



# **GENERATING VALUE WITH CONTINUOUS SECURITY TESTING AND MEASUREMENT**

**A Spire Research Report**  
Sponsored by Core Security Technologies

## Executive Summary

Efficiency and effectiveness are key tenets in managing any business group. In security, these concepts revolve around managing resources and risk. It is crucial to measure a security program to understand how efficient and effective it is.

There are four key challenges to traditional penetration testing that can make it inefficient and ineffective: 1) only a fraction of the enterprise is tested, 2) the testing cycle is too long, 3) nobody cares about the two thousandth vulnerability, and 4) nobody does the re-test. These obstacles create an opportunity for a paradigm shift to a continuous security testing approach.

Continuous security testing provides a framework for higher efficiency and effectiveness by prioritizing information assets and assessing the technical architecture that facilitates access to them.

Return on investment (ROI) measures the change in spending between two functionally-equivalent approaches to security management.

Return on security investment (ROSI) measures the reduction in risk compared with the resources used to get there.

There are opportunities for optimizing resources and reducing risk with continuous security testing which rethinks traditional penetration testing from a new perspective.

### About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," a security reference model that incorporates and relates the functions of identity management, trust management, threat management, and vulnerability management. Spire's objective is to help refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by Core Security Technologies. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and risk management experience.

# GENERATING VALUE WITH CONTINUOUS SECURITY TESTING AND MEASUREMENT

## Table of Contents

INTRODUCTION: JUSTIFYING SECURITY INVESTMENTS	I
EFFICIENCY AND EFFECTIVENESS IN CONTINUOUS SECURITY TESTING	I
THE ROI OF CONTINUOUS SECURITY TESTING	2
ROI in Brief	2
Getting to ROI with Continuous Security Testing	2
THE ROSI OF CONTINUOUS SECURITY TESTING	3
ROSI in Brief	3
Getting to ROSI with Continuous Security Testing	4
SCENARIO 1: LARGE FINANCIAL SERVICES CO.	4
SCENARIO 2: MID-SIZE BUSINESS	5
SPIRE VIEWPOINT	6

## Introduction: Justifying Security Investments

Is your security program efficient and effective? This is a fundamental question and yet extremely difficult for many security professionals to answer. In part, this is the nature of risk – when you are completely successful nothing happens. And even if some incident does occur, it doesn't necessarily mean that the program was at fault – reducing risk from a 1 in 10 chance to 1 in 1,000 still leaves that 1 chance to go wrong. Unfortunately, it can be challenging to determine whether any outcome is a matter of luck or skill. Measuring our program can provide key insight in dealing with this problem.

The initial question was more than rhetorical – efficiency and effectiveness are the two overall objectives for running a business unit. Management expects leaders to be efficient by optimizing their resources (people and technology) and providing services at the lowest possible cost. Similarly, there is an assumption that this activity is also effective; that it will lead to the highest quality of service available.

In information technology (IT) security, efficiency and effectiveness are established by “optimizing” risk – reducing risk to its lowest level given the amount of resources invested in the program. So the goal is to minimize the cost of any discrete security function and to ensure that it leads to the lowest likelihood of negative outcomes, or risk.

## Efficiency and Effectiveness in Continuous Security Testing

Mature security departments recognize the functional need for constant diligence in their testing of systems (networks, web applications and client machines). The challenge is determining whether the testing group is operating at its highest level of efficiency and effectiveness. Without benchmarking and the requisite metrics, it is extremely difficult to determine whether this is true. Sometimes, this requires a paradigm shift in how to approach a problem.

Consider penetration testing. A traditional goal in pentesting is simply to “break into a system” without anything but cursory consideration of the actual information assets at risk. While the pen tester is performing as expected, there are four factors that contribute to overall inefficiency and ineffectiveness:

1. Only a fraction of the enterprise is tested. Technical environments today are simply too large to be tested in a single project.
2. The testing cycle is too long. Trying to match up the frequency of tests against specific systems with the changes to the threat and vulnerability state of those same systems just doesn't scale.
3. Nobody cares about the two thousandth vulnerability. Once a test is complete, the typical organization directly addresses some small subset of the

vulnerabilities identified - typically, the highest risk ones. So the work performed finding the others, while not completely useless, is of lower value.

4. Nobody does the re-test. It is good work to conduct a penetration test and report on system risk, but the risk must be addressed (i.e. vulnerability fixed) and then validated to actually gain effectiveness.

Now consider a different approach: continuous security testing. This approach is concerned not so much with the systems but with individual information assets (and sometimes IT resources) that are being protected. It then takes into account *all* of the systems – applications, networks, servers – connected in a dynamic environment and develops a prioritized plan of attack (pun intended) to assess the risk in the organization.

Continuous security testing creates an opportunity for higher levels of efficiency and effectiveness in organizations by addressing the highest risks at the lowest costs. One simple way of measuring efficiency is using return on investment (ROI). Similarly, measuring effectiveness is possible using return on security investment (ROSI).

## The ROI of Continuous Security Testing

Return on Investment (ROI) measures the change to net income for an organization relative to some investment of resources. It is calculated by capturing and comparing the known capital and operating expenses associated with both “before” and “after” investment scenarios (we hold revenue constant given that it doesn’t change).

### ROI in Brief

The formula for ROI is a typical “return” formula – subtract the investment amount from the anticipated cost savings and divide by the investment amount:

$$\frac{\text{Cost Savings} - \text{Investment}}{\text{Investment}}$$

Of course, this means that an investment of \$100,000 should return at least that much money - and typically more - through its lifetime. If, for example, this \$100,000 investment results in cost savings from a previous scenario that cost \$120,000, then the ROI is  $(\$120,000 - \$100,000) / \$100,000 * 100 = 20\%$ .

### Getting to ROI with Continuous Security Testing

A continuous security testing program generates ROI by reducing the costs associated with individual tests in a pentesting program. It leverages software to provide significantly greater scale than a manual program.

Continuous security testing changes the paradigm. Rather than running discrete, point in time tests that focus on platforms, an organization can run ongoing tests that focus on risks to high-value information assets.

The move from a platform-centric penetration test to an information asset (and consequence) based approach means that the number of discrete tests can be

significantly reduced or made more productive in favor of the all-inclusive continuous testing of the environment.

While there might be some reduction in cost per test with a manual program as employees get proficient or discounts kick in, the typical program inevitably hits a roadblock due to resource shortages. Continuous security testing significantly reduces the variable costs of a test so that every time the software is used, the cost per test is reduced. And the roadblock comes much later on.

The typical penetration test is scoped against a set of IT assets so that it can be completed in 2-4 weeks at a cost somewhere between \$40,000 and \$100,000. A large organization might perform 10-30 of these a year for a total cost somewhere between \$400,000 and \$3 million.

With a continuous security testing solution, a \$250,000 investment is likely to cover those same tests and provide an opportunity for fuller coverage as well. In the conservative scenario, a \$250,000 investment to accomplish what usually costs \$400,000 reveals an ROI in the neighborhood of 60%.

$$\$400,000 - \$250,000 / \$250,000 = .6 \times 100 = 60\%$$

In addition to this ROI, an organization can perform more tests over and above the usual, providing coverage of the entire environment at higher frequency and extremely low marginal cost.

## The ROSI of Continuous Security Testing

Return on Security Investment (ROSI) is a concept that many confuse with ROI, but it is different. ROSI recognizes that the security professional's prime directive is to minimize risk with the resources available.

### ROSI in Brief

More specifically, "minimizing" risk involves reducing the likelihood of specified consequences - for example, reducing the likelihood of a \$1,000,000 loss from 20% to 10%. ROSI compares the difference in expected value between the two scenarios to the investment required for the reduction benefit. In the example, the risk is lowered from \$200,000 (\$1m \* .2) to \$100,000 (\$1m \*.1) for a difference of \$100,000.

The ROSI calculation is similar to the ROI measure except that the actual cost savings figure is replaced by the risk reduction amount:

$$\frac{\text{Risk Reduction} - \text{Investment}}{\text{Investment}}$$

If it takes an investment of \$75,000 to accomplish the \$100,000 risk reduction in our example, then, gives us a 33% ROSI  $(\$100,000 - \$75,000) / \$75,000$ .

## Getting to ROSI with Continuous Security Testing

Continuous security testing reduces the likelihood of compromise when it assists in identifying the highest-risk vulnerabilities based on the state of the threat. This translates to providing more current information on the vulnerable state of the environment while factoring in new threats on an ongoing basis.

Risk is reduced when the timing associated with penetration testing more closely matches the frequency of changes in the configuration of platforms in the environment and the new vulnerabilities and attack techniques available to the general public.

## Scenario 1: Large Financial Services Co.

Large financial services organizations have their own penetration testing teams or have outsourced testing and integrated it into security operations. In this scenario, a ten-person team tests five applications, plus associated systems and platforms, per month for a total of 60 penetration tests in a year. In an organization with 300 applications, the average application will theoretically be tested once every five years – though, in reality, high-risk applications will be tested annually while others may never be tested.

### ROI

The company incurs a salary expense at about \$1.2 million per year and invests \$100,000 for software licenses plus 20% maintenance over a five year lifetime for an annual cost of \$40,000. Any new investment must be lower than \$1,240,000 to reduce the costs associated with penetration testing.

Continuous security testing reduces the manual overhead associated with testing so that two people are required to run the system at an annual cost of \$240,000. The other eight people are allocated to remediation functions. Software licenses and maintenance run to \$300,000 annually for a total expenditure of \$540,000.

The total costs for the pentesting program are reduced from \$1.24 million down to \$540,000 for a reduction of \$700,000. This \$700k provides an ROI of 130% of the total \$540,000 cost of the program.

Category	Current	Proposed
Labor Expenses	\$1,200,000	\$240,000
Software Licenses	\$40,000	\$300,000
<b>TOTAL</b>	<b>\$1,240,000</b>	<b>\$540,000</b>
<b>Return on Investment</b>	<b><math>\frac{(\\$1,240,000 - \\$540,000)}{\\$540,000}</math></b>	<b>ROI = 130%</b>

Table 1: Return on investment calculation for scenario 1.

## ROSI

On the risk side, continuous security testing reduces estimated risk from one incident every five years (20%) to one incident every twenty years (5%). Total consequences are estimated in the area of \$10 million for a single incident and therefore risk is reduced from \$2 million down to \$500,000 annually.

Comparing the \$1.5 million reduction to the aforementioned \$540,000 expenditure for the program, the ROSI comes in over 275%.

Category	Current	Proposed
Estimated Likelihood	20%	5%
Consequences	\$10,000,000	\$10,000,000
<b>TOTAL RISK</b>	<b>\$2,000,000</b>	<b>\$500,000</b>
<b>Return on Security Investment</b>	<b><math>\frac{(\\$2,000,000 - \\$500,000)}{\\$540,000}</math></b>	<b>ROSI = 278%</b>

Table 2: Return on security investment calculation for scenario 1.

## Scenario 2: Mid-Size Business

Our second scenario involves an outpatient medical center. This organization has 30 applications that must be audited annually to meet regulatory requirements. They outsource the application reviews to a consultancy that has agreed to conduct each audit annually for \$15,000.

## ROI

Since the entire penetration testing exercise is outsourced, total costs are \$450,000 to complete the 30 audits annually. A continuous security testing solution would require an additional FTE (\$100,000) plus the cost of the software - \$150,000 plus 20% maintenance over five years for an annualized \$60,000. Costs are reduced from \$450,000 down to \$160,000 for an ROI of 181%.

Category	Current	Proposed
Labor Expenses (outsourced)	\$450,000	\$100,000
Software Licenses		\$60,000
<b>TOTAL</b>	<b>\$450,000</b>	<b>\$160,000</b>
<b>Return on Investment</b>	<b><math>\frac{(\\$450,000 - \\$160,000)}{\\$160,000}</math></b>	<b>ROI = 181%</b>

Table 3: Return on investment calculation for scenario 2.

## ROSI

The organization estimates the possible losses at over a million dollars. Running a continuous security testing tool reduces risk from once every four years (25%) to once every six years (17%). Comparing the \$80,000 reduction to the investment of \$160,000 leaves an ROSI of 50%.

Category	Current	Proposed
Estimated Likelihood	25%	17%
Consequences	\$1,000,000	\$1,000,000
<b>TOTAL RISK</b>	<b>\$250,000</b>	<b>\$170,000</b>
<b>Return on Security Investment</b>	<b><math>\frac{(\\$250,000 - \\$170,000)}{\\$160,000}</math></b>	<b>ROSI = 50%</b>

Table 4: Return on security investment calculation for scenario 2.

## Spire Viewpoint

Continuous security testing is a new way to think about penetration testing in the same way that batch processing gave way to transactional, real-time processing in supply chain management. The idea is to provide a solution that scales (reportedly on a level 10x greater than traditional pentesting) so that not only is there a cost savings ROI but also significantly reduced risk and higher associated ROSI.

## Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at [www.spiresecurity.com](http://www.spiresecurity.com).

This white paper was commissioned by Core Security Technologies. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.