Data Sheet

McAfee

McAfee Risk Advisor

Take the guesswork out of where to focus your security efforts

Organizations often deploy several security point products to try to stay ahead of constantly surfacing or evolving threats. However, even with all this deployed technology it's far too common for security and IT staff to be sitting in a war room on Patch Tuesday trying to answer the question, "Do we need to shut down our business and roll out this patch?" McAfee® Risk Advisor proactively combines threat, vulnerability, and countermeasure information to highlight those assets that are truly at risk. It takes the guesswork out of when and where to focus your security efforts—saving you time and money.

Key Advantages

- Balance business productivity needs with the right amount of security
- Quickly identify which assets are at risk to threats
- Eliminate the manual, time-consuming process of correlating threats to critical systems at risk to direct remediation efforts
- Stay current with threat feeds from McAfee Avert Labs
- Integrates with core McAfee products such as McAfee ePO console, McAfee Vulnerability Manager, McAfee Host Intrusion Prevention, McAfee Network Security Manager, McAfee Policy Auditor, and more

An industry first, McAfee Risk Advisor delivers risk metrics and analytics to take the guesswork out of where to direct your remediation efforts.

McAfee Risk Advisor correlates threat feeds with vulnerability and countermeasure information to deliver an immediate assessment of the specific assets that are at risk. With this information you instantly get information about a threat, its severity, and the risk it presents, allowing you to prioritize your remediation efforts according to an asset's value.

The distinction is significant, as an asset may be vulnerable to a threat, but with the appropriate countermeasures in place, it may not be at risk. Knowing which assets are both vulnerable and at risk helps security organizations focus their efforts on assets that need immediate attention.

Beyond the cost and administrative savings from McAfee Risk Advisor, you can determine a clear ROI of the countermeasure investments you've already made. Specifically, with McAfee Risk Advisor you can correlate threats with assets and get a clear picture of the countermeasures that protect those assets. This is true whether or not the countermeasures are in place. In addition, having this information aids you in determining which countermeasures you should invest in for future protection.

A Consolidated View

The Risk Advisor threat feed viewer provides up-to-the-minute information about new and updated threats from thousands of vendor and industry collection points. The viewer includes:

- Threat descriptions and overviews
- Detailed analysis
- Remediation and recommended actions
- Links to notices and exploit discussions
- Different risk scoring methods
- Applications impacted
- Threat impact on various regulatory mandates

The threat feed also contains specific McAfee countermeasures (if required) that can be deployed by the McAfee ePolicy Orchestrator® (ePO™) centralized management platform. The Risk Advisor viewer computes the number of hosts currently under management that contain the proper countermeasure and those that do not. A countermeasure compliance graph is generated directly in the threat view illustrating your countermeasure to the threat.

Specifications

Minimum System Requirements

- McAfee ePolicy Orchestrator 4.0 (Patch 3)
- Microsoft Windows Server 2003 (SP2 or higher)
- Microsoft SQL Server 2005 (SP1 or higher)

Optional System Requirements

- McAfee VirusScan® Enterprise 8.0/8.5
- McAfee Host Intrusion Prevention 7.0
- McAfee Rogue System Detection 2.0 (Patch 2)
- McAfee Vulnerability Manager 6.7

Risk Summary

In addition to countermeasure correlation, Risk Advisor's integration with McAfee Vulnerability Manager and McAfee ePO console enables you to chart your vulnerability profile to pinpoint where to focus your security efforts. The graph generated concisely reflects where and how your assets are at risk. The simple Boolean chart renders an "At Risk" and "Not At Risk" summary. When drilling down on the chart, a "Risk Details" chart reflects the following states:

1. **Green**—Not vulnerable and has protection (no vulnerability detected and has appropriate countermeasure protection).
2. **Yellow**—Vulnerable but protected (vulnerability detected but has the appropriate countermeasure to provide protection).
3. **Red**—Vulnerable and not protected (vulnerability detected and does not have the appropriate countermeasure).
4. **Gray**—Unknown (there is no data to determine vulnerability status or countermeasures; this is where devices such as routers and print servers are counted, as a countermeasure wouldn't apply to these assets).

To determine "At Risk" and "Not At Risk" status, Risk Advisor takes a pessimistic approach. The only way an asset can be classified as "Not at Risk" is if it's deemed, "Not Vulnerable and Has Protection." All other assets including the yellow (vulnerable but protected); red (vulnerable and not protected), and, gray (unknown) assets are put in the "At Risk" group.

Reporting

Simplified, top-down reporting lets you drill down quickly to see where you need to focus your remediation efforts. Starting from a consolidated dashboard, you can view granular and concise information about a threat. The level of detail provided lets you:

- Read about the threat and how it works
- See date and time the threat was first announced and the latest content update to the record
- View recommended remediation methods and countermeasures available from McAfee
- Identify which McAfee solution detects the vulnerability

Always up to date

To keep your organization current, McAfee Risk Advisor receives threat updates from our world-class research organization, McAfee Avert Labs. Our enterprise-class threat feed delivers concise, meaningful, up-to-the-minute data on threats as they materialize from our network of millions of data collection points.

The feed includes news and remediation information about a threat, along with links to disclosure and exploit information. In addition, the feed delivers illustrated risk scoring using CVSS v2 models and how a specific threat impacts industry regulations.

Also included is countermeasure information from McAfee VirusScan, McAfee Host Intrusion Prevention, and McAfee Network Security Manager as well as systems that detect vulnerabilities on an asset, such as McAfee Vulnerability Manager.

Visit www.mcafee.com or contact your local McAfee representative for more information.

McAfee®

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