

McAfee Integrity Control

Protect point of service systems from unauthorized applications and change



Key Advantages

Comprehensive change visibility and control

Track changes to critical files and directories continuously across fixed-function systems

Dynamic whitelisting lowers cost of ownership

Eliminate the manual effort of maintaining databases, rules, and updates on fixed-function systems

Enforce change policy

Ensure changes are made according to authorized policy and process

Operationally transparent

No additional operational overhead on fixed-function devices

McAfee® Integrity Control™ software combines industry-leading whitelisting and change control technology to ensure that only trusted applications run on fixed-function devices, such as point-of-service (POS) systems, automated teller machines (ATMs) and kiosks. McAfee Integrity Control software provides customers with continuous change detection capabilities while also offering the capability to proactively prevent unauthorized change attempts. McAfee Integrity Control software uses a trusted source model, so that even when systems are locked down, software updates from authorized sources are still allowed.

Block unauthorized applications and change attempts

McAfee Integrity Control software enables the IT organization to ensure that only approved software runs on the point-of-service infrastructure without imposing additional operational overhead. McAfee Integrity Control software easily blocks unauthorized, vulnerable, or malicious applications that can compromise the integrity of critical systems. The solution's dynamic whitelisting trust model keeps systems tightly secured yet allows for authorized updates or changes to be made from administrator-defined trusted sources. This eliminates the manual and costly support associated with other whitelisting technologies, as no databases, rules, or updates are needed.

The McAfee Integrity Control software also leverages change control technology that can block unwanted, out-of-policy changes before they occur. This level of protection is linked directly to policy, and changes can be verified against the change source, time window, or approved change ticket. Changes that are attempted outside of policy on enabled systems are blocked, and the change attempt is logged and sent as an alert to administrators. This greatly reduces change-related outages and compliance violations.

Monitor file integrity and changes

Through file integrity monitoring (FIM), McAfee Integrity Control software monitors files and directories for changes to content, permissions, or both. McAfee Integrity Control software provides continuous FIM, which is essential for testing and verifying the security of an environment or meeting critical compliance requirements such as those outlined in the Payment Card Industry Data Security Standard (PCI DSS). McAfee Integrity Control software provides comprehensive information about every change, including the user and program used to make the change.

Centralized deployment and management through ePO

Seamless integration with McAfee® ePolicy Orchestrator® (McAfee ePO™) software eases McAfee Integrity Control agent deployment, management, and reporting. The single McAfee ePO console lowers the cost of ownership by consolidating fixed-function device security and compliance management. This saves IT organizations hardware, training, and operational costs, and provides unified control over the policies and protections on each enabled ATM, kiosk or POS system. Integration with the McAfee ePO platform eliminates the need to manage data in two separate systems.

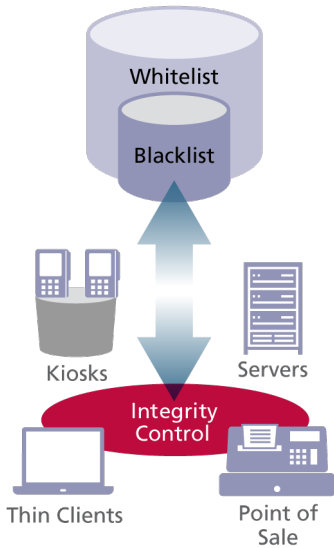


Figure 1. McAfee Integrity Control extends a layer of protection to fixed-function devices such as kiosks, POS terminals, and legacy platforms to reduce customer risk exponentially.

Deployment considerations

Increased control over fixed-function systems—In regulated industries such as retail, financial services, and healthcare, devices such as POS terminals, ATMs, and medical imaging systems perform critical functions and often store sensitive data. McAfee Integrity Control software is ideal for extending a layer of protection to systems that perform a fixed-function in terms of CPU or memory resources. The solution offers a low-overhead footprint that does not impact system performance and requires very low initial and ongoing operational overhead. It is equally effective in standalone mode without network access.

Meeting and sustaining PCI DSS compliance—Many point-of-service systems such as ATMs, POS terminals, and kiosks are in scope for meeting PCI DSS compliance. McAfee Integrity Control software provides continuous information about change events across the point-of-service infrastructure, which includes where the change was made (which server/servers), when it was made (time), which user made the change, how the change was made, what (content inside the file) changed, and whether the change was approved. This deep level of visibility into the point-of-service environment is delivered through the McAfee ePO platform and enables IT organizations to continuously verify the security of POS systems while validating PCI DSS compliance to auditors.

Improve service availability—Downtime on fixed-function devices is often caused by unauthorized or untested change, and most of the time taken to restore availability to these devices is spent discovering what changed. This is due to a gap between actual change activity and the documented change process. This change control gap results in manual activity by IT departments to control and minimize the high costs of change and change-related outages. McAfee Integrity Control software enables IT organizations to achieve higher service availability for fixed-functions devices by bridging this change control gap. McAfee Integrity Control software tracks changes continuously through the McAfee ePO platform and allows for the selective enforcement of change policies to prevent unknown changes from occurring before they cause a problem. McAfee Integrity Control software helps customers reduce the number of unavailability incidents (as measured by mean time between failures), as well as recovery time per incident (as measured by mean time to repair).

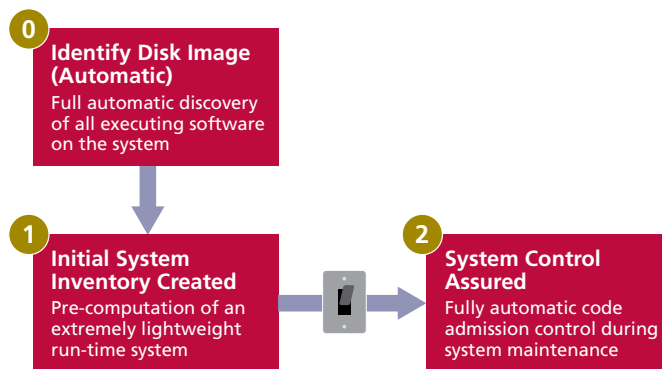


Figure 2: How dynamic whitelisting works.

