protected folders and then denies write access to file with an EXE extension, then c:\DWFolder\immune.exe cannot be written to, but c:\DWFolder\test.txt can still be written to.

Deny write access to specific file names in all folders

When the administrator specifies a file name in the Files to Protect text box, Outbreak Prevention denies write access to this file in all folders. For example, if the administrator adds immune.txt to the deny write file list, then all files named immune.txt will be protected, including:
`C:\test\immune.txt`
`D:\testfolder\test1\immune.txt`
\\testing\sharefolder\immune.txt



Dismiss the OPP

There are 4 scenarios can dismiss the OPP alert

1. OPP duration is expired

   The default value of duration for Red Alert / Yellow Alert is 2 days, and then after OPP is activated 2 days, the OPP will be auto stopped.

2. local components match OPP criteria

   OPP pattern has define the components that can defense the target malware, such like pattern ,engine, and TSC module, when client updated and matched the component version that defined in OPP pattern, OPP will dismiss.

3. Admin disabled the OPP manually

   Admin might disable the OPP from web console.

4. Another new OPP is activating

   When another new OPP from TrendLab, the existing OPP will be auto stopped, and then the new OPP will be activated.