



Best Practices for Deploying Behavior Monitoring and Device Control



Contents

Overview.....	3
Behavior Monitoring Overview	3
Malware Behavior Blocking.....	3
Event Monitoring.....	4
Enabling Behavior Monitoring.....	8
Device Control Overview	9
Using Device Control	10
How Behavior Monitoring and Device Control Can Affect Performance.....	13
Deploying Behavior Monitoring and Device Control.....	13
Step 1: Preparing a Pilot Environment	14
Step 2: Identifying System-Intensive Applications	15
Step 3: Adding System-Intensive Applications to the Behavior Monitoring Exception List.....	16
Alternative Ways to Prevent Performance Impact	18
Disabling Features from the Web Console.....	18
Disabling Features through the Registry	19
Stopping the Service.....	21

Overview

Trend Micro™ OfficeScan™ protects enterprise networks from malware, network viruses, Web-based threats, spyware, and mixed threat attacks. Behavior Monitoring and Device Control are some of the new OfficeScan features that proactively aim to prevent malware attacks.

This document aims to increase knowledge about Behavior Monitoring and Device Control and help readers avoid potential issues during deployment.

Behavior Monitoring Overview

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or installed software. Behavior Monitoring is composed of the following sub-features:

- [Malware Behavior Blocking](#)
- [Event Monitoring](#)

Malware Behavior Blocking

Malware Behavior Blocking provides a necessary layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time and as programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats.

Note: *To help ensure that this feature does not interfere with critical applications, OfficeScan leaves this feature disabled on server platforms, even when it is enabled through the console. To enable this feature on a server computer, manually modify registry settings on that computer. For instructions, see the Administrator's Guide.*

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Figure 1-1: Malware Behavior Blocking setting



Tip: Before deploying Malware Behavior Blocking, Trend Micro recommends running a pilot deployment. See [Deploying Behavior Monitoring and Device Control](#) for more information.

Event Monitoring

Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks. It uses a policy-based approach where system areas are monitored for certain changes, allowing administrators to regulate programs that cause such changes.

If attempts to change the system are made, Event Monitoring will:

- Refer to the Event Monitoring policies and perform the configured action.
- Notify the user or administrator

Use the Event Monitoring if you have specific system protection requirements that are above and beyond what is provided by Malware Behavior Blocking.

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Figure 1-2: Event Monitoring setting



The following Event Monitoring policies define which events it checks for and how it handles each event.

Table 1-1: Event monitoring policies

Events	Description	Default Action
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.	Assess
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the Web browser is redirected to infected, non-existent, or fake Web sites.	Assess
System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.	Assess
New Internet Explorer Plugin	Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.	Assess
Layered Service Provider	A Layered Service Provider (LSP) can manipulate inbound and outbound network traffic. Malicious programs can use LSPs to intercept network communication and gain network access.	Assess
Internet Explorer Setting Modification	Many virus/malware programs change Internet Explorer settings, including the home page, trusted Web sites, proxy server settings, and menu extensions.	Assess

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Events	Description	Default Action
Security Policy Modification	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.	Assess
Firewall Policy Modification	The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.	Assess
Program Library Injection	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.	Assess
Shell Modification	Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.	Assess
New Service	Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.	Assess

Events	Description	Default Action
New Startup Program	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.	Assess

Administrators can choose to perform one of the following actions to respond to monitored events:

- **Assess:** Always allow processes associated with an event but record this action in the logs for assessment

***Note:** Use this option during initial deployment to assess the impact of enabling Behavior Monitoring features.*

- **Allow:** Always allow processes associated with an event
- **Ask When Necessary:** Prompts users to allow or deny processes that may have violated Behavior Monitoring policies. If selected, a prompt asking users to allow or deny the process and add to the Allowed Programs or Blocked Programs appears. If users do not respond within the time period specified in the Behavior Monitoring settings screen, OfficeScan automatically allows the process to continue.
- **Deny:** Always block processes associated with an event and record this action in the logs

Enabling Behavior Monitoring

Path: Networked Computers > Client Management > Settings > Behavior Monitoring Settings

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

To enable Malware Behavior Blocking or Event Monitoring, select the following options:

- **Enable Malware Behavior Blocking** (workstation default: on; server default: off)
- **Enable Event Monitoring** (workstation default: on; server default: off)

Note: Since Malware Behavior Blocking is enabled by default, Trend Micro strongly recommends [identifying system-intensive applications](#) and adding them to the [exception list](#) before deploying OfficeScan. For more information, see [How Behavior Monitoring and Device Control Can Affect Performance](#).

Behavior Monitoring settings can be applied to specific entities in the client tree or all entities (root). If you are applying settings to the root, you need to select one of the following options:

- **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing/future domain (domains not yet created during configuration).
- **Apply to Future Domains Only:** Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Device Control Overview

Device Control regulates access to external storage devices and network resources. Device Control helps prevent the propagation of malware on removable drives and network shares and, combined with file scanning, helps guard against security risks.

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Figure 1-3: Device Control settings

Notification messages are displayed on the endpoints when device control violations occur. Administrators can modify the default notification message.

Note: To help ensure that this feature does not interfere with critical applications, OfficeScan leaves this feature disabled on server platforms, even when it is enabled through the console. To enable this feature on a server computer, manually modify registry settings on that computer. For instructions, refer to the Administrator's Guide.

Using Device Control

Path: Networked Computers > Client Management > Settings > Device Control

To configure Device Control:

1. Select the **Enable device control** option.
2. Choose whether to block or allow the AutoRun function (`autorun.inf`) on USB devices connected to the computer.
3. Select the permissions for each device type.


© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Table 1-2: Device permissions

Permissions	Files on the Device	Incoming Files
Full access	Operations allowed: Copy, Move, Open, Save, Delete, Execute	Operations allowed: Save, Move, Copy This means that a file can be saved, moved, and copied to the device.
Read and write only	Operations allowed: Copy, Move, Open, Save, Delete Operation blocked: Execute	Operations allowed: Save, Move, Copy
Read and execute only	Operations allowed: Copy, Open, Execute Operations blocked: Save, Move, Delete	Operations blocked: Save, Move, Copy
Read only	Operations allowed: Copy, Open Operations blocked: Save, Move, Delete, Execute	Operations blocked: Save, Move, Copy
No access	Any attempt to access the device or network resource is automatically blocked.	Operations blocked: Save, Move, Copy

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Note: *The antivirus feature in OfficeScan complements Device Control. For example, if Device Control allows a file to open from a regulated device but OfficeScan detects that the file is infected, a scan action will still be performed on the file to eliminate the malware.*

4. Select whether to display a notification message on the client computer when OfficeScan detects unauthorized device access.
5. If you selected domain(s) or client(s) on the client tree, click **Save** to apply settings to the domain(s) or client(s). If you selected the root icon  , choose from the following options:

Apply to All Clients: Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.

Apply to Future Domains Only: Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

How Behavior Monitoring and Device Control Can Affect Performance

The Behavior Monitoring and Device Control features both use the Trend Micro Unauthorized Change Prevention Service (running under the process name TMBMSRV.EXE). These features use TMBMSRV.EXE to monitor for system events and check these events against rules to determine whether certain application activities are unwanted.

TMBMSRV.EXE delivers highly beneficial behavior-based security functionality, particularly the capability to check applications for suspicious behavior (Behavior Monitoring) and control access to storage devices (Device Control). Its monitoring mechanism, however, can strain system resources, especially when the computer is running applications that cause numerous system events. To prevent impacting system performance, Trend Micro recommends configuring OfficeScan so that these “system-intensive” applications are *not* monitored by TMBMSRV.EXE.

Deploying Behavior Monitoring and Device Control

Running TMBMSRV.EXE and system-intensive applications on the same computer can affect system performance and disrupt critical applications. It is for this reason that a properly managed deployment of Behavior Monitoring and Device Control is recommended.

To ensure smooth deployment of OfficeScan with Behavior Monitoring and Device Control:

- Set up and deploy a pilot environment. See [Step 1: Preparing a Pilot Deployment](#).

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

- Identify system-intensive applications. See [Step 2: Identifying System-Intensive Applications](#).
- Add system-intensive applications to the Behavior Monitoring exception list. See [Step 3: Adding System-Intensive Applications to the Behavior Monitoring Exception List](#).

Step 1: Preparing a Pilot Environment

Before performing a full-scale deployment, conduct a pilot deployment in a controlled environment. A pilot deployment provides opportunity to determine how features work and, most importantly, how Behavior Monitoring and Device Control can affect your endpoints.

The pilot process should result in:

- A better understanding of the implications of deploying the new Behavior Monitoring and Device Control features.
- A better understanding of applications that may conflict with these features.
- A list of applications that can be added to the Behavior Monitoring exception list.

When setting up the pilot environment:

- Prepare an environment that matches the production environment as closely as possible.
- Ensure that the following are included in the pilot environment:
 - Business applications
 - Custom applications

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

- All network applications used by groups or individuals (such as payroll, inventory, accounting, and database applications)
- Deploy the OfficeScan clients into the pilot environment with the features that you intend to enable. For example, Behavior Monitoring and Device Control may both be enabled.
- Allow the pilot environment to run for a reasonable amount of time (give sufficient “soak time”) with the standard applications running and with average daily use.

Step 2: Identifying System-Intensive Applications

Trend Micro provides a standalone performance tuning tool to help identify applications that could potentially cause a performance impact. The TMPerfTool tool, available from Trend Micro Technical Support [here](#), should be run on a standard workstation image and/or a few target workstations during the pilot process to preempt performance issues in the actual deployment of Behavioral Monitoring and Device Control.

To identify system-intensive applications:

1. Unzip the `TMPerfTool.zip` file.
2. Place the `TMPerfTool.exe` file in the OfficeScan default installation folder (`%ProgramDir%/Trend Micro/OfficeScan Client`) or in the same folder as the `TMBMCLI.dll` file.
3. Double-click `TMPerfTool.exe`.
4. Click **Analyze** when the system or applications start to slow down. If a red highlighted row appears, it means that the TMPerfTool found a system-intensive process.
5. Select the highlighted row and click **Exclude**.

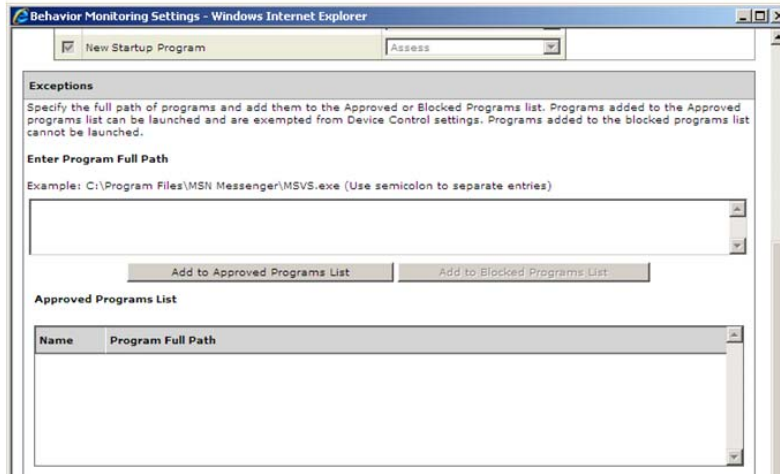
6. After excluding the process, verify if the system or application performance improves. If the performance improves, select the process row again and click **Include**. If the performance drops again, it means you found a system-intensive application. Perform the following:
 - a) Note the name of the application.
 - b) Click **Stop**.
 - c) Click **Generate Log** and save the .xml file in a specified folder.
 - d) Review the applications that have been identified as conflicting and add them to the Behavior Monitoring exception list. For instructions, see [Step 3](#).

Step 3: Adding System-Intensive Applications to the Behavior Monitoring Exception List

The Behavior Monitoring exception list is a user-configurable list of approved and blocked programs that are not monitored by Behavior Monitoring and Device Control. These features automatically allow approved programs to continue—approved programs are still checked by other OfficeScan features. Blocked programs are never allowed to run.

Trend Micro strongly recommends adding system-intensive applications to the Behavior Monitoring exception list to reduce the likelihood of performance issues from occurring. System-intensive applications can cause TMBMSRV.EXE (the service used by both Behavior Monitoring and Device Control) to consume very high amounts of CPU resources and disrupt critical applications.

Figure 1-4: Adding programs to the exception list



To add programs to the exception list:


Path: Networked Computers > Client Management > Settings > Behavior Monitoring Settings

1. Type the full path of the program under **Exceptions**.

Note: *Separate multiple entries with semicolons (;). The exception list supports wildcards and UNC paths.*

2. Click **Approved Programs** or **Blocked Programs**

Note: *All exceptions apply to both Behavior Monitoring and Device Control. Add only verified programs to the Approved Programs list to ensure network security.*

3. If you selected domain(s) or client(s) on the client tree, click **Save** to apply settings to the domain(s) or client(s). If you selected the root icon  , choose from the following options:
 - **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.
 - **Apply to Future Domains Only:** Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

Alternative Ways to Prevent Performance Impact

To prevent TMBMSRV.EXE from affecting performance, you can disable the service itself or disable both Behavior Monitoring and Device Control.

Warning: *Disabling the Behavior Monitoring, Device Control, and other features may put your network at risk from new and suspicious attacks. Perform these actions only as a last resort.*

You can disable Behavior Monitoring and Device Control from the Web console or from the registry.

Disabling Features from the Web Console


Behavior Monitoring

Path: Networked Computers > Client Management > Settings > Behavior Monitoring Settings

To disable Behavior Monitoring, deselect the following options:

© 2010 Trend Micro Inc. Information provided in this document is subject to change without notice. Trend Micro, OfficeScan, and the t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

- **Enable Malware Behavior Blocking**
- **Enable Event Monitoring**


If you selected domain(s) or client(s) on the client tree, click **Save** to apply settings to those domain(s) or client(s). If you selected the root icon , choose from the following options:

- Apply to All Clients
- Apply to Future Domains Only

Device Control

Path: Networked Computers > Client Management > Settings > Device Control

To disable Device Control, deselect **Enable Device Control**.

If you selected domain(s) or client(s) on the client tree, click **Save** to apply settings to the domain(s) or client(s). If you selected the root icon , choose from the following options:

- Apply to All Clients
- Apply to Future Domains Only

Disabling Features through the Registry

To disable features through the registry, you need to modify the registry on each affected endpoint. You can also save the edited registry section to a REG file and then deploy this REG file to your endpoints.

Note: *Changing the registry directly overrides settings on the console. However, changes made to the registry will not take effect if the Client Self-Protection*

feature is enabled. Disable Client Self-Protection before modifying OfficeScan registry entries. See the Administrator's Guide for more information.

To disable features through the registry:

1. Open Registry Editor. Click **Start > Run**. Type REGEDIT and click **Open**.
2. Navigate to the following registry key:

```
HKEY_LOCAL_MACHINE \SOFTWARE \TrendMicro\PC-  
cillinNTCorp \CurrentVersion\Misc.
```

3. Modify the value for the registry entry **DoNotDisableFuncOnServerPlatform** to **"1"**. Refer to the list below to understand how the different values affect OfficeScan:
 - **0**: Disable OfficeScan Firewall, Behavior Monitoring, Device Control, and Client Self-protection.
 - **1**: Enable OfficeScan Firewall but disable Behavior Monitoring, Device Control, and Client Self Protection.
 - **2**: Enable Behavior Monitoring, Device Control and Client Self Protection, but disable OfficeScan Firewall.
 - **3**: Enable OfficeScan Firewall, Behavior Monitoring, Device Control and Client Self Protection.
4. Restart the OfficeScan client.

Stopping the Service

Disable Behavior Monitoring and Device Control by stopping the Trend Micro Unauthorized Change Prevention Service (TMBMSRV.EXE). Perform this task directly on each endpoint.

Note: Starting and stopping services directly overrides settings on the console. However, these changes will not take effect if the Client Self-Protection feature is enabled. Disable Client Self-Protection before starting or stopping OfficeScan services. See the Administrator's Guide for more information.

To stop the service:

1. Open the Services console. Click **Start > Run**. Type SERVICES.MSC and click **Open**.
2. In the Services console, stop Trend Micro Unauthorized Change Prevention Service.