# Business Enablement with On Demand Vulnerability Management

## A Spire Research Report – June 2004

By Pete Lindstrom, Research Director

Spire Security, LLC
P.O. Box 152
Malvern, PA 19355
www.spiresecurity.com

# Executive Summary

Enterprises that care about security have long been conducting vulnerability management activities to minimize the exposure to systems in the computing environment. The traditional annual audit of a sample of systems has given way to continuous scanning that detects the latest vulnerabilities. This is true due to the rise of "Internet time" along with increased business risk.

In today's global environments, conducting scans can be difficult to say the least. An on-demand service gives the vulnerability management process global coverage, high accuracy, fast deployment, and low overhead.

This white paper discusses the challenges of security in today's business world and provides insight into the value of an on-demand Web-based service for vulnerability assessment. It closes with summary information and feedback regarding the QualysGuard service, as compiled from Qualys customers.

## 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 Qualys. All content and assertions are the independent work and opinions of Spire Security - the product of years of security audit, design, and consulting work.

# Business Enablement with On-Demand Vulnerability Management

## Table of Contents

# Introduction

The amount of risk facing any IT infrastructure is constantly in flux. Any change to a system or its broader computing environment also changes its security posture. New application deployments, upgraded servers or equipment, and modified architectures all are examples of changes that affect security. We secure our infrastructures by evaluating the security posture of our systems  and then taking calculated actions to remediate any problems that increase the likelihood of compromise.

One of the more strategic ways to reduce the risks against systems is through regular network security audits. A critical component of these audits is the practice of identifying vulnerabilities and taking the appropriate steps to correct these weaknesses before they can be exploited. Vulnerability management makes it possible for a company to take proactive steps to spot rogue devices, identify vulnerabilities, and help best configure defensive system policies for its firewalls and intrusion detection systems. Most importantly, these regular audits help answer the larger questions asked by security professionals and management alike – “Is our network secure?” and “ Where are our weaknesses?”

# Security Challenges in Today’s Computing Environments

Effectively every organization understands the need for firewalls and antivirus and has deployed them in their environments. And yet, with these controls in place, the limitations of these basic layers of security are constantly being highlighted – primarily, their reactive nature in dealing with threats. Today’s fast-moving viruses and worms have found ways to pass through firewalls and bypass anti-virus applications to infiltrate and pinpoint their attacks against the fundamental weakness -- the network vulnerability.

According to the Computer Emergency Response Team (CERT/CC), there was an average of over 10 vulnerabilities found every day in 2003 (3,784 in total). Regardless of the number, it is clear that with software and networks becoming more complex, more vulnerabilities will continue to be found on an ongoing basis. With this volume of vulnerabilities being found, the latency period between assessments becomes a factor in security, and monthly or weekly frequencies are often insufficient. A secure network last week may be significantly at risk this week if newly announced vulnerabilities are not quickly detected and resolved.

An enterprise security posture is affected by many factors, the most important being:

## New components of distributed architectures

Standardization and plug-and-play flexibility comes at a price – every standardized communication point is also a uniquely addressable attack point; a target at which a hacker can aim his exploit. As we componentized our architectures – storage, databases, application servers, print servers, and individual programs – we must constantly evaluate the exposure of these new attack points.

## Dynamic changes to networks and applications

Changes to networks and applications are increasingly dynamic, resulting in an increase in system complexity. We are beginning to consider autonomic and utility computing, that virtualize processes across many components. This complexity contributes to the degree of confusion and insecurity in an environment. As we build out our "anytime, anywhere" infrastructure, we must ensure that proper controls remain in place.

## Multiplying network access points

Network access points are multiplying, with remote access VPNs and wireless access points leading the way. Employees and business partners are accessing networks from more entry-points now than ever before, and these access points increase the number of ways in which viruses, worms, and attackers can access networks.

Firewalls and antivirus solutions are important parts of an effective security program, but companies today must understand their network, understand where there are weaknesses, and protect their most important assets first. Simply relying upon firewalls and antivirus solutions is not an effective security program. Understanding the network and understanding its weaknesses provide insight needed to protect critical data from the multitude of access points.

# Toward Business Enablement

Vulnerability management is not a new practice – auditors have been performing system audits for over twenty years. But today's architectures require continuous, comprehensive auditing rather than a periodic sampling of systems. The real-time nature of this new style of assessment leads to strategic benefits for business enablement. Consider the following scenarios:

## Offshore Outsourcing

Companies are increasingly looking offshore for software development, outsourced call centers, and other services. Enterprises look to contract for services from businesses in countries such as India, Russia, and Pakistan. While cost savings may be beneficial, the corresponding risk also increases when data is shared with the business partner. A vulnerability management solution can be leveraged to provide extra comfort that an extended network environment is properly protected and suppliers are adhering to security standards.

## Mergers and Acquisitions

As the economy strengthens, capital becomes available for use in M&A activities. Vulnerability assessments are extremely useful in these activities. During the due diligence phase, audits provide insight into the level of control over the financial systems and determines the depth of accounting testing required. After a merger, assessments help with the integration of computing systems.

## Service Providers

Making your own organization's assessments available for review, as part of a SAS70 audit, for example, provides an opportunity to be the outsourcer to others. An audit service provides prospects and clients with a record of the security profile of the organization and is indicative of the attention being given to security. This increased comfort level also leads to increased business.

New business opportunities pair with increased risk to make security a board-level issue. Data compromise or system downtime leads to lost business and limits the global opportunities of an enterprise. On-demand vulnerability management provides the proactive foundation for this enablement. Implicit in the "always on" strategy is ease of use and management. This is where an on-demand Web-based service fits in.

# On-Demand Vulnerability Management

Delivering a service over the Web is a strong technique for meeting the needs of today's global enterprises. Inherent to the Web-based service are characteristics that are key for the always on environment. These characteristics are discussed here.

## Global Coverage

Internet services eliminate the notion of geography from a discussion about breadth of coverage. Services can span to any place that is connected, providing a service with a level of scalability and breadth of coverage that is difficult to match with a product offering.

## High Accuracy

Obviously, accuracy is crucial for vulnerability management to maintain productivity levels and limit exposure. Any false positive or negative due to incorrect signatures or outdated software creates more work and higher risk for an enterprise. The service gets its accuracy from a consolidated team of developers that can quickly create and push out software updates to fix bugs and also create new signatures to detect newly-identified vulnerabilities.

## Fast Deployment

When you want it done, you want it done immediately. Services make deployment and growth of coverage a trivial exercise having more to do with the contractual obligations and financial considerations than the traditional obstacles associated with technology product deployment.

## Low Overhead

Mobilizing a support team to deploy a new solution, upgrade software, or maintain underlying components like databases and operating systems can be a difficult task.

A service takes the overhead issue away by absorbing all responsibilities and tasks associated with it.

# Qualys: in the Trenches

Spire Security interviewed a number of Qualys customers to address how these characteristics of proactive network auditing and vulnerability management in an on-demand service applied to their experiences with the QualysGuard service.

Using a Web-based service for vulnerability management provides a significant value proposition for meeting the needs of business enablement. Qualys has been in the vulnerability management business since 1999 when it saw the increased need for vulnerability management and understood the limitations of software-based tools to address the growing need of security professionals. Since that time, it has grown to the point where it now performs over a million scans of IP addresses each month for clients of its QualysGuard network auditing and vulnerability management service. The Qualys strength is in its ability to be flexible and nimble as a service – deploying quickly to meet the needs of the targeted scan that looks solely for new and existing vulnerabilities.

Qualys customers provided their own feedback in the benefits that the service offers:

## Instant Deployment

Upon selecting Qualys, the QualysGuard service is immediately available for use. After seeding the scanner with a list of IP addresses, the service can begin its assessment. The result is an audit report within a matter of hours, not days or weeks, from an external location. With today's complex networks and IT support silos, it is extremely difficult to deploy a software solution within months, let alone days. Global scanning within days is a reasonable expectation with QualysGuard.

## Immediate Upgrades

Using a service leaves control over the application infrastructure in the hands of the software developer – which significantly benefits the customer. There are no strange environments or multiple platforms that must be supported – just the primary scanning platform used in the service. Because of this, changes can be created, tested, and deployed quickly to all subscribers.

## Fast Updates

The complement to software upgrades is the signature update – the attribute characteristics being evaluated for new vulnerabilities. With the 10+ vulnerabilities found every day, it is important to have updates that can match this volume with timely response. With a service, updates can be added and deployed immediately.

## Scalability

On-demand service solutions can scale with the Web in its ability to touch the IP addresses that are intended for review. When it is time to expand, there is no need for more hardware to support the move; it is simply a matter of increasing the IP address range. With this level of flexibility and scalability, deployment times are measured in minutes rather than months.

### Shared Information

One of the missing pieces of the security puzzle is the ability to understand the prevalence of vulnerabilities and their significance across organizations. The primary symptom of this problem is an unwillingness for enterprises to share information. The downside is that they are not enriched by information being shared with them either. A service can leverage the information gained from its ability to evaluate many diverse environments, companies, and industries to identify new trends and areas of exposure while protecting the confidentiality of its customers.

### Self-Improving System

As a service, Qualys has a documented 99.997% accuracy rate. If the QualysGuard solution makes an inaccurate identification, it is fixed within 24 to 48 hours and the entire QualysGuard platform realizes the benefit of this correction immediately. In the case of software products, it is extremely difficult to reliably gather data on the accuracy of the solution since there is no direct feedback or accountability mechanism in place. Problems and needs must first trickle up to the manufacturer and then fixes and updates trickle back down to customers.

## Spire ViewPoint

The need for vulnerability management should be clear to any organization. Today's computing environments are extremely dynamic and the risks are constantly changing. With fast-moving worms and motivated hackers on the 'Net, organizations are increasingly targeted. Sometimes they are targeted for specific reasons, as with disgruntled employees, and sometimes they are random victims in the 'drive by shootings' and gang warfare going on among the hacker groups on the Internet.

Delivering an on-demand vulnerability management solution has an extremely strong value proposition. In fact, it is difficult to come up with any negatives, except for the increased reliance on service. In the case of Qualys, its reputation for service has been validated by the many customers who are willing to speak on its behalf. Software-based vulnerability assessment solutions will be hard-pressed to keep up with the proven benefits delivered by a service like QualysGuard.

## 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.

This white paper was commissioned by Qualys. All content and assertions are the independent work and opinions of Spire Security - the product of years of security audit, design, and consulting work.