Trellix

DATASHEET

Trellix Change Control

Prevent unauthorized changes. Automate regulatory compliance controls.

Changes in server environments are constantly taking place in many organizations today—and going undetected. It's a situation that is dangerous, both in terms of security and compliance. Trellix Change Control—part of the Trellix product offering—delivers continuous, enterprise-wide detection of authorized changes as they occur. It blocks unauthorized changes to critical system files, directories, and configurations while streamlining the implementation of new policies and compliance measures.

Trellix Change Control software eliminates change activity—which is far too common in enterprises today. Change activity can lead to security breaches, data loss, and outages. Featuring file integrity monitoring, and change prevention, Trellix Change Control enforces change policies and provides continuous monitoring of critical systems. It also detects changes made across distributed and remote locations and blocks unwanted changes.

With its intuitive search interface, Trellix Change Control helps users quickly home in on change-event information. For example, you can query the interface for data on all changes that occurred in the c:\windows\system32 directory that were made on the server xyz. acme.com.

Key Features

- File integrity monitoring: Continuously tracks changes to file and registry keys and identifies who made changes to which files
- Change prevention: Protects critical files and registry keys from tampering, with changes only permitted in accordance with update policies

Small Footprint and Low Overhead

- Easy setup and low initial and ongoing operational overhead
- Negligible memory usage
- No file scanning that could impact system performance

Next-Level File Integrity Monitoring

Payment Card Industry Data Security Standard (PCI DSS) requirements 10 and 11.5 call for tracking and monitoring all access to network resources and cardholder data and deploying file integrity monitoring (FIM) tools to alert personnel to unauthorized modifications of critical system, configuration, or content files. Trellix Change Control enables you to implement real-time FIM software and validate PCI compliance in an efficient, cost-effective manner. Trellix Change Control FIM provides the who, when, what, and why essentials. It gives you the 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 you identify root causes when troubleshooting in the event of an outage.

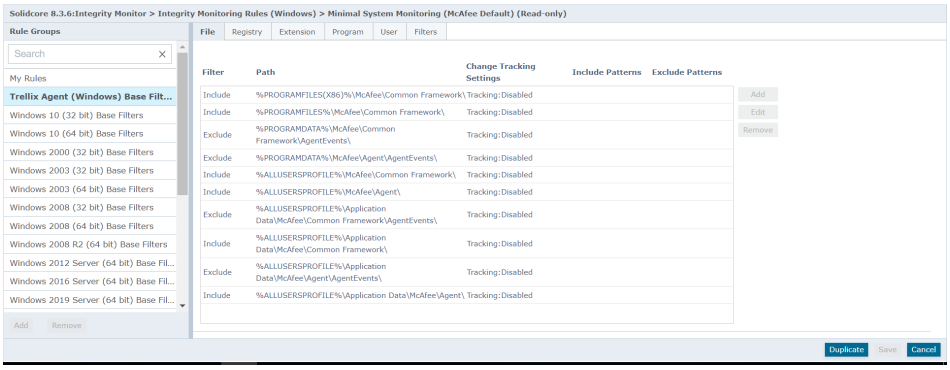

Figure 1: Trellix Change Control features out-of-the-box FIM rules and sophisticated filters for monitoring only relevant files.

Track Content Changes

Trellix Change Control allows you 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. This is handy while troubleshooting configuration-related outages.

Include/exclude filters can be configured so that only relevant, actionable changes are captured. What's more, special alerting mechanisms instantly notify you of critical changes, so you can prevent configuration-related outages—a recommended information technology infrastructure library (ITIL) best practice. Qualified security assessor (QSA) forms are provided for easy PCI reporting.

Key Advantages

- Provides continuous visibility and real-time management of changes to critical system, configuration, or content files
- Prevents tampering with critical files and registry keys by unauthorized parties
- Enables fulfillment of the PCI DSS regulation requirement for file integrity monitoring system
- Easy to get started with out-of-the box FIM rules
- QSA-friendly reports for easy PCI reporting
- One-click exclusion feature to avoid tracking irrelevant information
- Tight policy enforcement via proactively blocking of out-of process and unwanted changes before they occur
- Integrates with Trellix ePolicy Orchestrator (Trellix ePO) console for centralized IT management

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, Trellix Change Control eliminates the need for manual, error-prone, and resource-intensive compliance policies that are often associated with Sarbanes-Oxley (SOX) mandates. Trellix Change Control enables you to build an automated IT control framework in which 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 ePO platform software consolidates and centralizes management, providing a global view of enterprise security. It gives you the flexibility to adjust the types or scope of systems to cover and lets you determine which files, directories, and configurations should be included in change alerts, as well as the priority of alerts. Default profiles developed for most common types of server operating systems and enterprise applications are available to monitor for critical components without creating new ones from scratch. With Trellix Change Control and Trellix ePO software, new profiles can be activated at any point in time to increase protection—from simple monitoring to bullet-proof enforcement.

Trellix ePO is scalable and readily extensible. It integrates Trellix Change Control software and our other security management products with those of our partners.

Supported Platforms

Microsoft Windows (32-bit and 64-bit)

- Embedded: XPE, Pos Ready 2009, WES 2009
- Server: 2003, 2003 R2, 2008, 2008 R2, 2012 , 2012R2, 2016, 2019,2022
- Desktop: XP, Vista, 8, 10, 11

Linux

- RHEL 5, 6
- Suse 10, 11
- CentOS 5, 6
- OEL 5, 6
- SLED 11
- OpenSUSE 10/11

Enforcement Changes Everything

Trellix Change Control software tracks and validates every attempted change in real time on your server. It enforces change policies by requiring that changes be made within a time window, only by trusted sources, or with approved work tickets. The change prevention component of Trellix Change Control software can be fine-tuned to allow native applications to update their files continuously without interruption, while disallowing all other applications or users from making changes or even reading specified files.

Minimizing Risk and Maximizing Compliance on Multiple Fronts

We offer a wide array of risk and compliance solutions to help you minimize risk, automate compliance, and optimize security. In particular, Trellix Change Control and Trellix Application Control are a powerful combination for eliminating vulnerabilities and ensuring compliance throughout the enterprise.

Next Steps

Trellix Change Control software eliminates change activity in server environments that can lead to security breaches, data loss, and outages and makes it easy to meet regulatory compliance requirements. Prevent unauthorized changes while automating regulatory compliance controls with Trellix Change Control today.

Visit Trellix.com to learn more.