Total Protection for Compliance: Unified IT Policy Auditing

McAfee Total Protection for Compliance

Key Advantages

Integrated Agent and Agentless Solution (ePO)
Industry leading ability to effectively measure compliance across managed and unmanaged systems

Actionable Intelligence
Enables customers to find policy violations and vulnerabilities, and prioritize based on business risks

Open Standards
Content defined by authoritative committee, leveraged by US Federal government and open to inspection

Tailored Scoring and Risk Aware Measure Countermeasure
Prioritize remediation activity and accurately report on compliance violations

Continuous Audit Model
Ensures that data is always current for both internal and external audits

Issues and Waiver Management
Role Based Access Control (RBAC) workflow and waiver management aligned to operational processes

Remediation and Policy Enforcement
Leverage Remediation Manager to automate remediation and MNAC to enforce compliance

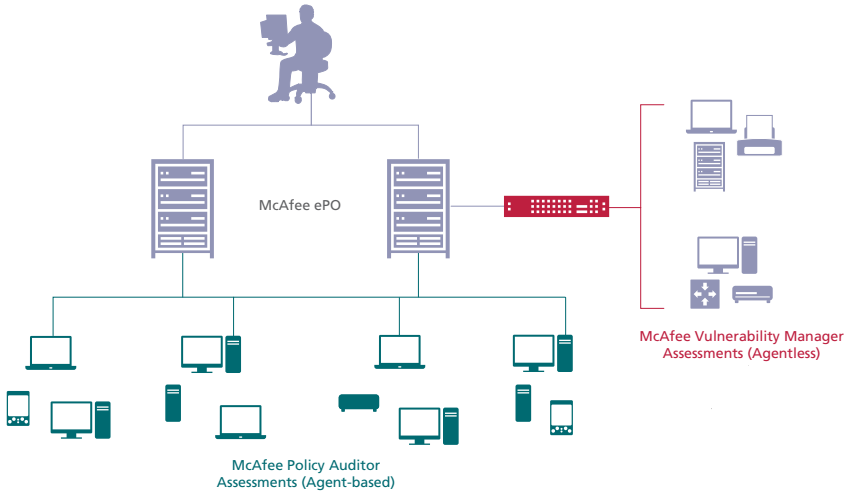
Regulations and standards are growing in number, and IT audits are increasing in complexity and cost. Until today, keeping pace with new requirements, more controls, and changing guidelines has meant deploying multiple technologies for managing IT audit cycles and sustaining compliance.

McAfee sets a new standard for true integration and automation by offering the best of both worlds: an approach combining agentless and agent-based policy auditing. McAfee® Total Protection for Compliance combines the power of McAfee Vulnerability Manager and McAfee Policy Auditor, and integrates them with McAfee® ePolicy Orchestrator (McAfee ePO™) to create a single platform for deployment, management, risk analysis, and compliance reporting.

McAfee Total Protection for Compliance solution:

- Simplifies compliance coverage through unified IT policy auditing
- Delivers the most effective technology approach by supporting both agent and agentless scans
- Automates time-consuming audit tasks by consolidating network and host-based assessments
- Enhances and optimizes existing investments in security management infrastructure
- Increases the value of security protection through McAfee's advanced countermeasure aware risk management technology
- Reduces audit preparation time by supporting automated industry standards content

McAfee Total Protection for Compliance Solution



Architecture Can Limit Compliance Coverage

A majority of regulations and standards call for ensuring security configurations that adhere to best practices and benchmarks across host platforms, along with regular scans for internal and external vulnerabilities. As a result, many organizations have implemented some form of automated controls assessment to define and measure compliance against security policy.

Automated assessments are achieved by using either agent-based or agentless solutions. Agent-based solutions must be deployed with a software agent that physically resides on the managed endpoint (server, desktop, network device, and so on). Agent-based solutions provide in-depth sets of policy assessments regardless of network availability, but they are limited to systems where the agents can be installed. Device types such as routers, switches, printers, and firewalls will not accept agents and must be assessed differently.

Agentless solutions are easily and quickly deployed across the network and can scan devices where agents cannot be loaded. Agentless solutions assess more endpoints (not just managed hosts), but the network must be available for them to perform assessments. They cost less to install and maintain, but they perform a more shallow audit (for example, they are not able to access registry information) since there is no software on the endpoint.

A conflict arises as to which technology solution to use. Agent-based technology protects managed endpoints and provides in-depth policy assessments, whether or not the network is available, but it's limited to systems where they can be installed. Agentless technology, on the other hand, greatly reduces the load on the network and can scan all devices but performs a shallower audit and requires the network to be available. Each technology has its advantages, but neither one alone provides a complete audit coverage and compliance validation solution.

How do most enterprises deal with this conflict?

Many companies end up purchasing products from different vendors and stitching them together, resulting in policy audits based on inconsistent criteria and lacking a consolidated management and reporting structure.

The optimal solution efficiently crosses technology boundaries and automates audit activities, integrating them with each other and with other system and network security processes. With Total Protection for Compliance, McAfee now offers the comprehensive solution that solves these problems.

McAfee Total Protection for Compliance—Unified IT Policy Auditing

The McAfee Total Protection for Compliance solution seamlessly automates compliance activities through the industry's first integrated, agent-based and agentless solution for patch assessment, compliance reporting, and risk analysis. Vulnerability Manager and Policy Auditor can be deployed in conjunction with ePO as the single management and reporting platform.

"In order to further safeguard customer data, we chose an integrated approach from McAfee. The result is an optimized data protection infrastructure that has enhanced our overall customer security program. With McAfee, we have the right solutions in place and the right strategic direction for the future."

—Grant Bourzikas, Director of Information Security & Business Continuity, Scottrade, Inc.

McAfee also extends risk management through awareness of countermeasures which increases the value of security protection. Until now, administrators received threat advisory information without any context; they had to determine the threat impact on their particular environment. Now, McAfee correlates threat information with the unique vulnerabilities, asset values, and existing protection measures of each user. By adding more intelligence into protection, McAfee provides security personnel with a customized threat intelligence perspective on their particular environment.

Reduce noncompliance with a consolidated view

To eliminate coverage gaps that reduce compliance and impair security, McAfee makes it easy to protect both managed and unmanaged assets. McAfee believes the agent status of the asset—managed or unmanaged—is less relevant than its adherence to security and configuration best practices. To deliver an accurate compliance assessment, McAfee provides a single, consolidated view within ePO of both agent-based and agentless systems. This consolidated view simplifies compliance coverage by

eliminating standalone processes and integrating critical tools into a single management and reporting environment. The integrated solution improves operational efficiency across the widest range of devices and systems and also reduces the window of noncompliance, a window that can present opportunities for hackers and malware.

To understand how McAfee simplifies the audit process, imagine a solution where customers can target a group of assets with or without an agent, select a template, and conduct an audit. Policy Auditor will determine which assets can be scanned through the McAfee agent and which need to be assessed through Vulnerability Manager. Throughout the process, ePO provides a centralized environment for managing, deploying, and reporting on policies and baselines. This combined functionality and integration provides complete coverage of all assets within an audit, with or without an agent, and reduces time spent on auditing tasks.

It's easy to customize policies and checks to support business-specific concerns and adhere to industry standards. And every activity is managed from the single, central ePO console. Updates from McAfee® Labs keep policy guidance current and delivers the latest threat advisories.

Define Once and Assess Many—Consolidated and Automated Policy Definitions

Most companies need to comply with multiple regulations and policies, and most regulated organizations already have written policies. However, the challenge is to create automated policy templates in a sea of change and complexity. Audits have become more frequent and more taxing. Regulations are expanding within each industry, and guidance is becoming more complex.

McAfee offers a powerful solution for automated policy definition that eliminates the need to create, maintain, and execute multiple editions of the same policy assessment benchmark. Within ePO, security administrators can define and select a policy benchmark once and then have the assessment performed across many different asset types. For example, for Payment Card Industry (PCI) compliance, there is no need to create one PCI template for host systems where agents reside and another for network devices without agents.

Customize templates to meet your specific needs

McAfee includes packaged templates with detailed compliance assessments of IT controls for the major regulations, standards, and frameworks. These templates can be modified, giving flexibility to various industries. New benchmark policies can be imported directly from external sources, such as the National Institute of Standards and Technology (NIST)—greatly reducing the amount of time IT spends on compliance assessments.

Use Existing Infrastructures to Lower Expenses

As organizations are forced to purchase new products that require additional agents, infrastructures, and consoles, cost and complexity increase. Companies also suffer from "agent overload," where so much additional software is added to the host that it impacts performance and availability. Servers may also be configured to a locked-down state where they cannot accept any changes or added software. In these cases, adding more consoles, agents, and management infrastructure is detrimental or prohibited by policy.

Save time and money

A more efficient path is to use the management infrastructure already in place and extend it to other functions necessary for compliance tasks. This streamlined approach leverages existing agents for other tasks, such as policy auditing. Synergies can be created from common consoles, reporting structures, and administration when agentless assessments are integrated. The McAfee emphasis on this type of integration helps improve return on infrastructure investments.

For existing McAfee ePO customers, adding Policy Auditor is a smaller overhead burden than installing yet another agent-based auditing product. Vulnerability Manager can be deployed by ePO customers as well to extend their coverage with no added overhead on the systems and devices it audits. In addition, McAfee integration delivers advanced risk analysis by correlating threat intelligence with vulnerabilities, assets, and countermeasures.

Make protection more intelligent with McAfee

McAfee integration through ePO results in improved metrics and communications about where vulnerabilities exist and which systems need priority attention. Many security intelligence services only deliver generic information on threat advisories, but McAfee goes beyond to specify how existing efforts to protect assets mitigate risk.

Using McAfee's countermeasure aware risk management application, new threats and vulnerabilities are evaluated against the deployment of anti-virus, buffer overflow, and intrusion prevention solutions. Assets that have these countermeasures are at less risk and allow administrators to allocate remediation efforts toward areas of highest criticality.

For example, when assessing a threat event, McAfee's technology allows IT administrators to identify and focus on only the vulnerable systems and not those that have acceptable levels of protection. This provides immediate insight, saves critical time, and dramatically improves security. When IT is empowered by this information, it can often mean the difference between worrying about 30 systems instead of 3,000.

McAfee's countermeasure aware risk management technology displays both the "what" and "how" of systems at risk, factoring in existing security protection.

Measure compliance levels with built-in content

In many cases, companies need solutions that have built-in content for measuring their compliance levels against regulations and standards. For example, U.S. federal mandates from the Office of Management and Budget (OMB) stipulate that federal agencies must demonstrate compliance to the Federal Desktop Core Configuration (FDCC) standard for Windows XP and Windows Vista systems. Basic to the FDCC validation is the use of XCCDF/OVAL content (descriptive formats and languages that represent system information).

Both Policy Auditor and Vulnerability Manager support XCCDF benchmarks and OVAL content. Policy Auditor has been validated as an FDCC Scanner and Authenticated Configuration Scanner. Vulnerability Manager's assessment capabilities include content built by third parties that follow XCCDF, OVAL, and other open standards included in the Security Content Automation Protocol (SCAP).

Simplifying IT Controls Assessments—An Example

To understand how McAfee simplifies the audit process, we will look at an example that shows how the Total Protection for Compliance solution delivers unified IT policy auditing by automating and integrating controls assessment processes and technologies:

- **McAfee Policy Auditor** uses an agent-based approach for deep policy assessments on host systems, enabling automated snapshots of compliance posture and accurately documenting violations and waivers.
- **McAfee Vulnerability Manager** further extends compliance coverage by incorporating agentless policy auditing into analysis of policy settings for account, file, network, and system access, and reviews the state of critical systems and files.
- **McAfee ePO** delivers real-time information and application integration for network, desktop, and server security, and is the common infrastructure for many McAfee solutions. McAfee ePO brings together both agent and agentless policy assessments under a powerful, single security management and reporting foundation.

Performing a unified IT policy audit: a scenario

Imagine a large retailer that is facing a Payment Card Industry Data Security Standard (PCI DSS) audit and must ensure compliance with PCI DSS Requirement 2.2 for developing IT system configurations "consistent with industry-accepted system hardening standards." Prior to deploying McAfee solutions, security professionals dreaded upcoming audits because it meant weeks of preparation time with only a fraction of the total audit scope completed. Administrators had to gather most of the data manually, and the few automated IT controls assessments available were only on an individual system basis. They also had to manually consolidate the results.

With McAfee Total Protection for Compliance, this retailer is able to cut the audit time down to a matter of days, while ensuring 100 percent coverage across all critical IT infrastructure components. The combination of Policy Auditor, Vulnerability Manager, and ePO working together extends the range of compliance coverage while reducing the time spent on auditing tasks. McAfee Total Protection for Compliance delivers streamlined, unified auditing. Let's take a closer look at how this is accomplished in this scenario.

McAfee Total Protection for Compliance Benefits

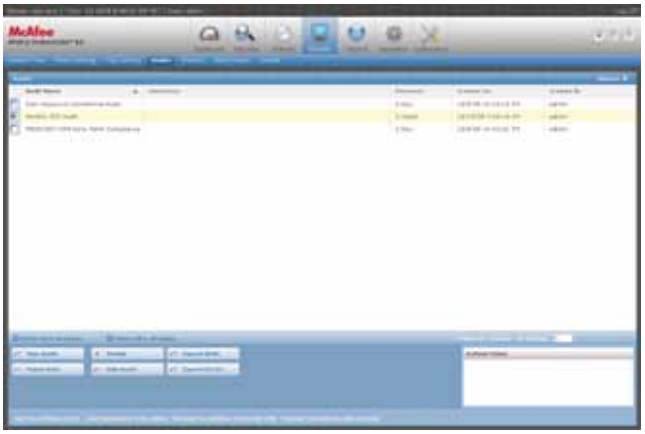
- Central Asset Repository
- Unified Policy Creation
- "Agent and Agentless" Assessments
- Single Management and Reporting Structure

Unified IT Policy Auditing in Action

Unified IT Policy Auditing—in Action

Step 1: Import all assets. With McAfee Total Protection for Compliance, this organization uses a central asset repository for information on all host systems and network devices where customer data resides or passes through. With its discovery scans, Vulnerability Manager supplies asset information on unmanaged systems. This information is synchronized on a scheduled basis with ePO, which centrally houses and manages the asset information. This eases the burden of determining which assets to assess at the time of an automated policy audit.

Step 2: Select the unified benchmark. From the ePO console, the security administrator selects the PCI DSS policy benchmark. Benchmarks contain the intelligence about which objects to assess and what properties to validate. They are created by McAfee and third-party authorities using frameworks and best practices matching regulations and standards. In most environments, separate benchmarks have to be created for different asset types or technology, but Total Protection for Compliance delivers a single benchmark to assess all assets. There is no need to create one PCI template for host systems where agents reside and another for network devices without agents.



Administrators use the ePO console to select a single benchmark to assess both managed and unmanaged devices for compliance with PCI DSS system configuration requirements

Step 3: Assign assets. From within ePO, the security administrator assigns the PCI benchmark to the systems and devices that need to be audited for PCI compliance. This ability to assess only those assets that are necessary saves time, both in management and execution.

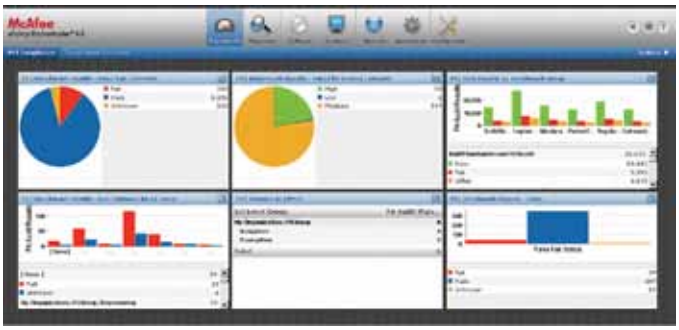
Step 4: Execute audits. The security administrator runs the assessments from within the ePO console. Once launched, the assessment will run against both managed and unmanaged assets. If the asset (for example, a Windows server) has a McAfee agent installed, Policy Auditor will perform the assessment. If there is no agent, Vulnerability Manager will perform the assessment, based on the same benchmark. This level of unified policy auditing is unique to McAfee Total Protection for Compliance.

Step 5: View audit results. Both Policy Auditor and Vulnerability Manager return their assessment results to ePO. Security administrators can review summary information in dashboards that visually represent the state of PCI compliance across multiple assets of different types. This high-level view shows the benchmark results (pass or fail), the severity of the failures, and a summary of the audit results by business area. This powerful, consolidated view lets security administrators assess the entire network—its risk and compliance, on an asset-by-asset basis—all at once.

Step 6: Drill down into details. From the summary views in ePO, administrators can then click on selected areas and view more detailed reports of assets and their compliance with PCI DSS requirements. Built-in reports display information on whether assets passed or failed a benchmark and also on their

individual compliance scores. Users obtain the information they need to determine which assets need the most attention and to prioritize remediation efforts.

From here, administrators can perform additional analysis, and report information can be automatically distributed across the organization to IT operations, line of business owners, and executives.



McAfee provides compliance dashboards to interpret the results of PCI DSS policy assessments quickly and easily.

Conclusion

Compliance audits are here to stay. As regulations increase and affect companies of all sizes, organizations need a new approach to managing multiple audits.

McAfee's Total Protection for Compliance solution seamlessly automates compliance activities through the industry's first integrated, agent-based and agentless solution for patch assessment, compliance reporting, and risk analysis. Through extensive standards support, McAfee reduces mistakes and misinterpretations that complicate and prolong the auditing process.

- **McAfee Policy Auditor** uses innovative automation and product integration to streamline processes throughout the policy management and auditing life cycles.
- **McAfee Vulnerability Manager** leverages its proven network scanning engine and an expanded library of many thousands of checks into a policy audit framework.
- **McAfee ePO** brings it all together through a unified platform for deploying, managing, and reporting on system security and policy compliance. ePO combines policy management with management of other McAfee products, as well as third-party security alliance partner products.

By integrating McAfee Policy Auditor and Vulnerability Manager with ePO, McAfee optimizes your security investment to deliver quantifiable operational efficiencies. ePO customers benefit from significantly fewer deployed servers and a reduced number of administrators, each spending less time per week administering and managing security products. These savings translate into measurably lower staff resources and operating costs.

For more information about McAfee's IT Governance, Risk and Compliance solutions or McAfee ePolicy Orchestrator (ePO), visit: www.mcafee.com/grc or call us at 888.847.8766—24 hours a day, seven days a week.

About McAfee, Inc.

McAfee, Inc., the leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world. With its unmatched security expertise and commitment to innovation, McAfee empowers businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security.

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

13602brf_tops-compl_0910_fnl