Trellix Embedded Security

Trellix Whitelisting Technology

Features

- Low overhead because dynamic whitelisting eliminates manual effort
- Low impact on system performance
- Low CPU and memory requirements
- Low ownership costs result from no-need-to-manage as long as devices are operating well

Key feature 1: Application Control

- Protects against zero-day-attack
- Only authorized software is allowed to run
- Prevents all unauthorized applications from being executed
- Makes sure the machine does what it should do
- Automatically accepts new software added through authorized process

Key feature 2: Change Control

- Sets access rights for who or which application can access protected data
- Prevents outages resulting from unplanned changes

Key feature 3: ePolicy Orchestrator

- Fast time to remote deployment/configuration
- Reporting
- Central management
- Compliance requirements
- Monitors data of managed clients

Introduction

Trellix Embedded Security Solution is ideal for protecting systems that are fixed-function in terms of CPU or memory resources. Its low overhead does not impact system performance, requires very low initial and ongoing operational overhead, and is equally effective in standalone mode without network access. We provide four different combinations to satisfy different embedded industry needs.

Package 1: Trellix Application Control without ePO

Trellix Application Control, protects your system by only allowing authorized code to run. It automatically creates a dynamic whitelist of the “authorized code” on the embedded system. Once the whitelist is created and enabled, the system is locked down to the known good baseline; no program or code outside the authorized set can run.

Package 2: Trellix Application Control with ePO

With all the functions of Package 1(without ePO), Trellix Application Control with ePolicy Orchestrator centrally manages all Trellix products through remote deployment, remote configuration and report generation. It effectively saves management costs for users who have more than one device with installed Trellix.

Package 3: Trellix Embedded Control

Trellix Embedded Control combines the functions of application control and change control (i.e., it includes all the functions of package 1 (without ePO), plus the function of change control). With a dynamic whitelist of “authorized code”, the system is locked down to the known good baseline; no program or code outside the authorized set can run, and no unauthorized changes can be made. It blocks unauthorized changes to critical system files, directories, and configurations. It allows you to enforce change-control processes by specifying the authorized means of making changes. You may control who can apply changes, which certificates are required to allow changes, what may be changed (for example, you can restrict changes to certain files or directories), and when changes may be applied (for example, update windows might only be opened during a certain time in the week).

Package 4: Trellix Integrity Control

Trellix Integrity Control combines application control, change control plus ePolicy Orchestrator (i.e. with all the functions of Package 3, and adds in the function of ePolicy Orchestrator). Trellix Integrity Security unifies the management of endpoints, networks, data, and compliance for all the Trellix products. More than remote deployment, remote configuration, and reports generated, Trellix Integrity Control monitors who read and changed protected data, and when, while streamlining the implementation of compliance measures. It effectively saves management costs for users who have more than one device with Trellix installed.

Feature details

1. Low Overhead

Trellix Embedded Security Solution is a low-overhead software solution.

- Easy setup and low initial and ongoing operational overhead
- Minimal impact on CPU cycles, and uses less than 10 MB of RAM
- No file system scanning that could impact system performance
- Designed to work in connected and in offline modes
- Requires no signature updates

2. Application Control

Application Control helps provide protection against any existing and unknown, zero-day polymorphic threats via malware such as worms, viruses, Trojans, buffer-overflow threats, etc., thereby ensuring that the operating device is secure and cannot be compromised. It also helps eliminate emergency patching, reduces number and frequency of patching cycles, and enables more time for testing before patching. It also reduces any security risk on difficult-to-patch devices that are remote and distributed in areas with little or no local support. The Application Control feature helps reduce costs of operations by reducing both planned patching and unplanned recovery downtime, thereby increasing device availability. This turns out to be an ideal solution, especially for lower end devices as it reduces the support costs by reducing number of touch points needed.

3. Change Control

Change Control allows you to prevent reading/changes to the file system registry. You can view details of who made changes, which files were changed, and when and how the changes were made. You can write-protect critical files and registry keys from unauthorized tampering. You can read-protect sensitive files. To ease maintenance, you can define trusted programs or users to allow updates to protected files and registry keys.

Real-time visibility for changes made across all systems is the foundation of the Change Control product framework. It provides real-time change tracking with minimal consumption of CPU, memory, disk, and network resources. It comprehensively logs all change attempts made to files and Windows registry keys on the target systems.

4. ePolicy Orchestrator

ePolicy Orchestrator is a complete management software for Trellix products. It helps Trellix Application Control do central management by remote deployment/configuration and reporting.

In Trellix Integrity Control, with ePolicy Orchestrator, file content changes can be viewed and compared side-by-side to see what was added, deleted, or modified. This is handy while troubleshooting configuration-related outages. ePolicy Orchestrator in Trellix Integrity Control may also be utilized to ensure that the control requirements are met for PCI, FDA, HIPAA, and other regulatory mandates. It provides the necessary tamperproof audit logs on the device to prove that regulatory controls are in place.

Specifications

Supported OSs

- **Windows**

Client: Windows 11 pro, windows 11 enterprise, Windows 11 IoT enterprise, windows 10 pro, windows 10 enterprise, Windows 10 IoT enterprise, Windows Embedded 8.1 Industry (Pro and Enterprise), windows 8.1 Tablet, windows 7, windows 7 embedded

Server: Windows Server IoT 2022, Windows Server IoT 2019, Windows Server IoT 2016, windows server 2022, windows server 2019, windows server 2016, windows server 2012, windows server 2008R2

- **Linux**

RHEL 6, 7, 8, 9
CentOS 6,7,8
OL 6, 7, 8
SLES 11, 12, 15
Ubuntu 14, 16, 18, 20, 22

Minimum Requirements

Trellix Application Control without ePO, Trellix Embedded control

Operating System	Recommended Hardware
Windows (64-bit)	▪ Processor supporting x86-64/AMD64 architecture ▪ 2 GB RAM ▪ 100 MB free disk space for installation on system volume ▪ 100 MB free disk space on every volume that is solidified ▪ TCP/IP protocol installed on the system
Windows (32-bit)	▪ Processor supporting x86-64/AMD64 architecture ▪ 1 GB RAM ▪ 100 MB free disk space for installation on system volume ▪ 100 MB free disk space on every volume that is solidified ▪ TCP/IP protocol installed on the system
Linux	▪ Single/Multiple AMD/Intel Pentium CPU ▪ 512 MB RAM ▪ 80 MB free disk space for installation on system volume ▪ Write permission on partition where Solidifier is installed

Trellix ePolicy Orchestrator
System requirements and recommendations

Component	Requirements and recommendations
Dedicated server	If managing fewer than 250 systems, Trellix ePO - On-prem can be installed on a pre-existing server, such as a file server. If managing more than 250 systems, use a dedicated server for Trellix ePO - On-prem.
Domain controllers	(Recommended) The server must have a trust relationship with the Domain Controller on the network. For instructions, see the Microsoft product documentation. NOTE: Installing the software on a Domain Controller is supported, but not recommended.
File system	NT file system (NTFS) partition.
Free disk space	20 GB — Minimum.
IP address	Use static IP addresses for Trellix ePO - On-prem.Static IP addresses are recommended for Trellix ePO - On-prem and Agent Handlers. Trellix ePO - On-prem supports IPv4 and IPv6 networks.
Memory	8-GB available RAM minimum.
Network Interface Card (NIC)	100 megabit minimum. TIP: If Using A Server With More Than One IP Address, Trellix EPO - On-Prem Uses The First Identified IP Address. To Use More IP Addresses For Agent-Server Communication, Create Agent Handler Groups For Each IP Address. For More Information, See KB56281.
Ports	▪ Make sure that the ports you choose are not already in use on the server system. ▪ Notify network staff of the ports you intend to use for Trellix ePO - On-prem and Trellix Agent communication.
Processor	▪ 64-bit Intel compatible ▪ (Recommended) 4 cores minimum

Other

For Package 1: Trellix Application Control without ePO, and Package 2: Trellix Embedded Control, Advantech provides a user interface tool “Trellix whitelisting Manager”, which allows users to do basic operations without using the command line.

Ordering information

For Asia Pacific Region (For Client OS)

Advantech PN	Description
968ELTAC01	Trellix Application Control w/o ePO
968ELTAP01	Trellix Application Control with ePO
968ELTEC01	Trellix Embedded Control
968ELTIC01	Trellix Integrity Control

For Asia Pacific Region (For Server OS)

Advantech PN	Description
968ELTACS1	Trellix Application Control without ePO for Serve
968ELTAPS1	Trellix Application Control with ePO for Server
968ELTECS1	Trellix Embedded Control for Server
968ELTICS1	Trellix Integraty Control for Server

For Japan, America, Europe and other regions (For Client OS)

Advantech PN	Description
968ETQTAC1	Trellix Application Control w/o ePO (Bundle)
968ETQTAP1	Trellix Application Control w/ePO (Bundle)
968ETQTEC1	Trellix Embedded Control (Bundle)
968ETQTIC1	Trellix Integrity Control (Bundle)

For Japan, America, Europe and other regions (For Server OS)

Advantech PN	Description
968ETQTACS	Trellix Application Control w/o ePO for Server (Bundle)
968ETQTAPS	Trellix Application Control with ePO for Server (Bundle)
968ETQTECS	Trellix Embedded Control for Server (Bundle)
968ETQTICS	Trellix Integraty Control for Server (Bundle)