Are you giving up on security measures

because of their impact on performance and of having to update pattern files?

Use Lockdown

to protect
application-specific terminals
or legacy OS terminals.

Lockdown security software

Trend Micro Safe Lock™

This product uses lockdown* to prevent intrusion and execution of viruses and other malware.

Because it has a limited impact on system performance and does not require updating of pattern files, it can protect terminals reserved for critical control systems, embedded devices, legacy OS terminals, etc.

Also, its easy user interface and cooperation with TMPS enables rapid deployment and a high degree of operability.

Application Whitelisting | No Internet connection required | Exploit protections | Easy operation

***What is lockdown?**

Changing a general IT system/device to a dedicated system/device for a specified purpose or purposes by limiting system functions, and by controlling system resources and accesses.

Product features

Application Whitelisting

Because of a mechanism that allows only pre-registered applications to run (whitelist), malware is prevented from running, while the impact on performance is reduced in comparison with compared to the security software that uses pattern files.

No Internet connection required

Because the routine of updating pattern files is not required, terminals can be protected in an environment that is not connected to the Internet.

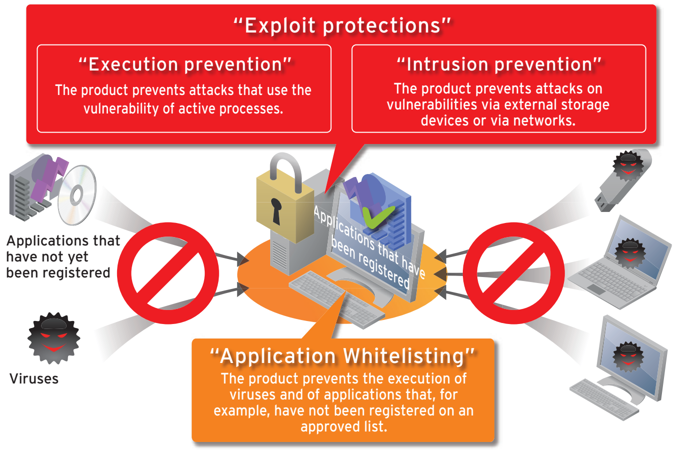
Exploit protections

By its intrusion prevention and execution prevention functions, the product prevents attacks on vulnerabilities mediated via external storage media or via networks, preventing attacks active processes, and thereby reducing the risk of virus infection and unauthorized execution.

Easy operation

Features such as a GUI with good visibility and operability and a function that cooperates with Trend Micro Portable Security™ (referred to below as TMPS) facilitate efficient maintenance work. In addition, a function whereby you can pre-specify an updater that you trust enables the product to operate without compromising maintainability.

Product image



"Exploit protections"

"Execution prevention"
The product prevents attacks that use the vulnerability of active processes.

"Intrusion prevention"
The product prevents attacks on vulnerabilities via external storage devices or via networks.

Applications that have not yet been registered

Viruses

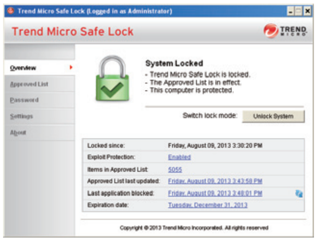
"Application Whitelisting"
The product prevents the execution of viruses and of applications that, for example, have not been registered on an approved list.

Function Overview

● Application Whitelisting

The product controls the execution of applications in accordance with a approved list*. It has two execution modes: "block" and "detect only".
Whitelisted files include Exe, DLL. Driver, script files etc.

*It holds file paths and hash values of target files.



System Locked
- Trend Micro Safe Lock is locked.
- The Approved List is in effect.
- This computer is protected.

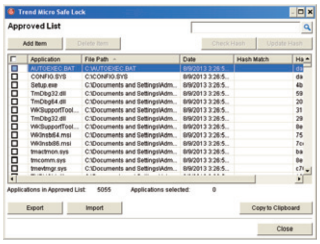
Switch lock mode: Unlock System

Locked since:	Friday, August 09, 2013 3:30:20 PM
Exploit Protection:	Enabled
Items in Approved List:	5055
Approved List last updated:	Friday, August 09, 2013 3:43:58 PM
Last application blocked:	Friday, August 09, 2013 3:48:01 PM
Expiration date:	Tuesday, December 31, 2013

Copyright © 2013 Trend Micro Incorporated. All rights reserved

● Approved list management

An easy default setting that automatically assembles the controlled files present in the system, a manual editing function, a function for pre-specifying a trusted updater, an export/import function, and a hash value checking function, make for ease of installation and operation and improved visibility.



	Application	File Path	Date	Hash Match	Ha
☐	AUTOEXEC.BAT	C:\AUTOEXEC.BAT	8/9/2013 3:26:5...		da
☐	CONFIG.SYS	C:\CONFIG.SYS	8/9/2013 3:26:5...		da
☐	Setup.exe	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		4b
☐	TmDbg32.dll	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		59
☐	TmDbg64.dll	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		20
☐	WKSupportTool...	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		31
☐	TmDbg32.dll	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		29
☐	WKSupportTool...	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		8e
☐	WKInsb64.msi	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		75
☐	WKInsb86.msi	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		7c
☐	tmactmon.sys	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		ba
☐	tmcomm.sys	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		8e
☐	tmevtmgr.sys	C:\Documents and Settings\Adm...	8/9/2013 3:26:5...		c7

Applications in Approved List: 5055 Applications selected: 0

● Exploit protections

Countermeasures against USB malware and network viruses, together with DLL injection prevention, API hooking prevention, and memory randomization, reduce the risk of unauthorized execution and of viral transmission.

● Role based administration

Two types of account are available: an administrator account and a restricted user account. The limited user account can be restricted as to the functions for which it can be used.

● Log

A log of all the activities of this product is entered onto the Windows event log. Because it is not displayed on the notification screen when in operation, it does not impede the use of the system.

● Cooperation with TMPS

When using the off-line terminal virus scanning and removal tool TMPS on a terminal on which this product has been installed, you can use TMPS without adding the permitted executable files to the approved list.

● Interfaces

In addition to a CLI (command line interface), a GUI with good operability and visibility is available.

System requirements

	Trend Micro Safe Lock for Client	Trend Micro Safe Lock for Server
OS	Windows 2000 Professional SP4 32bit Windows XP Professional SP1, SP2, SP3 32bit Windows Vista Business / Enterprise / Ultimate NoSP, SP1, SP2 32bit Windows 7 Professional / Enterprise / Ultimate NoSP, SP1 32/64bit Windows XP Embedded Standard SP1, SP2 32bit Windows Embedded Standard 2009 NoSP 32bit Windows Embedded Standard 7 NoSP, SP1 32/64bit Windows Embedded Enterprise XP SP1, SP2, SP3 32bit Windows Embedded Enterprise Vista NoSP, SP1, SP2 32bit Windows Embedded Enterprise 7 NoSP, SP1 32/64bit	Windows 2000 Server SP4 32bit Windows 2003 Standard / Enterprise / Storage SP1, SP2 32bit Windows 2003 R2 Standard / Enterprise / Storage NoSP, SP2 32bit Windows 2008 Standard / Enterprise / Storage SP1, SP2 32/64bit Windows 2008 R2 Standard / Enterprise / Storage NoSP, SP1 64bit Windows Embedded Server 2003 SP1, SP2 32bit Windows Embedded Server 2003 R2 NoSP, SP2 32bit Windows Embedded Server 2008 SP1, SP2 32/64bit Windows Embedded Server 2008 R2 NoSP, SP1 64bit
CPU	Conforms with minimum OS requirements	
Memory	Conforms with minimum OS requirements	
Free HDD space required	Minimum 300MB (*checked on installation)	
Display resolution	VGA minimum (640X480) minimum 16 colors	

- Some of the vulnerability attack prevention features (memory randomization, DLL injection prevention, API hooking prevention) do not work with a 64bit OS.
- If you have customized the OS components of Windows Embedded, product support may in some cases not be available in respect of faults that do not normally occur in a non-customized environment.
- If you are performing operations such as encryption of a folder or virtualization of an application by means of an OS function or a third-party product, any application whitelisted by such a folder will not be supported.
- If the Japanese edition is used in an environment in which the Japanese language pack has been installed on an English language OS, some garbling of text may occur. Also, in some cases product support will not be available in respect of failures that occur as a result of operation in this environment.
- The OS type, hard disk capacity and other items listed as system requirements, and the ending of support for an OS, are subject to change without notice in the event of product improvement or for any other reason.

Warnings

- Because there is a risk that the introduction of this product may affect the behavior of other applications, you should verify performance and functionality in advance prior to purchasing. The trial version that is available for verification purposes is available to the public at our Web site. http://jp.trendmicro.com
- This product cannot be installed in the same environment as other Trend Micro products.
- A file whose activation is blocked by this product cannot be checked by this product as to whether it is a virus or not. You should check whether it is a legitimate file by reference to its developer source. If there is a need for virus scanning and removal, you should purchase and use Search Trend Micro Portable Security, a virus removal tool for offline terminals. (For OS support of TMPS, please check the system requirements for TMPS.)
- If the applications necessary for the operation of the OS are not registered on the approved list the system will lock, and when the OS is rebooted there is a risk that the OS will not reboot normally, or of not being able to log into the OS. Should this occur, it will be necessary to re-install the OS because it will not be possible to unlock the system or perform any other control functions with this product. You should therefore take care to avoid this problem. (When updating the OS or any other application, you should register the updated files on the approved list.)
- If, after locking the system, if you forget the administrator password, you will not be able to change settings, uninstall or perform other operations with this product. In this case, it will be necessary to re-install the OS, so you should take care to avoid this problem.
- In some cases it may be necessary to update the product as the need arises in order to respond to the latest threats.

*The expression "maintenance and update contract" means the standard suppoer contract

For more detailed product info, please visit ▶ www.trendmicro.com Trial version available free of charge

TREND MICRO™ **Trend Micro Incorporated**
Securing Your Journey to the Cloud

Contact details:

www.trendmicro.com
TRENDMICRO, Trend Micro Portable Security, Portable Security, and Trend Micro Safe Lock are registered trademarks of Trend Micro Incorporated.
The names and products of each company are trademarks and/or registered trademarks of the respective companies.
The information contained in this document is accurate as of July, 2013. Content is subject to change without notice