The Risk Management Lifecycle
Protecting Critical Business Assets
Table of Contents

Overview 3
Diagram (10 Step Lifecycle) 4
I. POLICY 5
II. INVENTORY 5
III. PRIORITIZE 5
IV. VULNERABILITIES 6
V. THREATS 6
VI. RISK (Formula) 7
VII. BLOCK 7
VIII. REMEDIATION 8
IX. MEASURE 8
X. COMPLIANCE 8
Summary 9
Overview

Protection-in-Depth

In order to properly protect the critical assets in any business or government agency, security professionals, charged with this responsibility, must fully understand their risks prior to deploying any solution that will effectively protect these resources.

The following document outlines a ten-step Risk Management Lifecycle identifying the critical areas to effectively set up a risk management program that can be designed for any sized business within any industry. This paper will discuss specific research, strategies, and technologies that will help organizations mitigate their risk by rendering their networks more secure.

While many organizations have deployed security solutions such as firewalls and anti-virus programs, these efforts alone are not sufficient to protect crucial infrastructure components from the ever-evolving internal and external (Internet) threats.

By fully understanding their risks and utilizing each step of the lifecycle, any organization will be able to successfully deploy an information security program to protect against the latest threats to their digital assets.

All lifecycle steps can and should be personalized to meet specific organizational requirements and guidelines, but no step should be skipped or completed out of order.

As each step of the lifecycle is described, specific McAfee® proven technologies and solutions that are designed for achieving success in that step will also be explained.
The Risk Management Lifecycle

Ten-step Risk Management Lifecycle
I. Step One: POLICY

An effective security enforcement policy is critical in reducing or eliminating threats to an organization’s digital assets.

- **Strategy** – Understand what the goals and objectives are for an effective security program, making sure that it is fully supported internally (including the authority to be enforced).
- **Process** – Understand how to manage the policy in an organization and how it will be enforced. Establish procedures and process that will address violations or security incidents.
- **Standards and guidelines** – Build established standards into the policy and define new standards that will be supported and enforced by the policy.
- **Communication of the policy** – This is the most important step and includes educating all users affected by the policy, ensuring that they know where to find the policy, what to do and who to contact in the event of a violation or security incident.
- **Enforcement on trusted systems** – This step prevents users from installing unauthorized software, initializing insecure configuration changes, or adding components outside the bounds of a standard, authorized configuration.

**McAfee ePolicy Orchestrator® (ePO)**

By properly deploying ePO, organizations are able to use advanced policy and compliance features to control and enforce established policies and standards on trusted systems.

In addition data supplied by ePO will help to measure policy effectiveness.

- **System Compliance Profiler (SCP)** – An integral component of ePO, SCP runs vital compliance checks for the existence of critical operating system patches and common operating environment compliance.
- **Rogue System Detection** – This feature is designed to improve policy compliance within enterprises by identifying rogue or unprotected systems and allowing ePO to evoke a policy-based response on that system.

**McAfee Foundstone® Vulnerability Management**

McAfee’s Foundstone® Vulnerability Management product has been designed to provide data to achieve a success inventory.

By properly deploying the McAfee Foundstone product, an organization can accurately identify all assets in their computing and networking environment removing guess work. By scheduling periodic discovery scans, an organization can detect new assets soon after they are installed on the network rather than waiting for a periodic audit.

The Foundstone Vulnerability Management solution is fully scalable and is critical to success in this step and throughout the lifecycle.

**McAfee Foundstone**

Host inventory - Foundstone’s host discovery features can identify any device participating on the network (i.e. bearing an IP address). This technique covers not only a wide range of traditional devices such as servers, routers and databases but also non-traditional devices that are also Internet-connected such as specialized control systems and other customized hardware.

**McAfee ePolicy Orchestrator**

- Microsoft Active Directory integration - Scheduled importing of systems from AD into the ePO directory by regularly polling AD containers to discover new systems that have been added to the network.
- Rogue System Detection - Through distributed sensors, ePO is constantly monitoring, in real-time, new system connections to the LAN and establishing a yes/no rogue status. ePO then provides several manual and/or automated rogue system responses which include: instant notification of a rogue system connection, ePO agent deployment, exception marking, and execution of a third party tool.

II. Step Two: INVENTORY

To be effective once a set of security policies are established, an organization must fully understand all of its digital assets that need to be protected. These targeted assets should not only include the easily recognized assets required for the core “business process” but must include every network, segment, system, user, and application to achieve best practices for a comprehensive program of risk management.

**McAfee Foundstone**

By properly deploying McAfee Foundstone, an organization can accurately identify all assets in their computing and networking environment removing guess work. By scheduling periodic discovery scans, an organization can detect new assets soon after they are installed on the network rather than waiting for a periodic audit.

The Foundstone Vulnerability Management solution is fully scalable and is critical to success in this step and throughout the lifecycle.

**III. Step Three: PRIORITIZE**

Once vulnerable assets are identified a set of protection priorities must be created. The following issues should be considered when prioritizing:

- **Value** – Not hard cost, rather the cost of downtime and recovery. For example, if this is a customer-facing web application that generates revenue or has to be up to provide a service that supports revenue, consider the impact to revenue if down.
- **Incident recovery costs** – If an incident happened previously, how much did that down time cost and
how much did the recovery cost? Was there impact from Sasser, Slammer, or a virus? These are good baselines to consider helping resolve some of the guess work that often accompanies this step.

- **Lost productivity** – This includes the costs of data recovery, the amount of time a critical user or group are offline, the amount of time customers can’t access a site, missed delivery dates of new applications, etc.

- **Operational impact** – A specific example is the costs of system recovery that actually may fall outside of the security team. With Spyware, for instance, system response time slows over time, calls to the help desk increase, and eventually the only recovery option is to take that user offline and spend some period of time re-installing the infected system. This is where user priority becomes critical.

- **Business process mapping** – An example is the relationship between a customer-facing web application and the database it relies upon to provide service to the customer.

This step may seem daunting but a complete asset inventory and valuation is critical to effectively prioritize in terms of business systems versus development systems or customer data versus non-customer data.

**McAfee Foundstone**

- **Asset classification** – By using the asset classification features of Foundstone, organizations are able to classify systems using detailed, flexible criteria. This provides the ability to assign properties such as asset owners and criticality to align the asset value to business need.

- **Asset-based vulnerability management** – This feature allows organizations to focus remediation tasks on the most important systems.

- **Future integration with ePolicy Orchestrator will allow more complex asset prioritization and information sharing between the products and associated data stores.**

**V. Step Five: THREATS**

Quite often, an organization finds itself fixing vulnerabilities on a wide scale without fully understanding the asset value or threats. This step involves not only understanding what a threat is, but also how or if it can be effective in an environment based on potential vulnerabilities. This is the final step in determining the true risk level and will help clarify potential threats in an environment and the expected impact to the assets.

By understanding the threats against the most vulnerable and critical assets, discovered and prioritized in steps two through four utilizing McAfee ePolicy Orchestrator and McAfee Foundstone, any organization will be prepared to deploy the proper protective technology for specific problems and address those problems in a “Protection-in-Depth” manner, as discussed below.
McAfee Foundstone Threat Correlation Module
The Threat Correlation Module delivers up-to-the-minute Threat Intelligence Alerts from McAfee Research allowing organizations to respond immediately to breaking events such as worms and wide-scale attacks. The Threat Correlation Module creates a risk ranking for each threat by correlating events to asset and vulnerability information about an enterprise. Utilizing this information, organizations can quickly respond when and where the most critical assets are in danger.

Foundstone's Threat Compliance View
automatically tracks and graphs an organization's threat response efforts by business unit and platform, versus established remediation goals or policies. This up-to-date dashboard benchmarks and trends threat response to ensure security managers know that their team's remediation progress is neutralizing the threat.

VI. Step Six: RISK
By utilizing the following formula and data from steps one through five, a security manager is able to properly access the true level of risks to their organizations vulnerable assets.

\[ R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C} \]

- **R** = Risk
- **A** = Asset Value
- **V** = Vulnerability Severity
- **T** = Threat Criticality
- **C** = Countermeasures

McAfee Foundstone
- **Focus:** By correlating critical threats with important assets, an organization can focus on the threats and assets that matter the most—thereby spending less time focused on security and more time focused on their core business.
- **Compliance:** Establish internal security standards and guidelines and verify regulatory compliance.
- **Metrics:** Deliver the measurements and reporting tools to communicate and manage security decisions more effectively.
- **Action:** Improve security posture and initiate action with solutions aimed at real-world security problems.

Through the proper deployment and prudent use of the McAfee Foundstone Vulnerability Management product, and FoundScore® a security manager can understand their overall risk score which will then guide them to make decisions that prevent threats from impacting vulnerabilities on their most critical assets.

FoundScore is a security risk rating system that compares key aspects of a customer's network infrastructure against best practices in order to quantify their security posture. Based on an intuitive 0-100 scoring system, FoundScore rates networks' security health over time.

VII. Step Seven: BLOCK
Because of the new protective technologies that are available, organizations are now able to install "security vulnerability patches" while permanent operating system and application patches are properly tested and planned.

**McAfee IntruShield® Network Intrusion Prevention (NIPS)** – By deploying IntruShield, companies are able to prevent the newest breed of threats from impacting their networks and attached assets. IntruShield prevents exploitation of vulnerabilities from self-propagating worms, zero-day exploits, attacks within SSL encrypted sessions, and attacks directed against the routing or switching infrastructure. By deploying IntruShield all externally facing network segments and critical internal segments, gain an added depth in protection against known and unknown attacks.

**McAfee’s Secure Content Management (SCM)** – By deploying SCM in front of mail servers in the so called “DMZ” organizations prevent the delivery of Malware and malicious content through these mail servers directed at end users.

**McAfee Entercept® Host Intrusion Prevention (HIPS)** – By deploying Entercept on servers and desktops, organizations add an additional layer of protection to critical servers, notebooks, web servers and database servers. It ensures the availability, integrity and confidentiality of business processes by proactively blocking zero-day attacks, buffer overflow attacks, privilege escalation, and applications-specific attacks. Entercept utilizes behavioral rules, signatures and a system firewall to block attacks, reducing the urgency of patch deployment for new threats and giving organizations time to research, test and deploy patches.

**McAfee VirusScan® Enterprise 8.0i** – The next-generation in innovative anti-virus technology.
- **Protection beyond just malicious code and traditional viruses incorporating, Intrusion Prevention technology using provides buffer overflow protection for 23 common Windows desktop applications and processes.**
McAfee Anti-Spyware Enterprise
Anti-Spyware Enterprise users are protected against the newest threats to systems, from not only Spyware but other potentially unwanted programs.

By utilizing each step of the lifecycle and performing the deployment of the right technology for the right problem, any organization can successfully block threats in real time. However, if performed out of order there is a real danger of installing the “right” technology in the “wrong” place based on false assumptions.

Blocking doesn’t result in never having to patch again, rather an organization has the ability to update systems within its own policies and procedures rather than the terms of the vendor issuing the patch. The end result is a “security vulnerability patch” being put in place while operating system or application patches are tested and deployed in a prudent and controlled manner. Previously, the only option available was to immediately release a patch and hope it didn’t adversely affect other operations or assets.

VIII. Step Eight: REMEDIATION
Remediation involves reviewing all of the previous steps and then prioritizing remediation actions, based on discoveries and actions obtained from those steps.

With the proper deployment of process and technology within step seven (BLOCK) this remediation step will be obvious both to understand and execute (although this step is often completed too early in the lifecycle). When an early execution occurs, usually at the time a critical patch is released by a vendor, the result is the wrong protection technologies installed in the wrong place with the patch making no positive effect at stopping the attack.

End-user notification is a key component of Remediation, making sure the policy is available. This allows the end-users to be involved in the remediation of threats impacting them individually or the entire organization.

Keep in mind that not all systems, users, and data are treated equally. In fact, the results of remediation might mandate addressing less critical vulnerabilities on more critical systems, based on the specific attack situation.

Successfully achieving remediation is a directly affected by implementing the prescribed protective technologies discussed in step seven (BLOCK). Patches can then be rolled out in a prudent fashion after testing and scheduling to complete the operations remediation process.

IX. Step Nine: MEASURE
By the time this step has been reached, a certain level of success closing security gaps has been achieved. It is now time to take a measurement of the impact of prior decisions.

After accomplishing this step it maybe found that previously deployed solutions need refinement. Whatever the case, it’s critical that prior actions be measured.

Also, at this point a new, complete, vulnerability scan using Foundstone should be initiated to determine the latest risk score to answer the following questions:

- What impact to critical business systems did prior actions have?
- Were systems and users negatively impacted?
- Is the environment more secure now than when first started?
- Are additional actions necessary?
- Was productivity affected by any actions? Should these actions be curtailed?
- Did the environment change?
- Should additional technologies be deployed?

McAfee Foundstone and ePO
Both have extensive reporting and measurement tools to identify the level of success that’s been achieved to this point, or any point, in the process.

As Foundstone continues to scan for new systems and new vulnerabilities, measurements of the level of remediation will show an increasing level of protection and commensurate decreasing level of risk.

ePO is used to monitor and measure the compliance to security policy and measure the patch level of a system as part of the compliance profiling and measuring of a computing environment.

X. Step Ten: COMPLIANCE
This last step provides the mandatory review of each threat situation and how successfully an organization dealt with that threat. This involves the ability to discover, assess, react, and remediate security related problems. The results of this evaluation allow security managers to
review policy and identify any necessary adjustments in the policy and/or lifecycle process and take action to remediate.

There are many considerations to take into account during a compliance review such as:
- Did actions up to this point align with the security policy?
- Does the policy need to be adjusted based on these findings?
- Did the environment or user-base force additional change?
- Are all systems in compliance with established standards?

New threats, impact or changes to the computing environment or user base, new business systems or applications, or changes in the organization are also items to consider at this point.

McAfee’s Foundstone and ePO products were specifically designed for this purpose, and in association with the complete set of detection and prevention products provide business with the necessary protection for complete business piece of mind. Enforcing compliance includes knowing what assets are on the network (Foundstone), knowing their security level (ePO), and making adjustments or granting permissions based on pre-existing baseline security requirements for system or network access.

Summary
New threats and vulnerabilities are emerging on a daily basis, whether they are focused at a service providers network, a corporations enterprise, specific internal systems, critical data, or end users are inconsequential at this point. The fact is that they exist and are not slowing down forces security professionals to stay up-to-date on not only the latest security threats to their assets, but also the ever changing business priorities for these assets.

They must fully understand their vulnerabilities in order to properly understand their risks prior to deploying any solution that will effectively protect these assets.

By utilizing and adapting the Risk Management Lifecycle, resulting in the implementation of a “Protection-in-Depth” strategy any service provider, business enterprise, government agency, or organization can properly discover, understand, and defend their digital assets against both known and “zero-day” attacks.