A vulnerability scan of a large, complex enterprise network may yield thousands of vulnerabilities, with results doubling or tripling if you are using multiple scanners. Remediating this volume of vulnerabilities is impossible: how do you know which vulnerabilities are critical to your business, your network? Instead, you need to prioritize vulnerabilities based on your network context, and focus remediation on the critical risks that are both exploitable and threaten your mission critical systems. Enhancing McAfee® Vulnerability Manager with Skybox Vulnerability Control provides a closed-loop solution that identifies network vulnerabilities; eliminates vulnerabilities that are not exploitable; prioritizes remediation based on business impact and exploitability; and integrates actionable remediation steps to mitigate the most significant risks before they can be exploited.

The Business Problem
An effective vulnerability management program reduces the risks of cyberattacks, supports continuous monitoring, and provides executives with useful measurements of risk. To reduce security risks you need a proactive approach that prioritizes vulnerabilities by business impact and automates and tracks remediation activities. This allows critical risks to be found and resolved in a day instead of months, eliminating unnecessary patching and drastically reducing security management time.

McAfee Vulnerability Manager and Skybox Vulnerability Control
Vulnerability scan results from McAfee Vulnerability Manager are collected by Skybox Vulnerability Control, which simulates attacks and analyzes access paths to determine which vulnerabilities are actually exploitable. In a typical IT environment, only 1% to 2% of vulnerabilities require immediate attention, as the majority of vulnerabilities are blocked by firewalls, intrusion prevention systems (IPS), and other compensating controls. Skybox uses predictive security analytics to correlate firewall data, vulnerability data, and threat intelligence to form a complete security picture. Leveraging Skybox Security’s patented Attack Simulation technology, IT managers can quantify and prioritize vulnerabilities in the context of network topology, security controls, threat intelligence, and potential business impact to valuable assets.

Customer Benefits
Skybox Vulnerability Control collects network information from McAfee Vulnerability Manager to enable the following capabilities:

• **Filtering vulnerabilities**—De-duplicates vulnerabilities found by multiple scanners and removes vulnerabilities that are blocked by compensating control, significantly reducing false positives.

• **Attack simulation**—Simulates attack scenarios in minutes using patented Attack Simulation technology that highlights possible exploitation routes by attack vectors, including hackers, advanced persistent threats, malware, and internal threats. It also considers all network security controls and routing rules for the most accurate simulation.
• **Vulnerability prioritization**—Prioritizes vulnerabilities using predictive risk analytics to find exploitable vulnerabilities posing the highest risk impact to the business.

• **Drive remediation and track results**—Provides actionable options for remediation, tracks progress and closure with a complete workflow and ticket-generation systems that connects to your security operations systems.

• **Prevent unintended access**—Predicts risky changes with advanced "what-if" modeling capabilities, ranks potential business impact of proposed network changes, and analyzes and monitors key performance metrics continuously.

**Unique Advantages**

Skybox addresses the full range of security risk management challenges, providing continuous, non-intrusive tools that detect, prioritize, and drive remediation of critical risks, reducing risk assessment costs by 90% through quantifying and prioritizing risk exposures and eliminating unnecessary patching. The advantages include:

• The most scalable solution in the industry, Skybox is used by the world’s largest financial, energy, government, and military institutions to efficiently handle the huge numbers of vulnerabilities that can lead to an attack.

• Continuous, closed-looped vulnerability management solution is based on network context, business impact, and exploitability of vulnerabilities—with a minimum of false positives.

• View your network from an attacker’s point of view, using patented tools including risk modeling, attack simulation, and analysis of all attack paths and scenarios.

• Measurable reduction in overall security risks, which decreases the risk exposure window from months to hours.

• Business impact and risk metrics reports are generated in minutes.

![Figure 1. Skybox Vulnerability Manager.](image)
**Free Trial**

**About Skybox Security**
Skybox Security provides powerful risk analytics that give security teams the intelligence needed to eliminate attack vectors, respond to threats and improve security processes. Skybox solutions are used for enterprise-scale vulnerability and threat management, firewall management, and continuous compliance monitoring. Headquartered in San Jose, California, Skybox Security has a strong customer base in the Global 2000, with established accounts in Financial Services, Government, Energy, Defense, Retail, and more.

**About McAfee Vulnerability Manager**
McAfee Vulnerability Manager, with its McAfee Asset Manager feature, delivers unrivaled scalability and performance, actively or passively canvassing everything on your network. Now you can uncover devices hidden on your network as well as smartphones, tablets, and laptops that come and go between scheduled scans. What you haven’t been seeing or scanning will surprise you—and could be jeopardizing your compliance. Thousands of organizations rely on McAfee Vulnerability Manager to quickly find and prioritize vulnerabilities—with deployments ranging from a few hundred nodes to one, continuously scanning more than four million IP addresses. If it has an IP address or is using your network, McAfee Vulnerability Manager can discover and assess it, automatically or on a schedule, revealing the compliance of all assets on your network.