DATASHEET

Trellix Application and Change Control

Comprehensive protection against uninvited changes to or unauthorized control of applications, endpoints, servers, and fixed function devices

Advanced persistent threats (APTs) via remote attack or social engineering make it increasingly difficult to protect a business and can lead to security breaches, data loss, and outages. Particularly in today's continuously evolving server and cloud environments, nefarious changes can easily go undetected. Those who have zero tolerance for advanced persistent threats should take a closer look at Trellix Application and Change Control software.

Trellix Application Control helps IT outsmart cybercriminals and keeps business secure and productive. Using a dynamic trust model, local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this Trellix solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates.

Trellix Change Control software blocks unauthorized changes to critical system files, directories, and configurations while streamlining the implementation of new policies and compliance measures. Featuring file integrity monitoring and change prevention, Trellix Change Control enforces change policies and provides continuous monitoring of critical systems. It also detects and blocks unwanted changes made across distributed and remote locations. Its intuitive search interface helps users quickly home in on change event information.

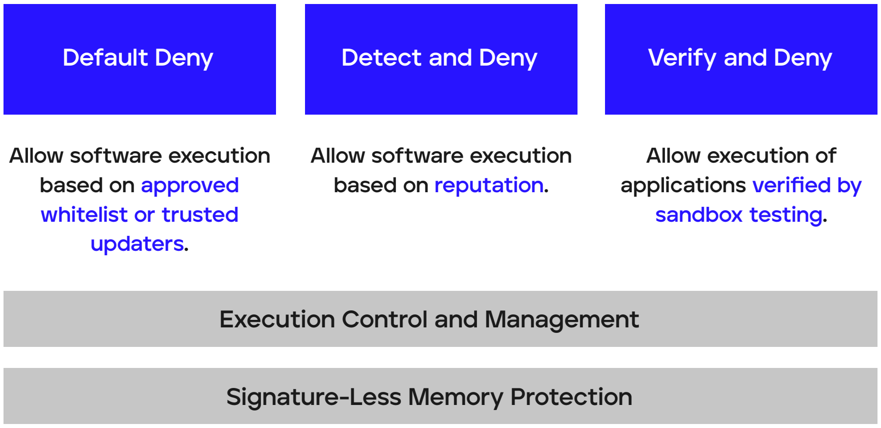
Combined, Trellix Application and Change Control ensures system integrity by only allowing authorized access to devices, blocking unauthorized executables, and taking a systematic approach to monitoring and preventing changes to the file system, registry, and user accounts. This helps ensure continuous, efficient, enterprise-wide detection and protection.

Intelligent Whitelisting

Prevent zero-day and APT attacks by blocking execution of unauthorized applications and allowing only known-good whitelisted applications to run. Trellix Application and Change Control groups binaries (.EXEs, DLLs, drivers, and scripts) across the enterprise by application and vendor, displays them in an intuitive, hierarchical format, and intelligently classifies them as well-known, unknown, and known-bad applications.

Implement the Right Security Posture

To allow greater application flexibility in the social and cloud-enabled business world, Trellix Application and Change Control gives organizations three options to maximize their whitelisting strategy for threat prevention:



Default Deny

Allow software execution based on approved whitelist or trusted updaters.

Detect and Deny

Allow software execution based on reputation.

Verify and Deny

Allow execution of applications verified by sandbox testing.

Execution Control and Management

Signature-Less Memory Protection

Figure 1: Three ways to maximize a whitelist strategy.

Key Advantages

- Take advantage of Trellix Global Threat Intelligence and Trellix Threat Intelligence Exchange to provide global and local reputation of files and applications.
- Strengthen security and lower ownership costs with dynamic whitelisting that automatically accepts new software added through trusted channels.
- Enforce controls on connected or disconnected servers, virtual machines, endpoints, fixed devices such as point-of-sale terminals, and legacy systems.
- Allow new applications based on application rating or self-approval for improved business continuity.
- Provide continuous visibility and real-time management of changes to critical system, configuration, or content files.

Complete and Fast Response

Whitelisting is enhanced with Trellix Global Threat Intelligence, an exclusive Trellix technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. Trellix Application Control uses this knowledge to determine the reputation of files in a computing environment, classifying them as good, bad, or unknown.

When deployed with Trellix Threat Intelligence Exchange, an optional module sold separately, Trellix Application and Change Control updates the whitelist based on local reputation intelligence to combat threats instantly. It also uses Trellix Threat Intelligence Exchange to coordinate with Trellix Intelligent Sandbox to dynamically analyze the behavior of unknown applications in a sandbox and automatically immunizes endpoints from newly detected malware.

Key Advantages

- Prevent tampering with critical files and registry keys by unauthorized parties.
- Enable tight policy enforcement via proactively blocking of out-of-process and unwanted changes before they occur.

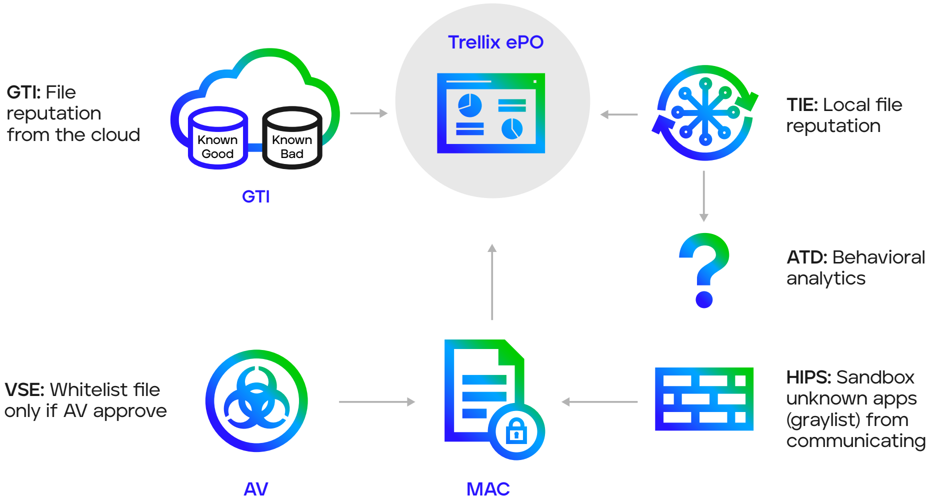

GTI: File reputation from the cloud
Known Good
Known Bad
GTI
Trellix ePO
TIE: Local file reputation
ATD: Behavioral analytics
VSE: Whitelist file only if AV approve
AV
MAC
HIPS: Sandbox unknown apps (graylist) from communicating

Figure 2: Trellix Global Threat Intelligence and Trellix Threat Intelligence Exchange provide global and local reputation for Trellix Application Control.

Powerful, Built-In Suggestions

Inventory search and pre-defined reports help users easily manage vulnerability, compliance, and security issues in application-related files and environments. It helps discover useful insights, such as recently added applications, uncertified binaries, files with unknown reputations, and systems running outdated software versions.

New in Trellix Application and Change Control 8.3, Inventory Mode continuously maintains up-to-date inventories of each system/device. This reduces CPU and system/device resource utilization while maintaining SWAM/CPE and PCI-DSS compliance. Inventory Mode allows users to track changes to files and binaries on the endpoint over time. Common Platform Enumeration (CPE) optionally matches NIST CPE data to gathered inventories for use in whitelist creation and compliance reporting.

No Impact on Business Continuity

To avoid interference with business continuity, new applications are automatically allowed based on application reputation. For unknown applications, a suggestions interface recommends new update policies based on execution patterns at endpoints. This is an excellent way to manage exceptions generated by blocked applications. After inspecting exceptions and details of the blocked application, simply approve and whitelist the file or ignore it to block the application.

Help Users Become Part of the Solution

For unknown applications, Trellix Application and Change Control explains to users why access to unauthorized applications is not allowed and allows users to take steps to approve the application through self-approvals or approval requests.

Keep Systems Up to Date

Keeping systems current with the latest patch is important. Trellix Application and Change Control's Dynamic Trust Model can automatically update systems without impacting business continuity. Keep systems up to date using trusted users, trusted local groups, certificates, processes, and directories. Trellix Application Control also prevents whitelisted applications from being exploited via memory buffer overflow attacks on Microsoft Windows systems.

Change Prevention and Integrity Monitoring

Often, there is the potential for configuration drift and there is no visibility into who performed the change, which can lead to security breaches, data loss, or outages. Trellix Application and Change Control can block or restrict any out-of-policy change attempts made to the system/device. If any changes are attempted, it will be logged and real time visibility to any change events can be provided. The system controller module manages communication between the system controller and the agents.

Supported Platforms

Trellix Application and Change Control:

- 8.3.x, 8.2.x, 8.1.x, 8.0.x, 7.0.x (Windows-based operating systems)
- 6.4.x, 6.3.x (Linux-based operating systems) 6.2.x, 6.1.x (Windowsbased and UNIX-based operating systems)
- Linux
- Microsoft Windows

Next-Level File Integrity Monitoring

Trellix Application and Change Control allows real-time File Integrity Monitoring (FIM) software implementation and PCI-DSS compliance validation in an efficient, cost-effective manner. Trellix Application and Change Control FIM provides the who, when, what, and why essentials, including user name, time of change, program name, and file/registry content data—all in one place and in real time. In addition, it can help identify root causes when troubleshooting in the event of an outage.

Track Content Changes

Trellix Change Control allows IT to track file content and attribute changes. File content changes can be viewed and compared side by side to see what was added, deleted, or modified. Configure include/exclude filters so only relevant, actionable changes are captured. System and device changes can also be restricted by users, local user groups, applications, certificates, and/or web services. System and device changes can even be restricted to specific times and dates (example: allow Windows updates to be applied only between 2 am to 4 am on Tuesdays). What's more, special alerting mechanisms instantly notify IT of critical changes to help prevent configuration-related outages—a recommended information technology infrastructure library (ITIL) best practice. Qualified security assessor (QSA) forms are provided for easy PCI reporting.

Prevent Outages Resulting from Unplanned Changes

Trellix Change Control allows IT to easily resolve incidents, automate regulatory compliance controls, and prevent change-related outages. Additionally, it helps eliminate the need for manual, error-prone, and resource-intensive compliance policies that are often associated with Sarbanes-Oxley (SOX) mandates. Trellix Application and Change Control enables users to build an automated IT control framework with all the information required to verify compliance is available in a single reporting system. Changes against authorizations can be validated automatically. Emergency fixes and other out-of-process changes are automatically documented and reconciled for easier audits.

Centralized Security and Compliance Management

Trellix ePolicy Orchestrator (Trellix ePO) platform consolidates and centralizes management, providing a global view of enterprise security. This award-winning platform integrates Trellix Application and Change Control with Trellix Host Intrusion Prevention, and other Trellix security products, including anti-malware for blacklisting. Single-step installation and update of Trellix Application and Change Control deployment can be done from Microsoft System Center as well. New profiles can be activated at any point in time to increase protection—from simple monitoring to bulletproof enforcement.

Next Steps

Confidently block or restrict unauthorized applications from executing in ways that put data at risk, and employ a systematic approach to monitoring and preventing changes to the file system, registry, and user accounts. Trellix Application and Change Control ensures system integrity by only allowing authorized access to devices and blocking unauthorized executables. New profiles can be activated at any point in time to increase protection—from simple monitoring to bulletproof enforcement.

Visit Trellix.com to learn more.