

McAfee Integrity Monitor

File integrity monitoring for compliance



Key Advantages

Comprehensive change visibility

Visibility of changes across distributed systems, such as point-of-sale terminals and data center infrastructures

Centralized deployment and management

Integration with ePO provides centralized reporting of monitored systems and change alerts for common IT infrastructures

File integrity monitoring for PCI compliance

PCI DSS file integrity monitoring solution for heterogeneous environments

File integrity monitoring (FIM) is the capability to monitor files and directories on a server for changes to content, permissions, or both. McAfee® Integrity Monitor provides continuous FIM that 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 Monitor provides comprehensive information about every change, including the user and program used to make the change.

When it comes to your IT infrastructure, strong compliance requires two key components: a trusted system state and the ability to verify and provide authorized changes that will not compromise corporate standards or compliance. The PCI DSS in particular highlights the need for safe change actions through PCI section 10.5.5 (“Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts”) and PCI section 11.5 (“Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files”).

Advantages of McAfee Integrity Monitor

- *Comprehensive change detection*—McAfee Integrity Monitor captures every single change to the file. Detecting all changes is important for sustaining compliance because it allows you to see where your compliance policies are being challenged and addresses inappropriate change at the source.
- *Rich forensic data capture*—McAfee Integrity Monitor captures details about every change, including the exact time of the change; who was logged into the machine at that time; what processes (such as editors) were running; whether the change was manual or made by an authorized program; and, if manual, which user made it. This information is critical for distinguishing between a safe change made to a trusted site and a violation. It also enables rapid investigation of change-related problems.
- *No operational trade-offs*—McAfee Integrity Monitor operates with very low overhead so the entire infrastructure can be monitored without impact.

Centralized deployment and management through ePO

Seamless integration with McAfee ePolicy Orchestrator® (ePO™) software eases McAfee Integrity Monitor agent deployment, management and reporting. The single McAfee ePO console lowers the cost of ownership by consolidating security and compliance management. This saves IT organizations training and operational costs, while providing unified control over the policies and protections on each enabled system. Integration with ePO eliminates the need to manage data in two separate systems.

Monitoring the Secure Environment

McAfee Integrity Monitor provides compliance and change alerts not only to servers, but also covers additional component coverage such as databases and network devices, offering a single view for change reporting and change alerts throughout the entire enterprise environment. Alternative components like virtual servers, IBM 4690 systems and AS400 servers not traditionally covered by other providers round out the broad set of platforms covered by Integrity Monitor.

- *Database monitoring*—Monitors three key areas:
 - » Activities (logons, logoffs, user/role creations, password changes, and more)
 - » Schema changes (CREATE/ALTER tables, indices, stored procedures, and more)
 - » Data changes (INSERT/UPDATE/DELETE of sensitive records)
- *Network configuration monitoring*—Provides alerts to configuration changes to some of the most commonly used networking components in the industry
- *AS400*—Offers continuous integrity monitoring for this well-respected enterprise platform, extending the existing value and ensuring compliance for this strong infrastructure
- *IBM4690*—Prevalent retail platform for point-of-sale (POS) systems now have a solution for file integrity monitoring, giving retailers more options for PCI compliance

Know What You Didn't Know Before

McAfee Integrity Monitor helps IT managers, directors and CIOs gain visibility and access reports that enable them to know what they did not know before. The capability to detect changes across distributed in-store systems or datacenter infrastructures gives IT the upper hand at identifying authorized changes versus unauthorized changes or possible malicious activities.

McAfee Integrity Monitor provides insight about actual activities and changes being made to the critical infrastructure, and it ensures that operational integrity has not been compromised.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

