

McAfee Policy Auditor McAfee Remediation Manager

Reduce risk by remediating non-compliant and vulnerable systems

Compliance—with industry regulations and internal policies—mandates speedy correction of policy violations. IT operations demand rapid remediation of systems that are vulnerable to attack. But the time between the discovery of a vulnerability and its exploit can be just a few days. You need an automated way to quickly remediate vulnerabilities and enforce policy.

KEY ADVANTAGES

Demonstrate compliance

- **Consistently report compliance with IT controls for industry regulations and internal policies**

Increase operational efficiency

- **Automate the manual process of collecting policy data and remediating vulnerabilities and policy violations**

Enforce compliance

- **Automatically remediate non-compliant systems according to your policy**

Reinforce confidence

- **Reduce risk by ensuring that critical business assets are free of vulnerabilities, service misconfigurations, and policy violations**

Protect investments

- **Leverage existing third-party products and build onto the McAfee approach to security risk management**

McAfee® Policy Auditor and McAfee Remediation Manager enable organizations to proactively define, measure, report, and remediate on the compliance of information systems based on industry, regulatory, and corporate security policies, standards, and frameworks. As key components of McAfee's approach to security risk management, Policy Auditor and Remediation Manager help you minimize risk and business disruptions as well as maximize your IT resources and security software investments.

McAfee Policy Auditor finds and reports agent-based vulnerabilities, service misconfigurations, and policy violations. By mapping IT controls against pre-defined policy content, Policy Auditor automates the manual audit process and enables organizations to produce consistent and accurate reporting against internal and external policies.

McAfee Remediation Manager enforces compliance and automates vulnerability remediation to minimize risk to your business. Remediation Manager collects vulnerability scan data and policy violation information from Policy Auditor and third-party assessment tools. It correlates this data with its extensive remedy library to automate remediation for the five classes of vulnerabilities: misconfigurations, software defects, unnecessary services, backdoors, and unsecured accounts.

Find Vulnerabilities and Policy Violations

Perform host-based assessment of technical controls, patch status, and configuration settings of Windows®, Solaris, Redhat, HP/UX, AIX, Tru64, and Mac OS-X platforms.

Evaluate What Actions to Take

Execute a prioritized response to complex and evolving threats based upon criticality, business units, high-risk assets, and custom prioritization queries. This ensures resources are deployed appropriately to critical areas.

Enforce Policy

Send prioritized action data to Remediation Manager to enforce compliance in accordance with your security policies. Integration with McAfee Network Access Control ensures that quarantined devices are remediated quickly, ensuring the fastest path to productivity.

Fix Problems

Deliver continuous, up-to-date remediation actions. With more than 28,000 tested remedies, our McAfee Avert® Labs security experts constantly monitor and compile data on security vulnerabilities and exploits to ensure quick remediation.

SYSTEM REQUIREMENTS

Operating systems

- Windows Server 2003 Standard Edition, SP1
- Windows Server 2003 Enterprise Edition, SP1

Processor

- Pentium compatible, 3GHz or above

Network

- Network interface: 100 Mb/s

Memory

- Number of devices/Server memory requirements:
 - o 2,000/1 GB
 - o 4,000/1.5 GB
 - o 6,000/2 GB

Free disk space

- Policy Auditor Server: 2.8 GB for server installation; allow an additional 10 MB per device
- Policy Auditor Download Server: 2.8 GB plus 20 GB for file downloads

Graphics

- 1024x768 resolution

Software

- Microsoft® SQL Server 2005 with Reporting Services
- Microsoft.NET Framework v1.1, SP2
- Microsoft ASP.NET
- Microsoft Internet Information Server (IIS)

Automated Policy Auditing

- **Identify** managed assets (workstations and servers with Policy Auditor agent) on your network
- **Create** inventory systems and software and services running on these systems
- **Audit** policies on these systems as defined by your organization or regulatory body

Automate Vulnerability Remediation

- **Detect** vulnerabilities based on industry-leading scanners, internal and external policies, and inventories of hardware and software configurations
- **Remove** vulnerabilities with an automated process using an extensive library of tested remedies for all classes of vulnerabilities
- **Report** vulnerabilities with enterprise-class and user-defined roll-up reporting

Regulatory Compliance Toolkit

- Delivers more than 40 predefined templates and examples of IT controls for the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), NSA, SANS Top 20, and other common regulatory guidelines
- Provides a policy engine that enables administrators to write custom checks to audit against their corporate security policy

Dashboard

- Policy Auditor delivers a visual, easy-to-interpret representation of current policy compliance, status of vulnerabilities, threat exposure, and overall risk levels
- Remediation Manager enables you to view executive-level snapshots of activity to monitor the status of remediations, device actions, and discovery, as well as manage and monitor operations

Seamless Integration

- Policy Auditor sends prioritized data to Remediation Manager, for automated remediation of non-compliant and vulnerable systems
- Policy Auditor and Remediation Manager work in concert with McAfee ePolicy Orchestrator® for simplified deployment and management of the Policy Auditor and Remediation Management agent across network endpoints—and eliminates the need to manage asset data in two systems
- Remediation Manager receives scan data from McAfee Foundstone® to remediate network-based vulnerabilities
- Remediation Manager works with McAfee Network Access Control to enforce policy by remediating vulnerable or non-compliant systems that are in violation of policy

McAfee Solution Services

Along with our McAfee SecurityAlliance™ partners, McAfee offers a wide variety of services to help you assess, plan, deploy, tune, and manage your security.

Technical Support

Make sure everything runs smoothly during and after installation with flexible programs from McAfee Technical Support. Our highly skilled and certified security specialists have a wealth of knowledge and resources to meet your security needs.

Learn More

Visit www.mcafee.com, or call us at 888.847.8766, 24 hours a day, seven days a week.