Lab Test Report

DR110208B

McAfee Risk Management Solution

February 8, 2011

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Taking a risk-based approach to vulnerability lifecycle management is becoming the norm for vulnerability assessment vendors. In fact, the latest PCI DSS standard (2.0) requires companies implement a risk-based vulnerability assessment system to demonstrate compliance with the regulation. With this in mind, we tested McAfee's Risk Management solution, consisting of McAfee Vulnerability Manager and McAfee Risk Advisor, from a holistic risk management and vulnerability lifecycle management perspective. We evaluated the product using the typical workflows required for end-to-end vulnerability, security, compliance and risk management.

During our testing, we found that the McAfee Risk Management solution is able to assess and manage risks across operating systems, networks, databases, and web applications from a single management console, McAfee ePolicy Orchestrator. Automated discovery of those broad infrastructures is made possible through integration with asset inventory technologies, such as Active Directory (AD) and LDAP. We also uncovered a unique ability to correlate countermeasure data with vulnerability and threat data to reduce remediation efforts and better focus security efforts. This is done by eliminating the devices already protected by existing network endpoint security products or some other form of countermeasure.

Miercom conducted an extensive battery of tests that the McAfee Risk Management solution passed in four major areas, including vulnerability lifecycle management, security and compliance assessment, risk management, and reporting. We found that the McAfee Risk Management solution provides a comprehensive, well-organized, "expert" security solution for mid-market and enterprise networks.

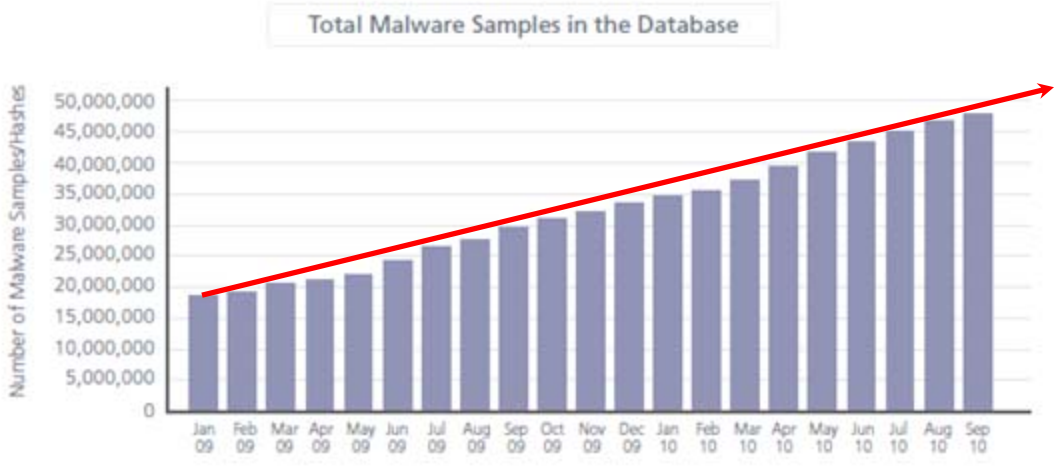
Rob Smithers
CEO
Miercom

2.0 Background

Our evaluation was based upon the premise that malware, specifically Advance Persistent Threats (APTs) are rising by leaps and bounds. To best protect against these threats, companies need to implement a holistic approach to risk management. In preparing to review the McAfee Risk Management solution, we considered several trends:

- According to McAfee's Global Threat Intelligence (GTI) report, there are currently more than 45 million pieces of malware. These malware are on a mission to steal the intellectual property and confidential data of your company. Successful exploits of malware can have a very real financial implication on your business. See *Figure 1*.
- In the past few years, operating system vulnerabilities are on the decline while web and database vulnerabilities, such as SQL Injections and Cross Site Scripting (XSS), are on the rise; especially XSS, which in 2010, is 17 times greater than it was in 2002. Web application vulnerabilities are 39% XSS and roughly 7% SQL injection. (See *Figure 2* on the following page.) Botnet infections have reached 500,000 per day.

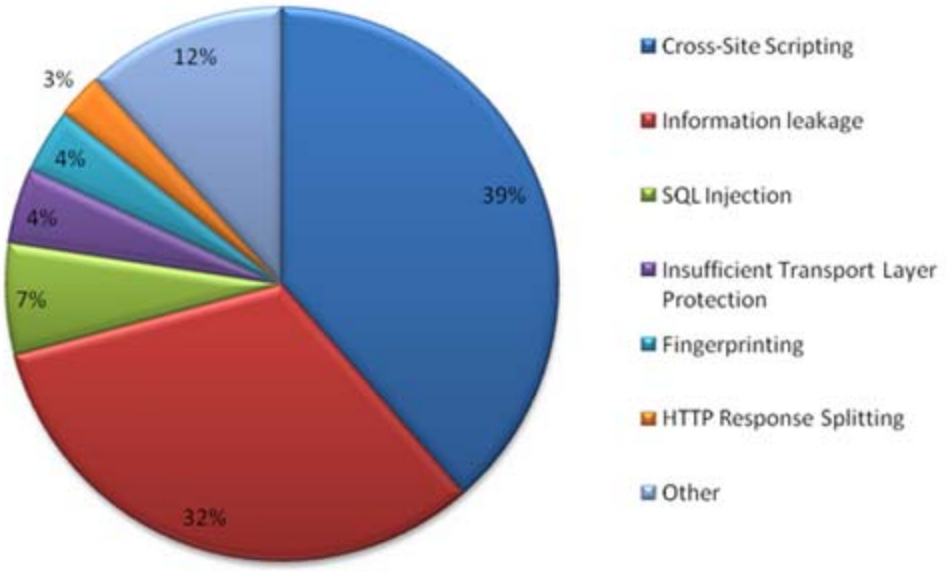
Figure 1: Malware Growth from 2009 to 2010



Source: McAfee Labs

Total count of unique malware (including variants) in the McAfee Labs database.

Figure 2: Percent of Vulnerabilities out of Total Number of Vulnerabilities



Source: Web Application Security Consortium

Increase in web and database vulnerabilities is shown above. Note that Web application vulnerabilities are 39% XSS and roughly 7% SQL injection.

Based on the above data, we believe the most important aspect required for managing risks is tight integration between detection, protection and remediation. The ability to tie risk, vulnerability, security, and compliance lifecycle management into one cohesive solution minimizes risk and hence, business impact. It is essential to have your risk management solution be efficient and manageable with limited resources. The first step in security and vulnerability lifecycle management is creating an asset inventory. Once assets are accurately identified, the next step is to detect vulnerabilities on network devices, operating systems, applications and databases. After vulnerability and compliance assessment, the security administrator would follow with the prioritization, remediation, and rescanning. Reporting on every stage will allow security administrators to gauge the progress. The overall risk, vulnerability, compliance and security lifecycle management can be summarized as follows:

Vulnerability and Compliance Life Cycle

Miercom evaluated the security capabilities of the McAfee Risk Management solution, which includes Vulnerability Management for operating systems, web applications, networks and databases, along with fully automated countermeasure aware risk based prioritization with unified reporting and alerting. We mapped use cases to each phase reflected above. The table below defines the use cases against each step in this lifecycle management process.

Category	Vulnerability and Security Life Cycle Management Stage	Specific Use Cases
Vulnerability Life Cycle Management	Asset Inventory (Section 4.1)	- Accurate discovery of assets - Accurate port and application discovery - Accurate database discovery - Asset Grouping - Integration and import from third party asset inventory databases - Accurate reconciliation
	OS/App/DB Detection (Section 4.1)	- Accurate port, OS and application discovery - Accurate database discovery
	Vulnerability Detection (Section 4.2)	- Content check - Accurate scanning - Coverage of vulnerabilities in operating systems, web applications, networks and databases - False positive and false negative handling - Scanning of networks not connected to the Internet or corporate network
	Remediate (Section 4.3)	- Ticketing workflow - Ticket bundling - Third party remediation integration
	Rescan (Section 4.4)	- Same use case as vulnerability detection
Security and Compliance assessment	Compliance Assessment (Section 5.1)	- PCI/SOX/GLBA/ISO 27001 - FDCC
	Baseline Configuration Audit (Section 5.2)	- Gold configuration testing

Risk Management	Prioritization based on advanced countermeasure correlation (Section 6.1)	- Correlation of threats with vulnerabilities and deployed countermeasures
	Prioritization based on CVSS score (Section 6.2)	- Prioritize remediation based on vulnerability severity and asset criticality
	Impact Assessment of a new vulnerability (Section 6.3)	- New threat identification using Stuxnet MS10-046 as reference - Impact of new threats - Risk of new threats - Correlating with existing countermeasure
Reporting	Reporting and Alerting (Section 7.1)	- PDF, HTML, XML and CSV report format - Operating system, web application, network and database vulnerabilities - Delta reports - Trend reports - Detail reports
	Positive Reporting for Auditors (Section 7.2)	- Auditor friendly report with evidence
	Business Reporting (Section 7.3)	- Total threats being covered by a particular countermeasure

3.0 Installation and Initial Configuration

McAfee Risk Management comes as a set of fully integrated products, which provide vulnerability, risk and compliance management capabilities. The vulnerability and compliance management component comes as software or an appliance. Advanced risk management via McAfee Risk Advisor is fully integrated into McAfee ePolicy Orchestrator.

The installation went smoothly and the configuration is fairly intuitive and very well documented.

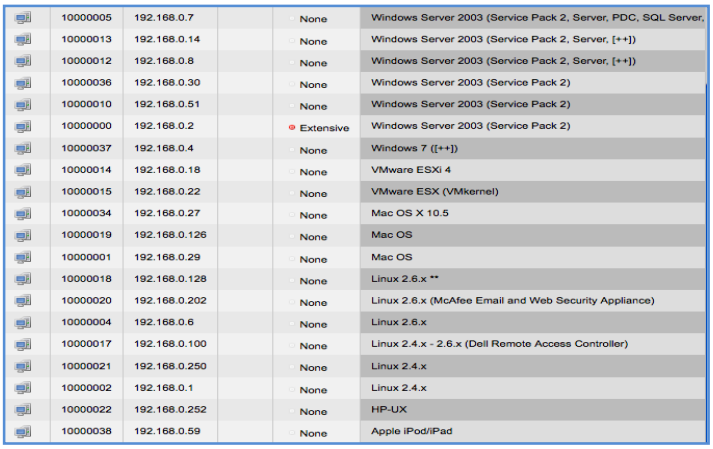
Miercom conducted 14 different scans to test different use cases. The host with DHCP and static IP addresses were scanned. Examples of the configured scans include:

1. Discovery Scan
2. Full Vulnerability Assessment Scan
3. Web Application Scan
4. PCI Scan
5. Base line Policy Compliance Scan
6. Database Scan

4.0 Vulnerability Life Cycle Management

4.1 Asset Inventory - operating systems, web applications and databases and networks

Figure 3: MVM Asset Inventory

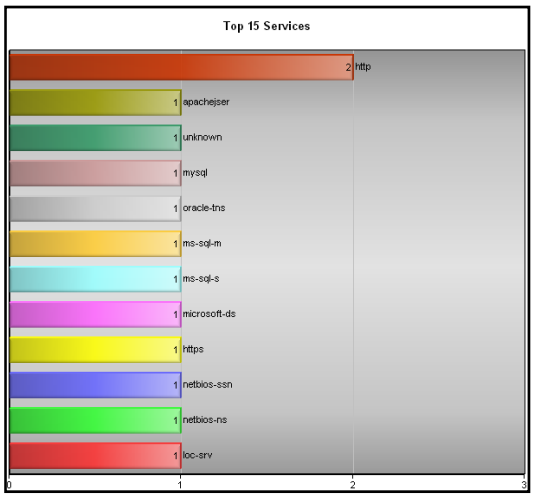


	10000005	192.168.0.7		None	Windows Server 2003 (Service Pack 2, Server, PDC, SQL Server,
	10000013	192.168.0.14		None	Windows Server 2003 (Service Pack 2, Server, [++])
	10000012	192.168.0.8		None	Windows Server 2003 (Service Pack 2, Server, [++])
	10000036	192.168.0.30		None	Windows Server 2003 (Service Pack 2)
	10000010	192.168.0.51		None	Windows Server 2003 (Service Pack 2)
	10000000	192.168.0.2		Extensive	Windows Server 2003 (Service Pack 2)
	10000037	192.168.0.4		None	Windows 7 ([++])
	10000014	192.168.0.18		None	VMware ESXi 4
	10000015	192.168.0.22		None	VMware ESX (VMkernel)
	10000034	192.168.0.27		None	Mac OS X 10.5
	10000019	192.168.0.126		None	Mac OS
	10000001	192.168.0.29		None	Mac OS
	10000018	192.168.0.128		None	Linux 2.6.x **
	10000020	192.168.0.202		None	Linux 2.6.x (McAfee Email and Web Security Appliance)
	10000004	192.168.0.6		None	Linux 2.6.x
	10000017	192.168.0.100		None	Linux 2.4.x - 2.6.x (Dell Remote Access Controller)
	10000021	192.168.0.250		None	Linux 2.4.x
	10000002	192.168.0.1		None	Linux 2.4.x
	10000022	192.168.0.252		None	HP-UX
	10000038	192.168.0.59		None	Apple iPod/iPad

MVM Asset Inventory shows IP address, installed operating system, and criticality of an asset.

The first step in a comprehensive security, compliance and risk management program is to accurately discover/identify assets and associated operating systems. We used the default discovery scan template in McAfee Risk Management solution to get the complete inventory with asset IP address, operating systems and ports. One of the typical scenarios was to disable ICMP ping on the target machine and test the discovery capability. We were impressed to see the McAfee Risk Management solution accurately detect the target system as alive. McAfee Vulnerability Manager, one of the critical components of McAfee Risk Management solution; with broad discovery mechanism was able to detect multiple operating systems. It uses ARP, TCP, UDP and ICMP protocols to detect if the system is alive. In our testing, we were able to accurately identify different operating systems. As shown in the Figure 3 above, we were able to accurately detect six Windows servers, one Windows 7 system, six Linux systems, three Mac OS systems and an Apple iPod. Alternatively, all of the assets can be pulled from a centralized asset management database or Active Directory/LDAP. It also has a strong reconciliation engine, reconciling assets based on MAC address, IP address, domain name or a combination of these parameters. It also uses a special string or GUID to identify the asset that provides accurate asset and vulnerability reconciliation, even in DHCP (dynamic IP) environments. Assets can be grouped by department or function. Logical assets, such as applications and databases, are also created in the asset tree to provide flexibility and manageability, along with segregation of duties to best manage risk.

Figure 4: Top 15 Services in the Network



Prioritized list of the 15 most used network services is displayed. HTTP is the most used service in this example.

The next step was to identify a list of applications and services running on the host. We scanned the systems and were able to identify all the installed applications visible from outside the network. HTTP, MySQL, Oracle, Microsoft SQL Server and other Microsoft services were identified. For vulnerability and compliance assessment, it is beneficial to have a list of accurate assets, operating systems and a list of services running on the network.

The final step was to identify the actual database instances. We used the database scanning component of the McAfee Risk Management solution to discover the database instances. We were able to identify two different instances of databases (Oracle and MS-SQL) running on the target system.

4.2 Vulnerability Detection

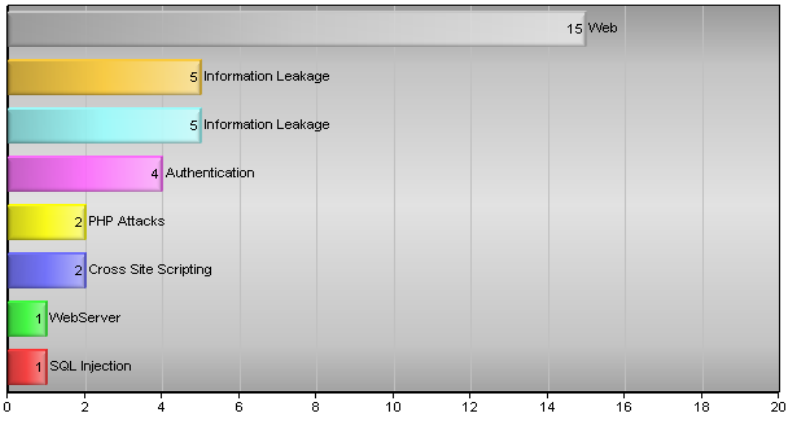
The heart of vulnerability management is the accurate detection of vulnerabilities. McAfee Risk Management solution provides out-of-the-box vulnerability scanning templates for network devices, operating systems, web applications and databases. We selected five systems from the target network under test. Four systems were running a Windows 2003 server and one system was running Windows XP. McAfee Risk Management solution identified:

- 203 operating system vulnerabilities
- 984 vulnerabilities on MS-SQL and Oracle express database instances (293 were critical vulnerabilities out of 984 reported vulnerabilities for the database)

Some of the operating system critical vulnerabilities detected included:

- Microsoft Windows server service vulnerability (CVE-2006-3439)
- Microsoft server service MailSlot Heap overflow (CVE-2006-1314)
- Microsoft Win32 API Vulnerability (CVE-2007-2219)
- Microsoft Internet Explorer Cookie Session Fixation (CVE-2008-3173)
- Microsoft SMB Validation Remote Code Execution Vulnerability (CVE-2008-4835)
- Microsoft Windows Threat Elevation of Privilege Vulnerability (CVE-2008-2540)
- Microsoft Internet Explorer 'User Add' Code Execution Vulnerability*

Figure 5: Top Web Application Vulnerabilities



Most severe application vulnerabilities are prioritized for an action by an administrator.

(* Exploit was published on 15th Feb 2010 on http://www.exploit-db.com/exploits/11457/)

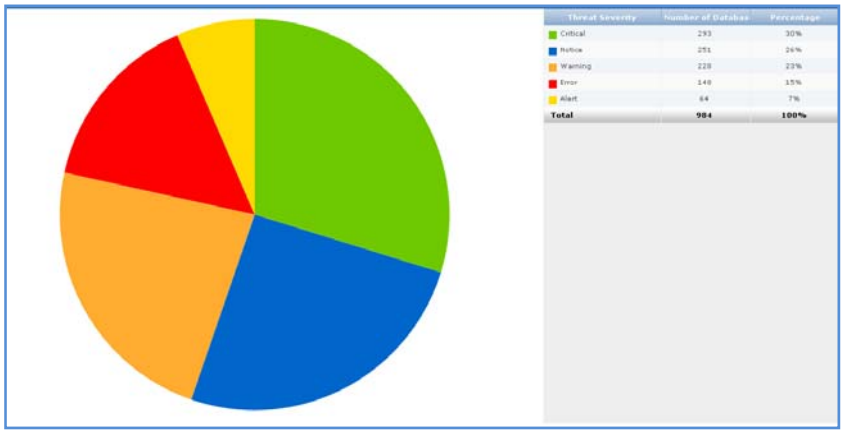
Some of the application level vulnerabilities detected included:

- Cross Site Scripting
- SQL-Injection
- Possible Authentication Bypass via Forced Browsing
- Apache Request Header Information Leak (CVE-2010-0434)

Some of the database vulnerabilities detected included:

- Buffer overflow in sp_rplwriteovarbin (CVE-2008-5416)
- Database vulnerable to .Net API problem (CVE-2009-2504)
- Database vulnerable to a GDI+ PNG Heap Overflow (CVE-2009-2500)
- Columns contain unencrypted SSN number

Figure 6: Database Vulnerability by Category



McAfee Risk Management solution shows different types of vulnerabilities separated by threat severity.

McAfee Risk Management solution and specifically its operating system and network scanning components, provides the ability to scan completely isolated networks hosting sensitive data. Critical Infrastructure Providers with SCADA environment, certain government networks, and large distributed institutions may have networks that cannot be reached from the Internet or even their own networks directly. However, they are still required to scan, report and manage the risk due to the vulnerabilities. McAfee Risk Management solution provides the answer to satisfy such requirements.

4.3 Remediation

McAfee Risk Management solution provides close-loop remediation which can be segregated based on each functional area, such as vulnerability, security and compliance management. Additionally, it provides an optional centralized remediation, alerting and reporting capability. For remediation, tickets can be automatically created and closed. The ticketing system also has false positive and false negative detection workflow; delegation capabilities; integration with third party ticketing; and automated remediation systems. Top level ticket search capability provides a list of tickets based on criteria of interest. Tickets are further categorized by users, vulnerabilities and assets, presenting relevant information that matters most for the user by

filtering out all unnecessary information. This approach provides a clear list of tasks for security and system administrators which results in an efficient remediation process. Ticket status is grouped into a single summary email, which provides clear remediation status across all tickets.

4.4 Rescan

Scheduling and rescanning is very flexible with the McAfee Risk Management solution. Operating system, database and web application scans can be scheduled separately on predefined time intervals to accommodate the specific SLA requirements of an organization. For all vulnerabilities that were fixed from the previous scan, McAfee automatically closes the ticket for those vulnerabilities, which provides substantiating evidence that the fix is protecting the asset.

5.0 Security and Compliance Life Cycle Management

5.1 Compliance Testing

We tested the ability of the solution to provide out-of-the-box compliance templates to audit against regulations and frameworks, such as SOX, HIPAA, ISO27002, PCI and FDCC. In our testing, we created multiple scans for PCI and FDCC**. All the scan templates including the PCI scan template can be customized.

Figure 7: PCI Summary Report

PCI Vulnerabilities

IP Address MAC Address	DNS Name NetBios Name Label	Vulns	PCI Violations	Result
10.100.250.227	VULN-APP-DB	106	86	✖
10.100.250.230	MVM-01	216	49	✖
10.100.250.229	MVMDB	10	3	✖
10.100.250.228	MCAFEE-EPO-00	7	2	✖

PCI compliance issues by IP address and device name.

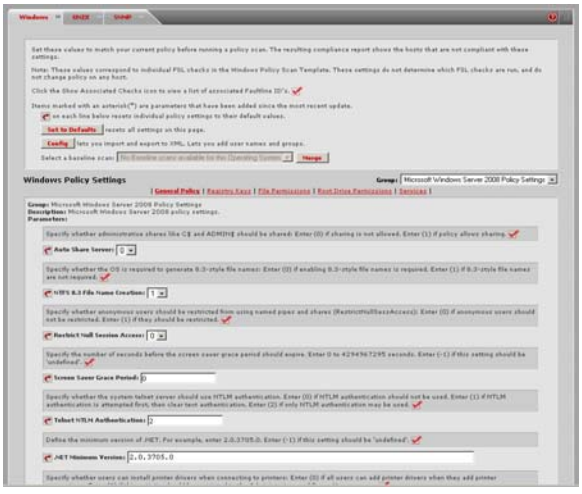
A PCI scan on one of the systems yielded 86 violations. As a result of those violations, the test system failed the PCI audit. In other words, an organization would have to fix the 86 violations to pass the PCI audit. The report clearly quantifies the actions required to pass the PCI audit.

(** For FDCC we had to make some configuration changes on the target host for administrator login, as suggested by Microsoft in the KB article http://support.microsoft.com/kb/555910)

5.2 Baseline Policy Compliance Testing

A good number of PCI checks were also part of the baseline security policy template. This template allows organizations to test all systems against a gold or known good configuration standard. Organizations are able to choose a default policy template provided by McAfee as a gold standard or they can create their own gold standard. A gold standard can be created by tweaking an existing template or by scanning a system with the gold standard configuration. Once the system with gold standard configuration is scanned, it becomes the reference source to compare all configurations on all machines.

Figure 8: Policy Compliance Configuration

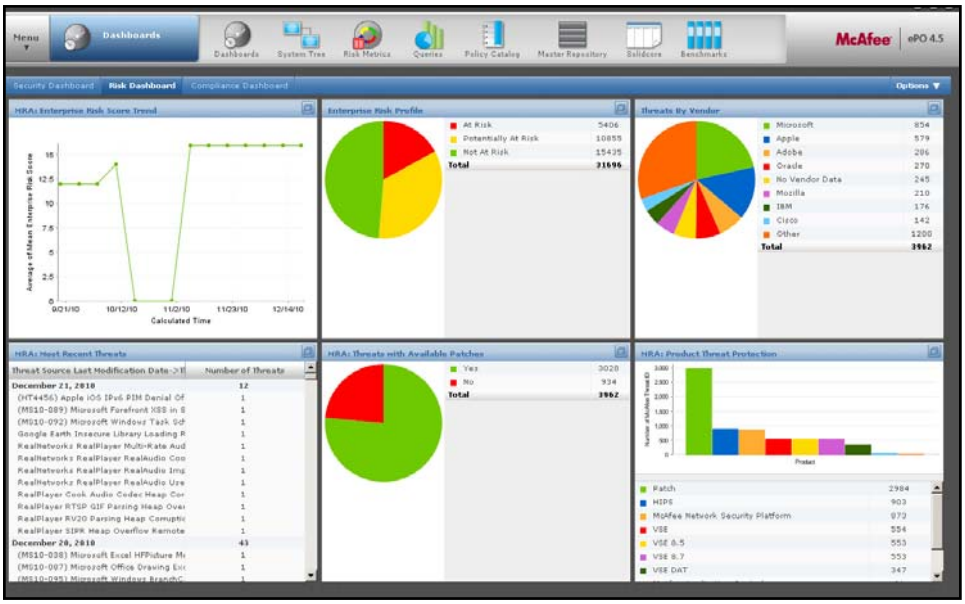


A checklist format provides a quick baseline policy compliance overview.

6.0 Risk Management

We tested the risk-based approach to vulnerability management as mandated by PCI 2.0 standard. The testing was based on the solution's ability to support CVSS scoring. Based on this scoring, organizations can prioritize their remediation efforts. However in this category we were impressed by McAfee Risk Management solution's ability to correlate countermeasure mitigating the new or existing threats; advanced correlation capability provided by the McAfee Risk Management solution.

Figure 9: C-Level Risk Dashboard



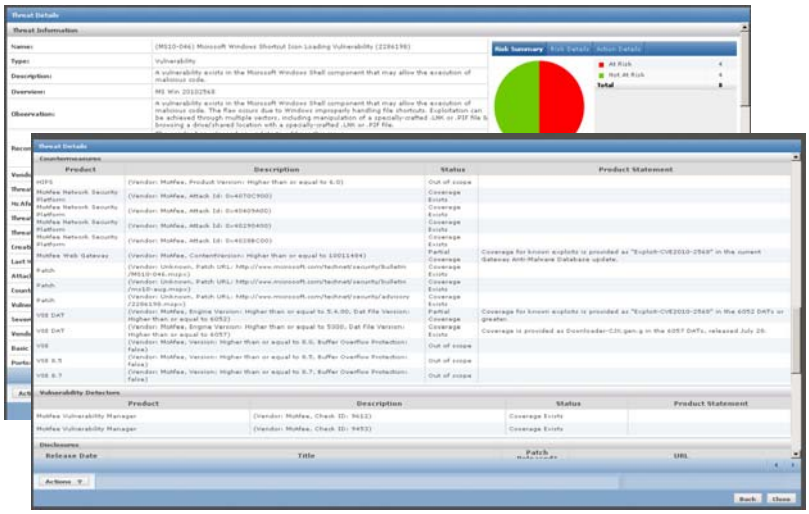
Risk dashboard with risk reports based on criteria of interest.

On McAfee ePolicy Orchestrator, one can quickly view the enterprise-wide risk trend; risk by vendors; or risk by impact.

6.1 Prioritization based on Advanced Countermeasure Correlation

McAfee Risk Management solution reduces the risk score of the system already protected by endpoint or network countermeasures. This advanced countermeasure correlation ability against threats makes the entire vulnerability, risk and compliance lifecycle management efficient. Most importantly, it allows organizations to focus their limited resources on mitigating the most severe threats against the most critical, unprotected assets.

Figure 10: Countermeasure Correlation – Example MS10-046 (Stuxnet)



Countermeasure correlation for computer worms targeting windows machine with MS10-046 vulnerability are shown.

6.2 Prioritization based on CVSS Score

McAfee Risk Management solution also supports vulnerability risk calculation methodology such as the Common Vulnerability Scoring System (CVSS). CVSS scoring is simple but a very effective approach to prioritize the remediation effort. Organizations can start remediating the most severe vulnerability impacting the most critical asset in the environment.

Figure 11: CVSS Scoring

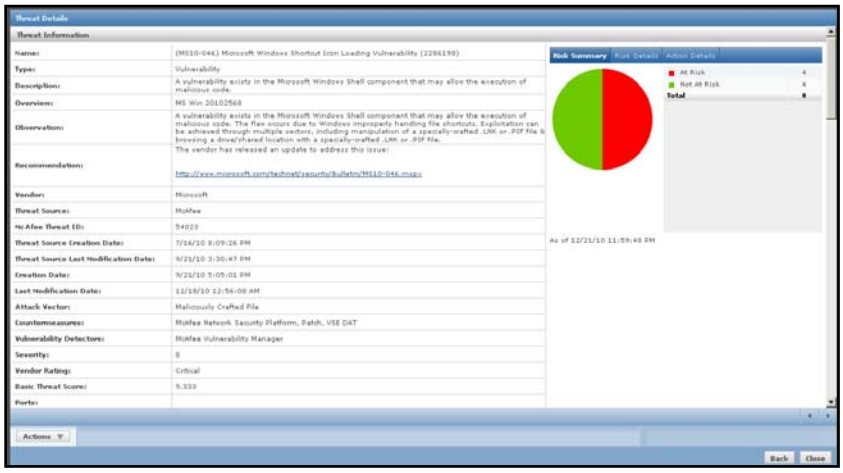
CVSS Information

Owner Name	Vector Description	Base Score	Temporal Score	Environmental Score	Score Detail
McAfee	(AV:N/AC:M/Au:N/C:P/I:P/A:P)(E:U/RL:OF/RC:C)	6.822	5.045	5.045	{AV:1.0, AC:0.61, Au:0.704, C:0.275, I:0.275, A:0.275, E:8.589, RL:0.87, RC:1.0}
NVD	(AV:N/AC:M/Au:N/C:C/I:C/A:C)	9.333	9.333	0	{AV:1.0, AC:0.61, Au:0.704, C:0.66, I:0.66, A:0.66, E:8.589}

Common Vulnerability Scoring System for IT vulnerabilities is displayed.

6.3 Impact Assessment of New Vulnerability

Figure 12: Impact Assessment based on Countermeasure Status



This view provides actionable impact information to help administrators prioritize countermeasure deployment.

McAfee Risk Management solution includes a threat feed from McAfee Labs' Global Threat Intelligence (GTI). McAfee GTI acts as a cloud intelligence hub for threats and vulnerability information. Any new vulnerability detected by GTI is pushed to the McAfee Risk Management solution, which in turn gets correlated with an organization's environment to calculate the residual risk. In this example, we chose a very well known vulnerability, "MS10-046 .lnk," which was exploited by the Stuxnet worm to illustrate the importance of advanced correlation. With a few mouse clicks we could identify the total number of systems at risk due to Stuxnet and the systems that are already protected against Stuxnet. Total time to assess the impact of the new threat was no more than two mouse clicks (i.e., a couple of seconds).

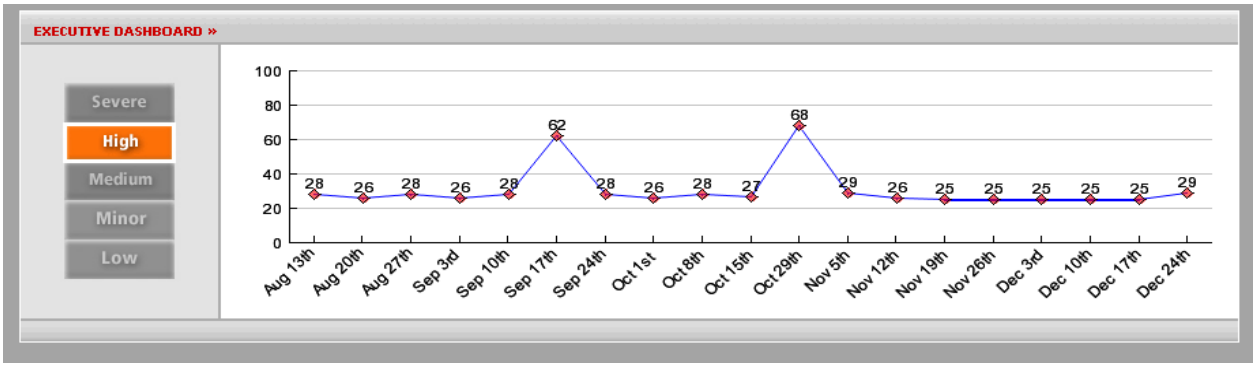
7.0 Reporting

As reporting is one of the most critical aspects of the security, risk and compliance process, we added a special category to assess the reporting aspects. All components of this solution have their own local reporting and optional vulnerability and compliance management components that can be integrated into McAfee ePolicy Orchestrator for centralized alerting and reporting purposes.

7.1 Reporting and Alerting

The McAfee Risk Management solution provides various alerting capabilities from email to an SNMP trap. It also provides the ability to create reports in a variety of different formats, such as HTML, CSV, XML or PDF. We configured multiple scans using the scan configuration wizard that also includes a reporting option. Reporting is straightforward.

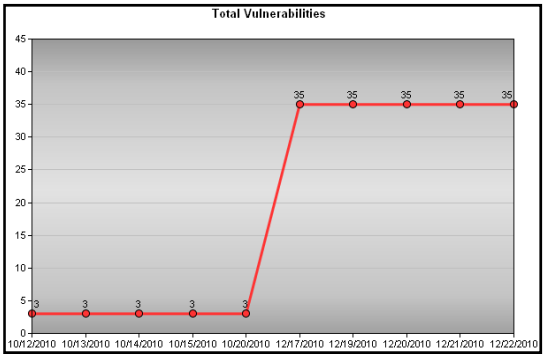
Figure 13: Trend Report: Global Risk Score Trend



A time-based analysis of the overall risk acts as a key risk indicator.

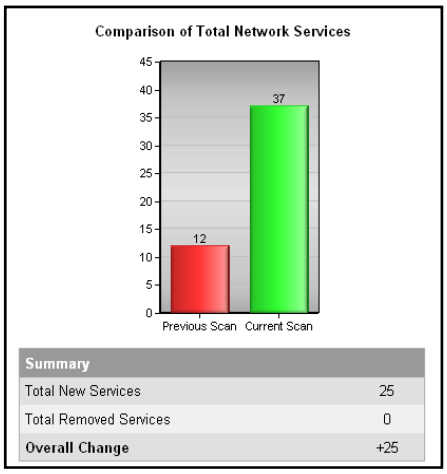
There are several out-of-the-box trend reports, which provide organizational level trending or very granular asset level trending on vulnerabilities and risk scores.

Figure 14: Trend Report: Total Vulnerability Trend for a Host



Vulnerability trend which can also act as one of the key risk indicators.

Figure 15: Delta Report: New Services Added since Last Scan

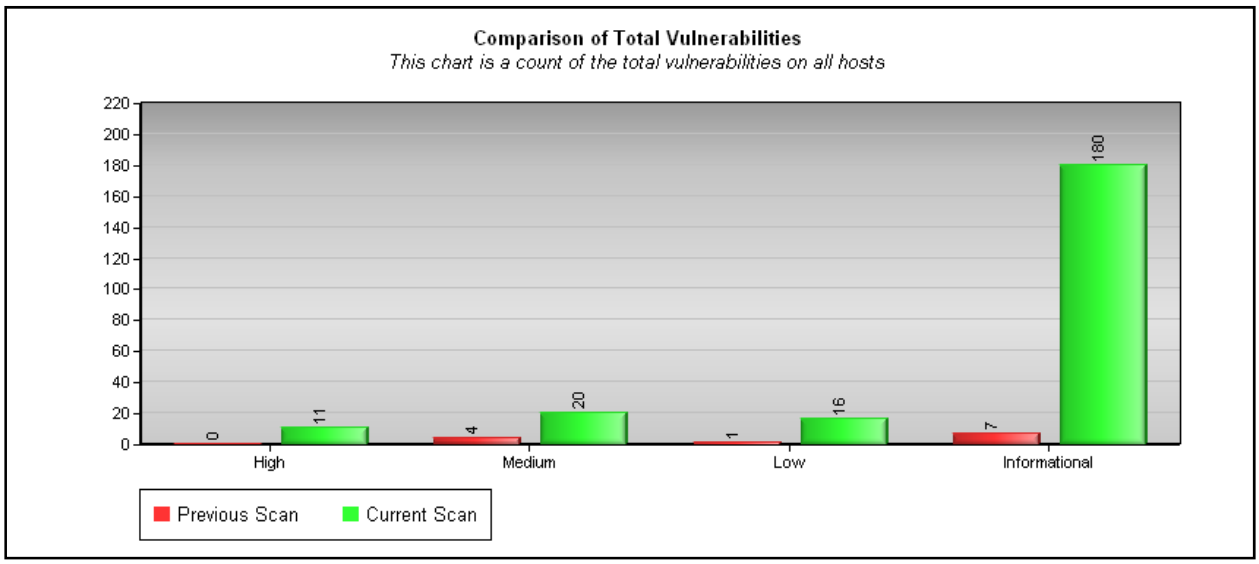


Summary	
Total New Services	25
Total Removed Services	0
Overall Change	+25

Network changes are shown by comparing total network services between previous scan and current scan.

McAfee Risk Management solution provides delta reports to indicate changes in the network. In this case, we detected an additional 25 services that started in our target network. This is essential to correlate the impact of changes to the overall risk score. Delta reports provide insight into the total new vulnerabilities added to the network since the last scan. The report indicated that as we added new services to the network, new vulnerabilities were introduced along with them.

Figure 16: Delta Report: New Vulnerabilities Added since Last Scan



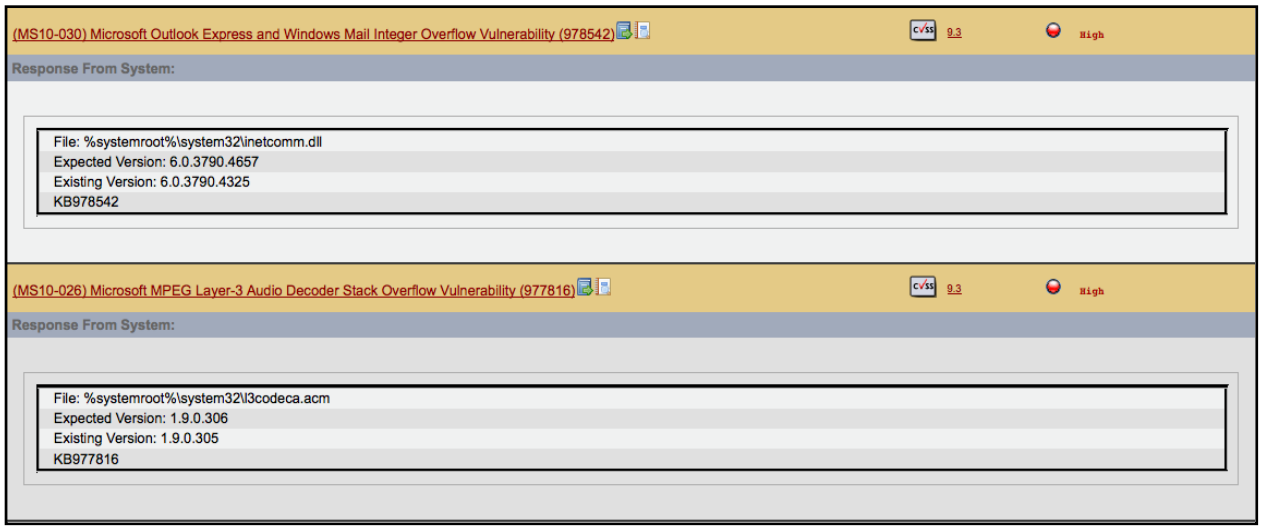
The changes in vulnerabilities between current and previous scan are displayed.

7.2 Positive Reporting for Auditors

Auditors require evidence to confirm that all vulnerability and compliance checks were enabled and tested against the target. Traditional vulnerability or compliance scanners only report on failed checks.

McAfee Risk Management solution, and in particular McAfee Vulnerability Manager, reports on all checks irrespective of the result of the check. Security/compliance managers can generate reports on pass, as well as failed checks. This type of positive reporting which includes pass and fail checks, assures an auditor that all target systems were assessed against all the required checks.

Figure 17: Report: Positive Reporting

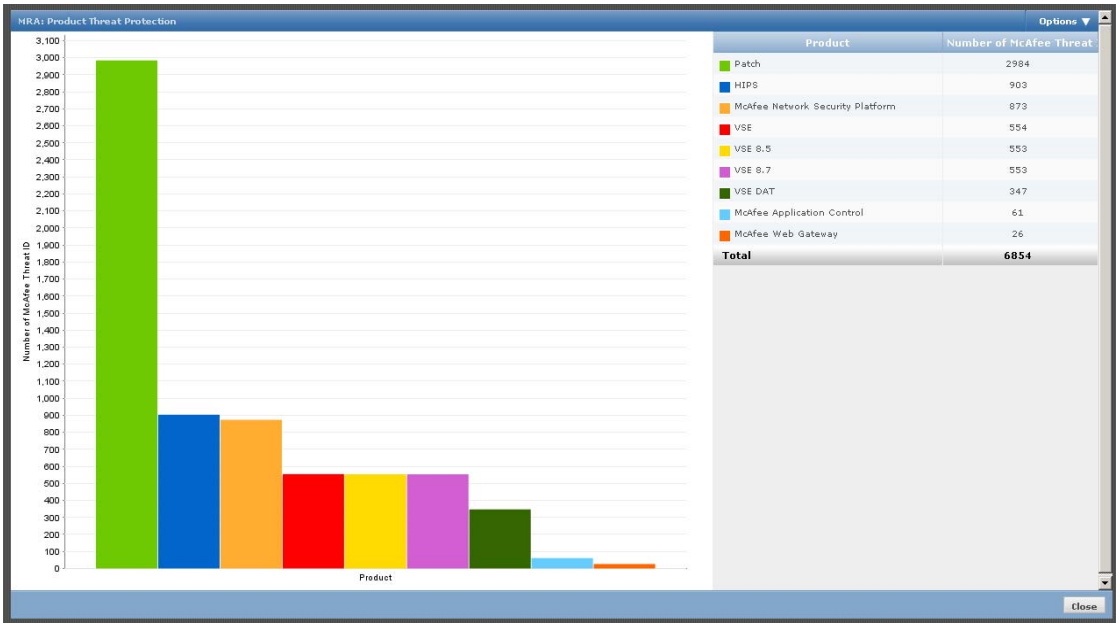


Vulnerabilities are shown that exist in Microsoft Outlook Express and in Microsoft MPEG Layer-3 Audio Decoder.

7.3 Reports for Business Users

Organizations are investing heavily to purchase and maintain security products. However, they do not have the metrics to measure the efficiency or effectiveness of those products, or information needed to support the business case for procuring the new products. McAfee Risk Management solution provides clear data on prevented threats by patches and deployed countermeasures, such as antivirus, host intrusion prevention, etc. With these features, the metrics to support existing investments is provided and/or the business case for new security products can be made.

Figure 18: Report: Countermeasure Effectiveness



Administrators can assess the relative impact of various deployed countermeasures.

8.0 Conclusion

It is important to note that even though it is rich in features, the McAfee Risk Management solution is not what would traditionally be classified as a full-blown Governance, Risk and Compliance (GRC) product. For example, it does not have the ability to create manual survey questionnaires or document HR policies. Rather, it is focused exclusively on IT security risk. We believe, based on our testing, that organizations looking for a comprehensive and cohesive means for risk and vulnerability lifecycle management should give the McAfee Risk Management solution serious consideration.

9.0 Test Environment

For this report, Miercom engineers created the network found in typical enterprise IT infrastructures. McAfee Risk Management solution was tested in use cases related to vulnerability, risk and compliance management.

The network was comprised of 16-20 hosts with a variety of server and desktop operating systems. Considering the rampant use of virtualization, VMware ESX 4.0 was also in our test network. The test network also included a mix of patched and un-patched systems with different applications installed. We installed database servers, Oracle Express, MS-SQL 2005 server, mail servers, and a vulnerable web application server, along with other typical server services such as file and print servers. Some of the OWASP vulnerabilities were purposely introduced in the web application.

We also made sure that some of the machines were misconfigured, for example: default password or dictionary passwords were used. Some of the machines had McAfee endpoint security countermeasure, such as Anti-Virus, installed.

The test was conducted for 72 hours with different out-of-the-box scanning templates for operating system, network, web application and database.

The test bed used Dell PowerEdge containing VMs for clients and McAfee products.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Miercom recommends customers conduct their own needs analysis and testing specifically for the expected environment for product deployment before making a product selection. Contact reviews@miercom.com if you wish to receive assistance from Miercom professional services to conduct these tests.

10.0 About Miercom

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including *Network World, Business Communications Review, Tech Web - NoJitter, Communications News, xchange, Internet Telephony* and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.