

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 this 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 pinpoint 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
- The risk score delivers a quantifiable measure for evaluating risk mitigation efforts
- 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 Labs
- Integrates with core McAfee products, such as the McAfee ePO console, McAfee Vulnerability Manager, McAfee Host Intrusion Prevention, McAfee Network Security Manager, McAfee Policy Auditor, and more

Eliminate the Guesswork

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 calculates risk metrics by correlating threat feeds with asset criticality, vulnerability, and countermeasure information. The risk metrics deliver an immediate assessment of the specific assets that are at risk. You instantly get information about a threat, its severity, and the risk it presents, helping 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® (McAfee ePO™) centralized management platform.

The Risk Advisor viewer computes the number of assets 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 against the threat.

Risk Summary

In addition to countermeasure correlation, McAfee Risk Advisor's integration with vulnerability assessment tools and the 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 you drill down, a “Risk Details” chart reflects the following states:

1. **Red**—“At Risk.” These assets are at risk because they are vulnerable and not protected by any countermeasure.
2. **Green**—“Not at Risk.” Assets categorized as “Not at Risk” are not vulnerable or when vulnerable, have appropriate countermeasure protection in place.
3. **Yellow**—“Potentially at Risk.” These assets require further investigation because there is no data to determine vulnerability status or countermeasures; typically, these assets do not have the McAfee agent and are also not scanned by a vulnerability detector like the one in McAfee Vulnerability Manager.

To determine “At Risk” and “Not at Risk” status, McAfee 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” or “Vulnerable, But Has Protection.”

Risk Score

An industry first, the McAfee Risk Advisor risk score delivers a quantifiable measurement for evaluating risk mitigation efforts. The risk score unifies vulnerability/threat status, asset criticality, and countermeasure protection available for specific threat to quantify the risk of a threat on an asset. For example, with risk scoring, an administrator is able to say: “Risk mitigation efforts for past week have reduced net enterprise risk by 20 percent.”

Patch Optimization

With McAfee Risk Advisor, organizations are able to optimize and reduce patching cycles, as well as articulate an appropriate response for out-of-band, critical patches. With the patch prioritization report, administrators are able to establish patching priorities and workflow by seeing threats and available patches.

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 the 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 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. This data is leveraged by McAfee Risk Advisor to quickly and accurately reflect those critical assets that are both at risk and vulnerable to threats.

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 common vulnerability scoring system, version two (CVSS v2) models, and how a specific threat impacts industry regulations.

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

Next Steps

For more information, visit www.mcafee.com/riskadvisor or contact your local McAfee representative or reseller near you.

About McAfee Risk and Compliance

McAfee Risk and Compliance products help you minimize risk, automate compliance, and optimize security. Our solutions diagnose your environment for real-time insight into your vulnerabilities and policies so that you can protect your most critical assets by focusing security investments where they matter most. To learn more, visit www.mcafee.com/riskandcompliance.

