Trellix

DATASHEET

Trellix Embedded Control

Simple defense for the devices you rely on

Today's expanding attack surface is dominated by non-traditional endpoints that range from wearable fitness devices to critical connected sensors that control generation and distribution. As the number of connected devices grows, so do the risks from malware and attacks. Trellix Embedded Control ensures the integrity of your systems by only allowing authorized access to devices and blocking unauthorized executables.

Trellix Embedded Control focuses on solving the problem of increased security risk arising from the adoption of commercial operating systems in embedded systems. Trellix Embedded Control is a small-footprint, low-overhead, application-independent solution that provides "deploy-and-forget" security. Trellix Embedded Control converts a system built on a commercial operating system into a "black box" so it looks like a closed proprietary operating system. It prevents any unauthorized program that is on disk or injected into memory from executing and prevents unauthorized changes to an authorized baseline. This solution enables

manufacturers to enjoy the benefits of using a commercial operating system without incurring additional risk or losing control over how systems are used in the field.

Assured System Integrity

Executable control

With Trellix Embedded Control, only programs contained in the Trellix dynamic whitelist can execute. Other programs (exes, dlls, scripts) are considered unauthorized. Their execution is prevented, and the failure is logged by default. This prevents worms, viruses, spyware, and other malware that install themselves from executing illegitimately.

Memory control

Memory control ensures that running processes are protected from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted, and logged. This way, attempts to gain control of a system through buffer overflow, heap overflow, stack execution, and similar exploits are rendered ineffective and are logged.[1]

Trellix Global Threat Intelligence Integration: The Smart Way to Deal with Global Threats for Air-Gap Environments

Trellix Global Threat Intelligence (Trellix GTI) is an exclusive Trellix technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. This feature uses cloud-based knowledge to determine the reputation of all files in your computing environment, classifying them as good, bad, and unknown. With Trellix GTI integration, you'll know with certainty when any malware has been inadvertently whitelisted. The GTI reputation is accessible in internetconnected, as well as isolated Trellix ePolicy Orchestrator (Trellix ePO) platform software environments.

Change control

Trellix Embedded Control detects changes in real time. It provides visibility into the sources of change and verifies that changes were deployed on the correct target systems. It also provides an audit trail of changes and allows changes to be made only through authorized means.

Key Advantages

- Minimizes your security risk by controlling what runs on your embedded devices and protecting the memory in those devices
- Enables you to give access, retain control, and reduce support costs
- Selective enforcement
- Deploy and forget
- Allows you to make your devices compliance and audit ready
- Real-time visibility
- Comprehensive audit
- Searchable change archive
- Closed-loop reconciliation

1. Only available on Microsoft Windows platforms.

Trellix Embedded Control 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 may restrict changes to certain files or directories), and when changes may be applied (for example, update Microsoft Windows may only be opened during certain times of the week).

Proactive change verifies each change before it is applied on target systems. With this module enabled, updates to software systems may only be made in a controlled manner.

The real-time change tracking module logs all changes to system state, including code, configuration, and the registry. Change events are logged as they occur, in real time, and sent to the system controller for aggregation and archival purposes.

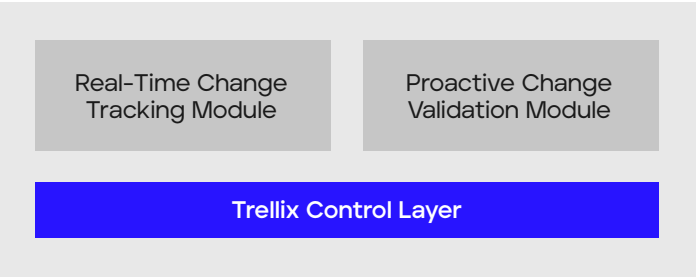

Figure 1: The Trellix control layer.

The system controller module manages communication between the system controller and the agents. It aggregates and stores change event information from the agents in the independent system of record.

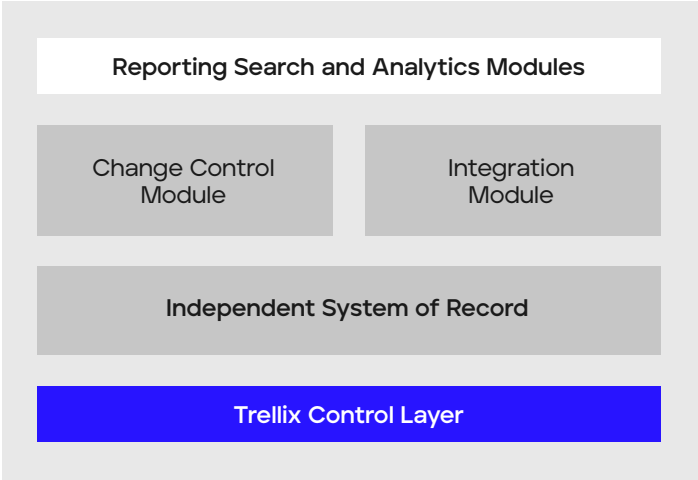

Figure 2: Reporting, search, and analytics modules.

Audit and Policy Compliance

Trellix Integrity Control provides dashboards and reports that help you meet compliance requirements. These are generated through the Trellix ePO console, which provides a web-based user interface (UI) for users and administrators.

Trellix Embedded Control delivers integrated, closed-loop, real-time compliance and audit, complete with a tamperproof system of record for the authorized activity and unauthorized attempts.

About Trellix Embedded Security

Trellix Embedded Security solutions help manufacturers ensure that their products and devices are protected from cyberthreats and attacks. Trellix solutions span a wide range of technologies, including application whitelisting, antivirus and anti-malware protection, device management, encryption, and risk and compliance—and all leverage the industry-leading Trellix Global Threat Intelligence. Our solutions can be tailored to meet the specific design requirements for a manufacturer's device and its architectures.

Feature	Description	Benefit
Guaranteed System Integrity		
External threat defense	Ensures that only authorized code can run. Unauthorized code cannot be injected into memory. Authorized code cannot be tampered with.	▪ Eliminates emergency patching, reduces the number and frequency of patching cycles, enables more testing before patching, reduces security risk for difficult-to-patch systems ▪ Reduces security risk from zero-day, polymorphic attacks via malware, such as worms, viruses, and Trojans, and code injections, like buffer overflow, heap overflow, and stack overflow ▪ Maintains integrity of authorized files, ensuring the system in production is in a known and verified state ▪ Reduces the cost of operations by limiting unplanned patching and recovery downtime and improves system availability
Internal threat defense	Local administrator lockdown offers the flexibility to disable even administrators from changing what is authorized to run on a protected system, unless presented by an authentic key.	▪ Protects against internal threat ▪ Locks down what runs on embedded systems in production and prevents change even by administrators
Advanced Change Control		
Secure authorized updates by manufacturer	Ensures that only authorized updates can be implemented on in-field embedded systems	▪ Ensures that no out-of-band changes can be deployed on systems in the field. Prevents unauthorized system changes before they result in downtime and generate support calls. ▪ Manufacturers can choose to retain control over all changes themselves, or authorize only trusted customer agents to control changes
Verify changes that occurred within approved window	Ensures that changes were not deployed outside of authorized change windows	▪ Prevent unauthorized change during fiscally sensitive time windows or during peak business hours to avoid operational disruption and/or compliance violations.
Authorized updaters	Ensures that only authorized updaters (people or processes) can implement changes on production systems	▪ Ensures that no out-of-band changes can be deployed on production systems.
Real-Time, Closed Loop, Audit and Compliance		
Real-time change tracking	Tracks changes as soon as they happen across the enterprise	▪ Ensures that no out-of-band changes can be deployed on production systems
Comprehensive audit	Captures complete change information for every system change: who, what, where, when, and how	▪ Keeps an accurate, complete, and definitive record of all system changes
Identify sources of change	Links every change to its source: who made the change, the sequence of events that led to it, the process/program that affected it	▪ Validates approved changes, quickly identifies unapproved changes, and increases change success rate

Feature	Description	Benefit
Low Operational Overhead		
Deploy and forget	Installs in minutes, no initial configuration or setup necessary and no ongoing configuration necessary	▪ Works out of the box and is effective immediately after installation—no ongoing maintenance overhead, thereby a favorable choice for a low OPEX security solution configuration
Rules-free, signature-free, no learning period, application independent	Does not depend on rules or signature databases and is effective across all applications immediately with no learning period	▪ Needs very low attention from an administrator during server lifecycle ▪ Protects server until patched or unpatched server with low ongoing OPEX ▪ Effectiveness not dependent on quality of any rules or policies
Small footprint, low runtime overhead	Takes up less than 20 MB disk space and does not interfere with an application's runtime performance	▪ Ready to be deployed on any mission-critical production system without impacting its run-time performance or storage requirements
Guaranteed no false positives or false negatives	Logs only unauthorized activity	▪ Accuracy of results reduces OPEX as compared to other host intrusion prevention solutions by dramatically reducing the time needed to analyze logs daily/weekly ▪ Improves administrator efficiency, reduces OPEX

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.