



Information Security Metrics

**Using McAfee Foundstone FoundScore to
assign metrics and measure enterprise risk**

Table of Contents

Introduction	3
Why Use Security Risk Metrics?	3
The limitations of a qualitative approach	3
Solution	4
Quantitative risk approach yields results	4
Quantitative vs. qualitative approach	4
Argument for quantitative analysis	4
FoundScore Delivers Comprehensive Quantitative Assessment	5
Internal FoundScore	5
External FoundScore	5
Industry Sectors	6
Uses and benefits of FoundScore	7
Cost reduction	7
FoundScore Flexibility	7
Risk algorithm	8
Conclusion	8
About Foundstone Vulnerability Management Solutions	9
About McAfee Foundstone Professional Services	9
About McAfee	9
Find out how	9

Using McAfee Foundstone FoundScore to assign metrics and measure enterprise risk

Security has always been viewed as a cost center, never typically associated with revenue-driving initiatives. This can make it difficult to get approval for and justify security budgets and expenditures on software, hardware, personnel, services, training, processes, and procedures. To overcome this challenge, many security organizations use a well-established approach called Return on Security Investment (ROSI).

Introduction

The purpose of this white paper is to address the use of reliable metrics in measuring the business value of expenditures and actions taken relative to information security, and effectively communicating this information to the highest levels of the organization. This paper discusses why you should use security metrics to understand risk in your environment, how to use McAfee® Foundstone® FoundScore to track security improvements in the environment, and what the evolution of risk-based management will be in the future.

Foundstone helps companies take control of their digital risk and manage it intelligently and proactively. It provides expertise in strategic security that enables customers to create the right balance of technology, people, and processes for continuous and measurable vulnerability and risk management. Using Foundstone's priority-based approach, an enterprise can reduce risk and protect its critical assets.

Measuring risk with FoundScore makes it possible for customers to quantify progress by assigning measurable values to security, allowing them to demonstrate tangible results for security programs, significantly extending "soft" or qualitative measurements. They can analyze risk objectively, based on three factors:

- Asset values and countermeasures in place to protect those assets
- Threats against those assets
- Vulnerabilities that take advantage of the threats

The FoundScore is a metric that customers can use as a guide for spending and resource allocation, to show specific returns on investments and tangible change measures. Customers can track the metrics over time, benchmarking against industry averages. Companies can also compare the scores of their individual offices, to apply the right security measures to areas of greatest risk to achieve significant cost reductions.

FoundScores are industry-specific, to accommodate different tolerance levels for risk. For example, risk associated with information access might be more important in the financial industry than the healthcare industry, which may be primarily concerned with confidentiality and integrity. Calculations for measuring risk can also differ by sector. Because McAfee tests a variety of companies, it can create a quantitative list of FoundScores for use as a yardstick for each industry.

Why Use Security Risk Metrics?

In tighter economic climates, it can be extremely difficult to justify the cost of new technologies. Implementing security technologies does not translate to direct revenue generation; therefore, security professionals must use other means of analysis to substantiate expenditures.

Security metrics help shift from purely qualitative values to significant numerical measurements. A qualitative approach is subjective ("What is my company's reputation worth?"), while a quantitative approach uses hard numerical values to measure security risks and return on investment.

The limitations of a qualitative approach

In the past, the effectiveness of security spending has used soft measurements—factors such as the size of a security staff relative to that of the annual budget, or by the speed of resolution or patches based on new vulnerabilities or viruses. This left a large gap, because it didn't demonstrate cost savings of preventing digital attacks. The method was reactive, and not quantifiable. For example:

Scenario A: An outdated approach to security

Assets, threats, and vulnerabilities:

- **Asset**—The public can reach your company's web servers and potentially attack them

- **Threat**—A new vulnerability is released that targets web servers
- **Vulnerability**—The exploit is immediately released to the public and your web server is vulnerable. The IT team can only react when something actually occurs. The intrusion detection/prevention system alerts you after an actual break-in to the server, stimulating a reaction

Solution

The IT/security team patches vulnerable servers as needed. Problems with this solution:

- The IT/security team is not proactive
- The IT/security team can apply individual patches to fix vulnerabilities, but they have not addressed the overall security posture of the environment
- The value of the web servers is unknown, resulting in the application of too many or too few security resources; there is no value measured in dollars of the servers, nor risk ratings applied to the assets
- The IT/security team makes changes on an ad-hoc basis
- It is difficult to measure the results of changes

Quantitative risk approach yields results

ROSI fills this measurement gap, providing a necessary, quantifiable approach. Many security organizations use it as the approved method for calculating the value of security investments in total dollars saved. Organizations can calculate it by linking specific security products to numerical measurements of their security posture. For example, if you purchase a firewall, how will it affect your overall security status? Can you show that you saved a specific dollar amount because you weren't exploited after the latest web server vulnerability was discovered, and therefore didn't lose any downtime or sales? ROSI delivers these answers.

Using a strategic, risk-based approach, such as that offered by Foundstone, an organization presented with Scenario A will dedicate resources—through constant monitoring and analysis—to high-risk areas, defined by the importance of the assets. The web server is the asset, and it may be deemed “high risk” and thus require greater security measures. A practical approach will have an organization test the security of the web servers in advance so that it can find and fix any weaknesses before they are exploited. By knowing up front the level of risk to each of your assets, either by assigning a dollar value or by specifying a criticality rating, you can quantify the security measures, and implement the appropriate level of security.

Quantitative vs. qualitative approach

Quantitative approach: Use of numerical values assigned to assets to measure risk

Quantitative Approach to Measuring Risk

PROs	CONS
• Results based on objective measurements	• Calculations can be complex
• Monetary value assigned to risk and security measurements	• Significant up-front time and effort required to assign risk ratings to assets
• Comparisons of security posture over time can be calculated	• Industry standards for risk and return have not yet been set
• Risk management measures can be tracked over time	
• Resources can be dedicated to high-risk areas	
• Return on investment on security solutions can be measured and tracked	
• Business impact analysis can be performed	
• Comparison to industry standards can be performed	
• Management can understand dollar costs of security based on risk	

Qualitative approach: Use of subjective values to assign resources to potential risk

Qualitative Approach to Measuring Risk

PROs	CONS
• Easy calculations, if any, are used	• Results are purely subjective
• Monetary value does not have to be used	• Resources can be deployed in the wrong area
• Measuring threats and countermeasures is not necessary	• No way to calculate monetary value of implementing security measures and results
• Cost of countermeasures does not need to be measured relative to threat	• Cannot analyze cost/benefits
• Generalizations about risk can be made and acted upon quickly	• No objective way to identify risk
	• Cannot analyze business impact

Argument for quantitative analysis

To quantify security measures, you assign a risk rating to each measure, and assign values to each asset and function. Assigning risk ratings is done in a risk analysis. What is the level of risk associated with your finance department's subnet versus your test environment subnet? What is the level of risk associated with your online banking application server versus your internal intranet server? By assigning criticality values to your assets, you can then begin to

determine the level of risk to each asset and the value of the countermeasure that protects that asset.

Measuring security implementation means mitigating risks where possible and focusing finite security dollars on the right countermeasures. To justify the risk countermeasure, you need to quantify (in dollars) the risk ratings and the value of an asset.

Security metrics change in three ways:

- Over time—Every environment changes. Changes come in all forms, such as the introduction of new vulnerabilities, when new services come online, and when new systems come online. Security is a moving target, so measuring your security posture on a daily basis via metrics will enable you to see real-time security changes in your environment
- By industry—Each industry values data and resources differently. For example, security measures in the financial industry may not be as important in the manufacturing industry. By determining the risks relative to your industry, you can develop realistic methods of measuring the security posture of your organization
- By action—The countermeasures that are in place to mitigate risk affect the overall risk rating. With more or fewer countermeasures, your security posture changes. By understanding how each technology, process, and procedure affects your security posture in a numerical fashion, you can dedicate resources to the most cost-effective countermeasures where they'll have the greatest impact

FoundScore Delivers Comprehensive Quantitative Assessment

FoundScore is a security rating system that compares aspects of your environment against best practices in order to quantify your security risk. McAfee Foundstone Enterprise tests your global network for vulnerabilities and generates a FoundScore. With these scores, you can see how your security efforts change over time, and can track the impact of those efforts.

Foundstone Enterprise measures FoundScore in two ways, depending on whether it is assessing an internal or external network. The risk of particular vulnerabilities or exposures that exist on an internal network may be completely different when those same items exist in an Internet-facing network.

Foundstone Enterprise also takes into account asset criticality when measuring FoundScore. For example, if it finds a medium-risk vulnerability on an asset that is considered highly business-critical, such as an accounting server, the point deduction for FoundScore will be greater than if that same vulnerability was found on a non-critical asset such as a test server.

Internal FoundScore

Internal FoundScore is divided into two components:

Vulnerabilities 70 points—Based on the combination of high-, medium-, and low-risk vulnerabilities discovered within your environment, Foundstone assesses you a score between 0 and 70 points. Foundstone deducts points for each vulnerability found based on its risk ranking (high, medium, and low).

Exposure 30 points—A rating of how exposed your network is to Internet threats based on generally accepted security principles. A total of 30 points are possible. Foundstone deducts points for each violation in three categories.

The attributes of your environment that are assessed to determine your overall FoundScore rating (vulnerabilities + exposure) are as follows:

Does your environment possess vulnerabilities that attackers can exploit to harm your systems and/or gain unauthorized access?

Are there wireless access points in your environment that attackers can compromise?

Are any Trojan ports open on any machines in your environment?

Are any rogue or commonly prohibited applications (e.g., instant messaging applications, peer-to-peer data-sharing applications, etc.) running in your environment?

External FoundScore

External FoundScore is divided into the same two components:

Vulnerabilities 50 points—Based on the combination of high-, medium-, and low-risk vulnerabilities discovered within your environment, you are assessed a score between 0 and 50 points. Foundstone deducts points for each vulnerability found based on its risk ranking (high, medium, and low).

Exposure 50 points—A rating of how exposed your network is to Internet threats based on generally accepted security principles. A total of 50 points are possible. Foundstone deducts points for each violation in three categories.

The attributes of your environment that are assessed to determine your overall FoundScore rating (vulnerabilities + exposure) are as follows:

Does your environment possess vulnerabilities that attackers can exploit to harm your systems and/or gain unauthorized access?

Does your environment possess non-essential network services that increase the possibility of a security breach?

Are there machines in the environment that do not perform a function necessary to support normal Internet operations?

Do you permit inbound UDP traffic to your network (other than DNS traffic on port 53)?

Do you permit inbound ICMP to your network?

The comparison of your network against the five criteria listed above provides you a quantitative view of your environment's security risk. Within the FoundScore system, a network starts with a full 100 points. For each violation, FoundScore deducts a number of points. Thus, a higher

score reflects a network environment that is inherently less risky. A lower score indicates that your environment possesses more security weaknesses and consequently more risk. The highest score possible is 100, the lowest score is zero. The table below indicates the qualitative ratings assigned to the range of possible scores.

Score Range	Ranking
0–26	Poor
26–50	Below average
51–70	Average
71–85	Above average
85–100	Excellent

Industry Sectors

By collecting security information across a variety of industries, McAfee can provide a baseline model to compare the security of your enterprise to that of peers within your industry. The industries that we track most loosely include the following:

- Broadcasting
- Entertainment
- Financial
- High technology
- Insurance
- Manufacturing
- Professional services
- Utility

Because McAfee tests a variety of companies, we can create benchmarks for each industry, using a list of FoundScores. Using McAfee as a central repository of industry data, you can depend on an objective third party to assist you in comparing your security posture with those in your industry as well as other industries, all through completely anonymous functions. Chart 1 shows the average FoundScores of some of the industries we analyze. We extracted these averages from approximately 53,000 FoundScores generated from scanning over 1.6 million hosts.

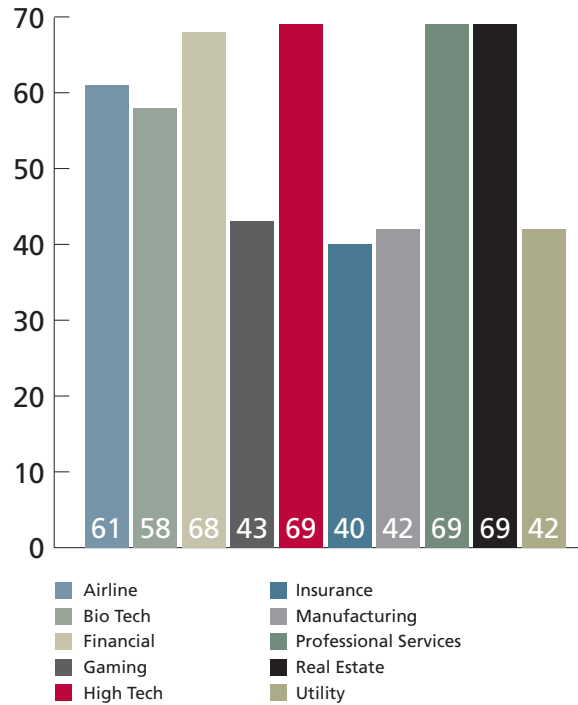


Chart 1: Industry average FoundScores

Individual organizations can track their own FoundScores over time. In the example shown in Chart 2, the FoundScore varies wildly in the date range of systems scanned. If this were a financial organization, we could compare the FoundScore average of an individual company, 78, against the financial industry average of 63.

This organization has a better FoundScore than its industry average, and the FoundScore indicates that the company vulnerability rating falls into the “above average” category.

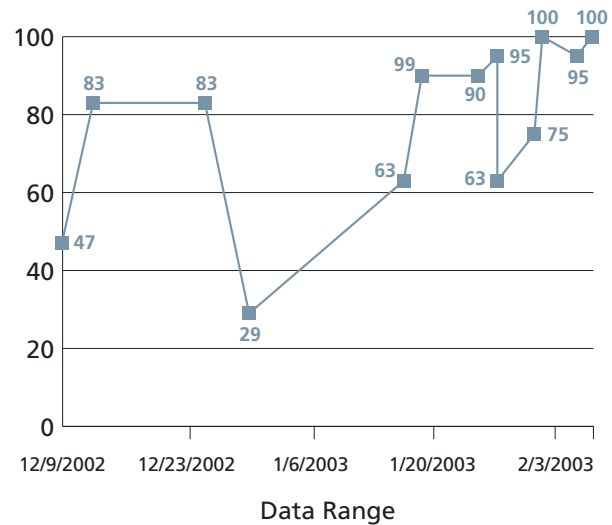


Chart 2: Individual organization's FoundScore

Practical application of FoundScore: a case study

Current Foundstone customers use their FoundScore effectively in a variety of ways. This section details how a multi-national organization can use the solution to assess and correct its security backbone.

Uses and benefits of FoundScore

Customer	Multi-national with remote offices all being assessed with Foundstone Enterprise
Comparisons	<ul style="list-style-type: none"> • Compare FoundScore between offices • Compare cumulative FoundScore for the entire organization within an industry • Compare FoundScore relative to other industries • Track FoundScore changes as a new vulnerability is released in the public domain • Track FoundScore changes as a new virus is released in the public domain • Track FoundScore over time as patches and fixes are implemented
Benefits	<ul style="list-style-type: none"> • Upper management can see tangible changes in the security posture of the organization relative to security spending • Managers can see tangible results as a single metric, showing the effectiveness of proactive measures that are being taken to reduce risk • Security posture of different offices can be compared • The effectiveness of the IT staff in remediation of vulnerabilities across different offices can be compared and assessed • Cost reduction can be gained by focusing resources on correct and productive security measures • MBO metrics can be set using FoundScore as a measure of how effective security becomes over time

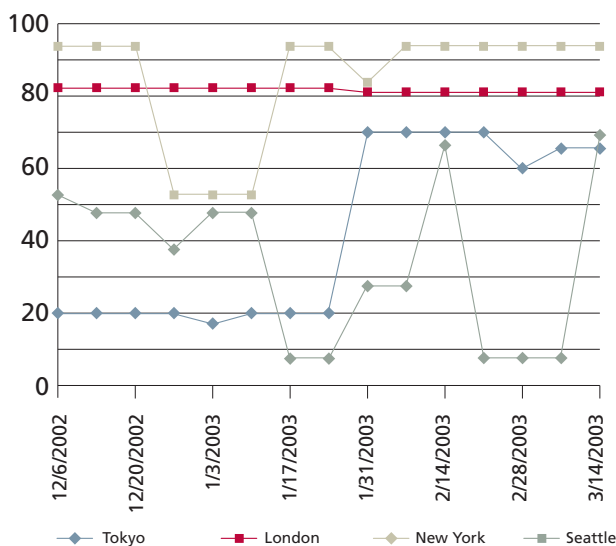


Chart 3: Office comparison of FoundScores

Chart 3 compares the FoundScores of different offices in the example organization.

This chart shows a wide variety of security postures in various offices, illuminating important issues for the company to address.

- The only consistent office results are from London. Why is there such a big range in results for the other offices?
- New York has the highest FoundScore rating except for a period of approximately three weeks. What happened there?
- Seattle has the greatest rate of change in their security stance. Why?
- Tokyo saw vast improvement in their security stance, but hit a plateau at 60. Why didn't it continue to get better?

By asking similar questions based on the FoundScore results, a security administrator can get to the heart of the cause for changes in the security posture and determine why improvements are not being made.

The major benefit in measuring and comparing FoundScores is the ability to determine where security measures are most effective. First we can determine the area of greatest weakness as shown by a low FoundScore. Chart 3 tells us that the organization's Seattle office has very poor FoundScores; therefore, an analysis should be conducted to decide the solution.

Cost reduction

By conducting a risk analysis, the company can determine what its exposure is in the Seattle office. It could be that the network in this office has been cordoned off from other offices, or that there are no assets in that network critical to the financial success of the organization. This information tells us that it would be more effective to spend security dollars on another office, such as the Tokyo office, which stores all the research and development material. If the Seattle office does have valuable resources, such as accounting servers, the low FoundScore tells us this is a very high-risk office. The sample organization could then increase the allocation of security dollars to the Seattle office and reduce it in another office, such as New York, which is very secure already.

By tying dollar costs to assets, the organization can know its true asset values. The FoundScore then shows the organization which assets have the greatest risk and potential dollar loss, and so it can distribute budgets effectively.

FoundScore Flexibility

McAfee FoundScore also provides great flexibility for a unique environment. FoundScore has the ability to allow organizations to create a custom risk score called "MyFoundScore." This capability allows organizations to modify risk-scoring criteria and risk weightings to more closely match the specific information security policies of

the organization. One organization may value particular vulnerabilities differently than the ratings of the default Foundstone system. Another organization may decide that inbound ICMP traffic is perfectly acceptable to external networks. By providing a customizable risk-scoring mechanism, MyFoundScore can reflect the risk rating of the organization specific to the acceptable security policies of that organization. An organization may also compare the MyFoundScore value with the baseline of the Foundstone FoundScore to see how risk ratings and perception differ from the industry perspective.

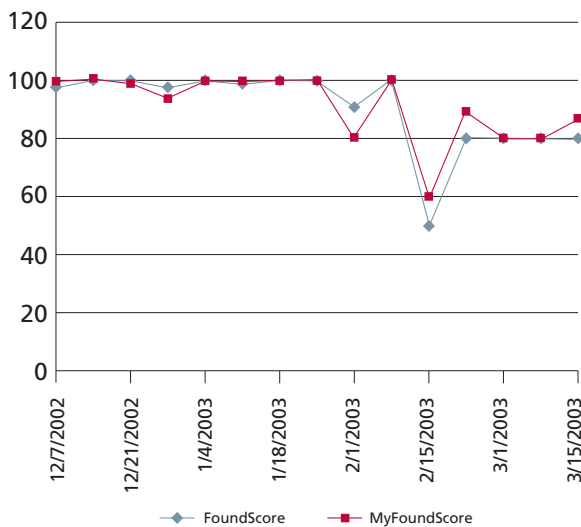


Chart 4: Comparison of the FoundScore versus modified MyFoundScore

In Chart 4, the FoundScore and MyFoundScore closely match, but there are some differences. In this example, the company views several risk factors differently from the Foundstone Enterprise risk solution. By being able to modify the risk weightings to more closely meet your environment, you can get a clearer picture of how your organization views risk.

Risk algorithm

There is a risk algorithm that Foundstone Enterprise uses to quantify the value of assets, threats, vulnerabilities, and countermeasures. By applying a mathematical formula to these components, the risk algorithm can measure risk and dollar costs of every aspect of security within the enterprise. By assigning a risk rating and dollar cost based on risk, you can theorize how changes in the environment will affect security and the cost of security. Linked to the FoundScore, this risk algorithm provides a unique automated measurement of risk throughout the enterprise.

The risk algorithm measures the following:

- **Asset**—Any function, task, capability, equipment, or information that has value to the organization or supports the ability of the organization to conduct business
- **Asset countermeasure**—Any processes that facilitate replacement or provide equivalent service if an asset is lost, unavailable, or damaged
- **Threat**—Any person, circumstance, or event that has the potential to cause damage to an organizational asset or business function
- **Threat countermeasure**—Any process, procedure, product, feature, or function that will restrict or block access, deter, or lower the occurrence of a threat within the specified environment
- **Vulnerability**—Any flaw in the design, implementation, or administration of a system that provides a mechanism for a threat to exploit the weakness of a system or process
- **Vulnerability countermeasure**—Any process, procedure, product, feature, or function that will eliminate, reduce the impact of, or change the exposure for the vulnerability

Conclusion

The need for quantifiable measurements of risk is slowly being realized in security departments of both large and small organizations. These organizations want to take control of their security risk and be able to communicate improvements tangibly throughout the company. Everyone from the CIO to the IT manager needs a method of calculating the cost of new security technologies, processes, and procedures, as well as the price paid for security measures not taken. FoundScore lets you apply a numerical measure to risk that can be translated into implemented security measures and real dollar savings.

Using FoundScore over time to track changes in security posture can demonstrate a real ROI. By proving that security initiatives directly impact the organization and save money, budgeting for security will be an easier process.

It is now also possible to examine how your organization's security posture compares with others in the same industry. With an objective third party such as Foundstone, you can compare your risk rating against industry peers to determine where you stand as an organization. Internally, you can compare how various offices compare in terms of individual FoundScores and adjust accordingly. This provides a clear advantage above your competitors.

Actionable security measures show tangible results. By monitoring the changes in your FoundScore as you implement new security measures, you can see what has

the greatest impact on your environment. By protecting the right assets from the right threats with the right countermeasures, Foundstone helps you use your finite security dollars in the best way possible.

About Foundstone Vulnerability Management Solutions

Foundstone Enterprise allows you to reduce business risks from vulnerabilities and threats with a priority-based solution that automates, integrates, and simplifies vulnerability management for medium and large enterprises.

About McAfee Foundstone Professional Services

Foundstone provides updated services and education programs to help you respond to your organization's ever-changing security demands.

- Business security consulting—We thoroughly diagnose your current security posture and lay the foundation for a program to address your current and future needs
- Technology security consulting—Our experts uncover vulnerabilities in your network and applications and recommend ways to fortify your defenses
- Education courses—We offer world-class training for everyone involved in security, from technical staff to management

About McAfee

McAfee, Inc., proactively secures systems and networks from known and as-yet-undiscovered threats. Our customers and partners trust our unmatched security expertise and have confidence in our comprehensive and proven solutions to effectively block attacks and prevent disruptions.

Find out how

Find out how Foundstone vulnerability management can help secure your organization. Please visit us on the web at <http://www.mcafee.com>, email sales@mcafee.com or call 1-888-847-8766 for more information.