McAfee

McAfee PCI Pro

McAfee PCI Pro provides a comprehensive file integrity monitoring (FIM), audit trail and network configuration audit solution designed to help merchants and service providers quickly, easily and cost-effectively meet the following requirements of v 1.2 of the Payment Card Industry Data Security Standard (PCI DSS).

Key Advantages

- Real-time change monitoring for server, databases, network devices and Active Directory servers
- Configuration Assessment for Servers and Network Devices
- Centralized data repository to securely store audit trails
- Prepackaged PCIaudit reports to prove compliance

File Integrity Monitoring (PCI DSS § 11.5 and 10.5.5)

PCI DSS sections 10 and 11 specify the use of file integrity monitoring, which is the capability to monitor changes to files and directories on a server. The changes can be to content, permissions or both. PCI DSS compliance specifies that changes to existing data in log files must be detected, whereas the addition of new data can be ignored (PCI DSS §10.5.5). For other files, such as critical configuration files, any change may be important (PCI DSS §11.5). When a change of interest occurs, the FIM solution needs to provide an alert.

These requirements have previously been difficult to satisfy because existing tools have merely provided "periodic" file integrity monitoring capabilities that would detect changes through resource-intensive system scans. McAfee PCI Pro has solved this problem with "continuous" file integrity monitoring (CFIM) technology that detects all changes in real-time with a very small performance overhead. McAfee PCI Pro gives IT and compliance professionals continuous file integrity monitoring with a minimal impact on system resources, eliminating the need to perform repeated scan after scan.

PCI Requirement	Endpoint Types	PCI Pro
File Integrity Monitoring § 11.5 and 10.5.5	Servers	✓
Network Configuration § 1.1.1, 1.1.4, 1.1.5, 1.1.6, 1.2.1, 1.2.2, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 2.1.1	Network Devices	✓
Configuration Assessment § 2.2,6.2, 8.5.9, 8.5.10, 8.5.11, 8.5.12, 8.5.13, 8.5.14, 8.5.15	Servers	✓
Access to cardholder data § 10.2.1, 10.2.3, 10.2.4, 10.2.5	Databases	✓
Actions by privileged users § 10.2.2, 10.2.7	Servers, Databases, Network Devices	✓
Username Tracking § 10.3.1	Servers, Databases, Network Devices	✓
Event Attributes § 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6	Servers, Databases, Network Devices	✓
Securing the Audit Trail § 10.5.1, 10.5.2, 10.5.3, 10.5.4	Servers, Databases, Network Devices	✓
Maintaining Audit Trail History § 10.7	Servers, Databases, Network Devices	✓

"McAfee PCI Pro gives us a quick and simple way to audit our critical systems and files, and allows me to quickly identify exceptions and violations on specific servers, or those across our entire IT environment."

Keith Spahn,
Systems Administrator,
Clerk of the Circuit Court,
Sarasota, Florida

Detecting all changes is important for sustaining compliance because it allows organizations to see where their compliance policies are being challenged and address inappropriate change at the source. Related to this, if a file is changed inappropriately and then changed back, it creates a transient compliance violation. The continuous FIM capabilities of McAfee PCI Pro captures every change and information about the user who made the change. Alerts can be configured to warn administrators even on the transient violations.

Default Filter Profiles (rule sets that specify which files are to be monitored) are provided for more than 50 operating systems and applications like AIX, HP-UX, CentOS/Redhat/SuSe Linux, Solaris, Windows, iSeries (AS400), Apache Webserver, IIS Webserver, Apache Tomcat server, IBM Websphere, JBoss, BEA WebLogic, Siebel, DB2, Oracle and SQL Server. These filter profiles have been validated by leading QSAs and have been used in successful PCI audits by our customers. An intuitive Web-interface also makes the customizations of these filter profiles an easy task.

Configuration Assessment (PCI DSS § 2.2, 6.2 and 8.5.x)

McAfee PCI Pro ships with PCI-DSS benchmarks as specified by the Center for Internet Security (CIS) to automate PCI DSS requirements 2.2, 6.2 and 8.5.x. These benchmarks allow administrators to automate their configuration assessments to an extent that was not possible before. Administrators can perform configuration assessments on-demand or on a scheduled basis.

The Benchmarks specify a pass/fail score for the rules that are part of the benchmark. At the end of the Configuration Assessment, Administrators will be able to see the benchmark compliance score of their servers and even drill down to the rules that passed/failed on a particular host.

The results of the Configuration Assessments are stored in the database and made available through Dashboards and Reports. Reports are available to summarize the results of Configuration Assessments and compare benchmark scores across multiple servers. Trends of Benchmark compliance scores are also available through the dashboards.

Audit Trails (PCI DSS § 10)

PCI DSS Section 10 lists the requirements of monitoring all access to network resources and cardholder data. Monitoring activity and changes on database servers is especially critical to pass the section 10 audit. McAfee PCI Pro not only tracks the schema and data changes, but also database login activity, changes to roles, users, and permissions.

The audit trail from servers, databases and network devices are managed and stored by McAfee PCI Pro in a central database. The database can be secured to prevent highly privileged users, including powerful application database administrators, from accessing sensitive applications and data outside their authorized responsibilities.

Network Configuration Management (PCI DSS § 1)

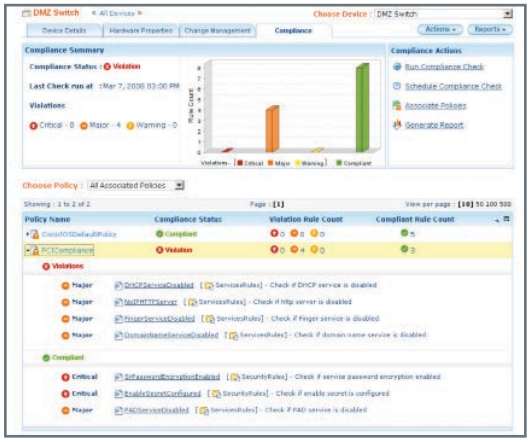
PCI DSS section 1 states that network devices, like routers and firewalls that transmit cardholder data, must be protected from man-in-the-middle attacks and data breaches. The network is only as strong as its weakest link, and even one poorly configured network device could put the business at risk. McAfee PCI Pro allows organizations to establish configuration standards for network devices and provides the capability to monitor the compliance of the devices in real-time. All configuration changes are tracked and versioned to meet the PCI DSS section 10 requirements for audit trails. Policies can also be set to rollback to a "Trusted Device Configuration" when any unauthorized configuration change is detected.

McAfee®

"McAfee's new offerings provide a means for PCI-challenged organizations of all sizes to rapidly attain difficult-to-achieve maturity in more PCI requirements, and at an affordable combination of cost and essential features that meet multiple requirements for a broad range of businesses."

Scott Crawford,
Security Research Director
EMA

Startup-Running conflict graph identifies devices that violate PCI DSS 1.3.6 guidelines to secure and synchronize router configuration files.



Dashboards and reports can be used to identify unauthorized changes and improve policy compliance. Supported Platforms: McAfee PCI Pro supports integration with more than 300 network devices, including those from device vendors such as Cisco, HP, Nortel, Force10, D-Link, Juniper-NetScreen, 3Com, Foundry, Fortinet, ADTRAN, Enterasys, Huawei, Extreme, Proxim, Aruba and Blue Coat.

Summary

McAfee PCI Pro provides immediate, cost-effective PCI compliance for many PCI DSS requirements outlined in sections 1, 10 and 11 (network device configuration, audit trail and file integrity monitoring). Sold via an annual subscription that minimizes first year costs, McAfee PCI Pro provides a solution that is both affordable and expandable. PCI Pro is upgradeable to McAfee's Change Control, which allows organizations investing in compliance solutions to easily expand to meet broader PCI requirements with IT benefits that include higher IT service availability, Sarbanes-Oxley compliance and streamlined Information Technology Infrastructure Library (ITIL) processes.

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. www.mcafee.com.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

6616ds_pci-pro_0709_ETMG