2015 Enterprise Vulnerability Management Trends Report

A survey and analysis of 974 end-users' current vulnerability management practices
April 29, 2015

Executive Summary

Vulnerability management is an essential component of any information security program. Tasked with protecting business systems and services, IT security managers seek out information about vulnerabilities—the collection of flaws in network devices, hosts, and applications that can be exploited by malware or an attacker. Once found, the security team examines the risks of these vulnerabilities, and develops strategies to remove or block these risks.

Vulnerability management practices vary tremendously among organizations due to differences in people, policies, network environments, and a myriad of other concerns. In the 2015 Enterprise Vulnerability Management Trends Report we set out to explore vulnerability management in enterprise environments looking for factors correlating overall satisfaction with the vulnerability management program.

This report is based on a survey conducted by Skybox Security in December 2014. The survey questioned IT personnel about their roles, tools, and experiences in vulnerability management programs. The results revealed several insights in enterprise vulnerability management programs today, such as:

- **Correlation between vulnerability management policy maturity and satisfaction:** Organizations with formal vulnerability management policies had higher levels of satisfaction with their vulnerability management program results. This indicates that the time spent to define processes, policies, and metrics is well justified.
- **A lack of formal vulnerability management programs:** 50 percent of organizations surveyed do not have a formal vulnerability management program in place, making it difficult to define processes to detect, assess, prioritize, and remediate weaknesses in their network on a regular basis.
- **General dissatisfaction with current vulnerability management programs:** Nearly half of those respondents involved with the vulnerability management expressed dissatisfaction with their program. Dissatisfaction was highest among executives and organizations with less rigorous vulnerability management policies.
- **Patchwork of scanner vendors with no clear frontrunner:** 63 percent of respondents use two or more vulnerability scanners. In an attempt to improve coverage and accuracy organizations have deployed multiple solutions to discover vulnerabilities across their network.
- **Complicated analysis ecosystem:** Most organizations incorporate a variety of tools including home-grown and third-party analytics to make sense of vulnerability and threat data.
- **More timely data:** Nearly all respondents expressed a desire to scan the network more frequently and to be able to determine the impact of a new vulnerability or threat immediately.

Our findings indicate that security practitioners are seeking ways to achieve better results from their vulnerability management programs. The intention of this report is to help security managers and executives looking to take their vulnerability management practices to the next level and to provide insight to how the industry can rise to meet these needs.

Research Overview

Skybox Security conducted a broad survey on vulnerability management practices among organizations worldwide. The objectives of the survey were:

- Understand what vulnerability management tools organizations use today
- How those tools are implemented
- Uncover common challenges in the vulnerability management process

The findings from this research are outlined in this report and covered in the following sections:

People

- Demographics
- Roles and responsibilities

Vulnerability management program characteristics

- Maturity level of program
- Vulnerability assessment use cases

Tools used in vulnerability management processes

- Vulnerability assessment (typically active scanners)
- Analysis and prioritization tools

Scanning coverage and frequency

- Reality vs. ideal

Satisfaction with vulnerability management program

- Vulnerability assessment
- Analysis/prioritization and remediation
- Desired improvements

Demographics

Global Representation

The survey represents an international security audience, with 974 IT security practitioners from 59 countries. Of these, 44.8 percent (436 respondents) are from North America; 35.5 percent (346) from Europe, Middle East and Africa; and 19.6 percent (191) from Asia Pacific and all other countries.

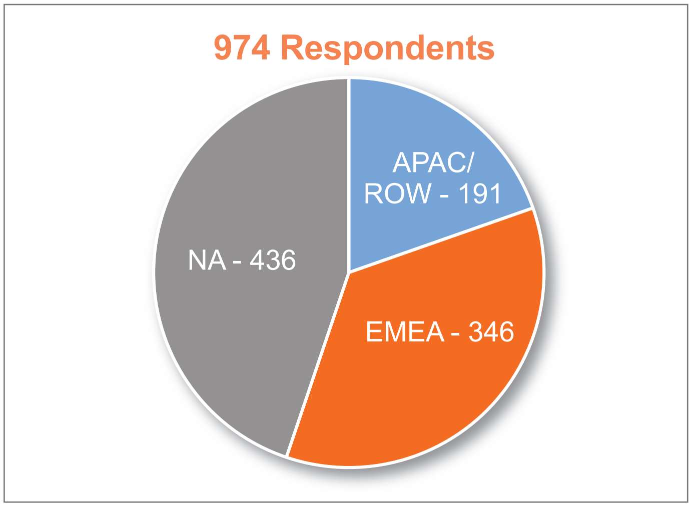


Figure 1

Organization Size

This survey focuses on large enterprise-class vulnerability management programs, so the size of companies participating is heavily represented by large enterprises.

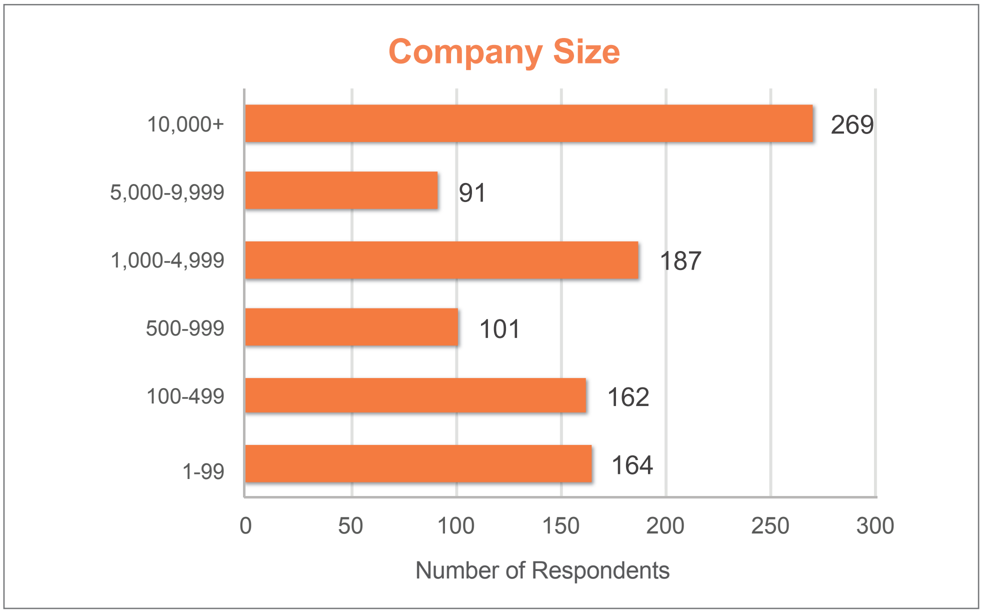


Figure 2

66.5 percent of respondents represent organizations with more than 500 employees. This respondent segment includes large Fortune 500 and Global 2000 corporations as well as large government organizations with hundreds of thousands of employees.

Nevertheless, smaller companies are well represented in the data, with 16.8 percent SMB (1-99 employees) respondents and 16.6 percent small and medium enterprises (100-500 employees). For the purposes of this large-enterprise report, the rest of the analysis focuses on the results from companies with more than 500 employees.

Industries Represented

Survey results represent a wide swath of industries, with financial services, internet/telecom, government and defense, computer hardware/software, and services providing the largest number of respondents.

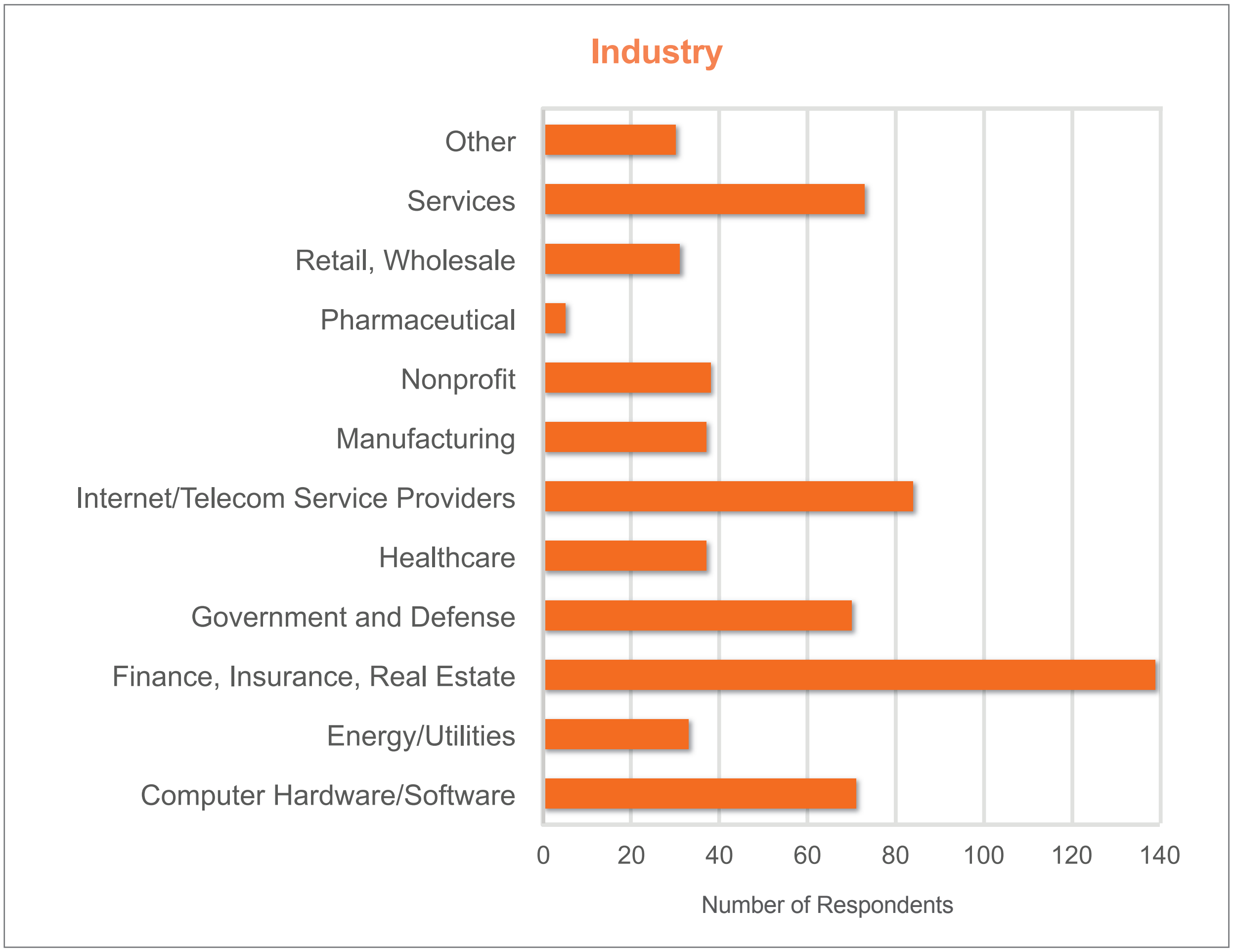


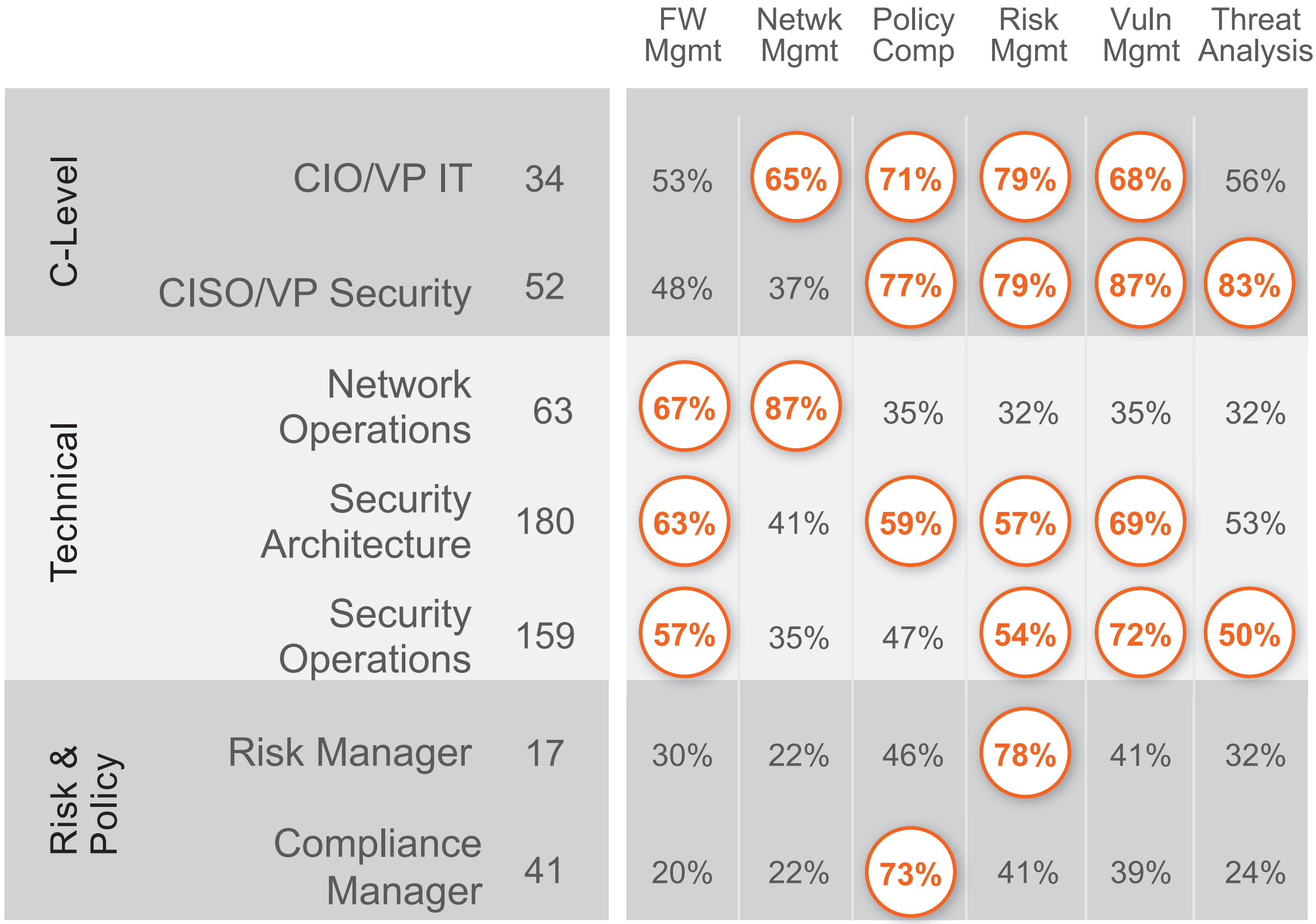
Figure 3

Roles & Responsibilities

While many people within the security team touch the vulnerability management processes, the CISO is the executive champion and leading influencer. 87 percent of CISO respondents reported that they are directly involved with vulnerability management on a daily basis.

Security operations management and security architects are also heavily involved as technical owners, with 72 percent and 69 percent respectively.

Role in IT Organization and Area of Responsibility



			FW Mgmt	Netwk Mgmt	Policy Comp	Risk Mgmt	Vuln Mgmt	Threat Analysis
C-Level	CIO/VP IT	34	53%	**65%**	**71%**	**79%**	**68%**	56%
	CISO/VP Security	52	48%	37%	**77%**	**79%**	**87%**	**83%**
Technical	Network Operations	63	**67%**	**87%**	35%	32%	35%	32%
	Security Architecture	180	**63%**	41%	**59%**	**57%**	**69%**	53%
	Security Operations	159	**57%**	35%	47%	**54%**	**72%**	**50%**
Risk & Policy	Risk Manager	17	30%	22%	46%	**78%**	41%	32%
	Compliance Manager	41	20%	22%	**73%**	41%	39%	24%

Figure 4

In the recent past, questions have been raised as to whether vulnerability management is still an important responsibility of the IT security team. Given the high level of daily involvement by CISOs (68 percent), it seems that vulnerability management processes are still an integral part of a comprehensive security strategy and important enough to merit the top spot on their daily activities. In short, effective management of vulnerabilities matters a great deal to C-level IT staff.

Established Vulnerability Management Policy

In order to gauge maturity of vulnerability management programs, we questioned respondents about their vulnerability management policies and scanning protocols for various parts of their network.

Policy maturity was defined in three stages:

- **No policy:** The organization is only performing vulnerability management-related activities on an ad-hoc basis.
- **Informal policy:** Vulnerability management activities occur routinely, but the process is not well defined and may not be written or monitored.
- **Formal policy:** A written methodology exists for scanning, analysis, prioritization, and remediation of vulnerabilities.

According to a Gartner report, "Gartner defines vulnerability management as 'the key process for finding and remediating security weaknesses before they are exploited.'" Organizations need to establish a formal, written policy as a key component of best-in-class vulnerability management programs: "Security processes, unlike appliances, software and services, cannot be acquired in exchange for cash. They can only be established by an organization and then mature to an appropriate level."[1]

Do you have a policy for your vulnerability management program that defines the methodology for scanning, analysis/prioritization, remediation of vulnerabilities?

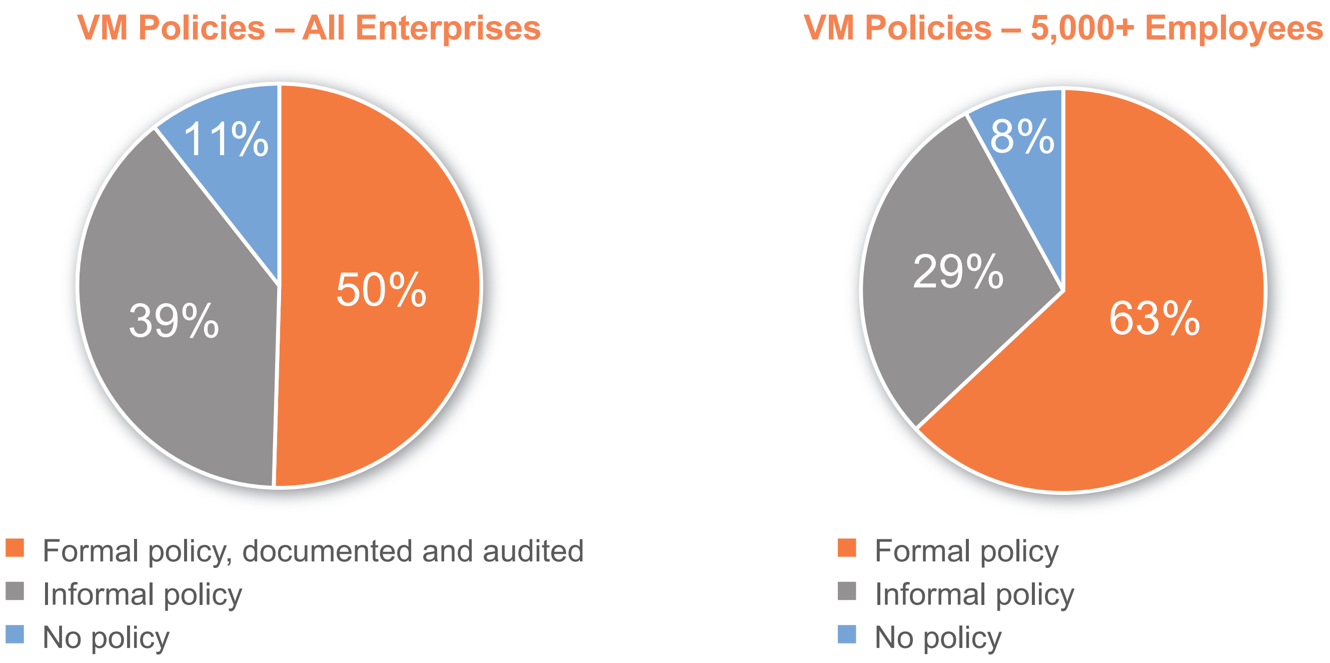


Figure 5

Even with the current C-level attention given to vulnerability management programs, only 50 percent of all enterprise organizations (more than 500 employees) said they have a formal vulnerability management policy. While larger enterprises are more likely to have a formal vulnerability management policy than smaller enterprises, nearly 37 percent of companies with more than 5,000 employees still have no formal vulnerability management policy defined.

[1] Gartner Vulnerability Assessment Technology and Vulnerability Management Practices – Feb. 2014, refreshed May 2015

Vulnerability Assessment Use Cases

We asked respondents to rank the importance of common reasons that organizations give for using a vulnerability scanner. The most important use case was determining risk level, followed by prioritizing vulnerabilities.

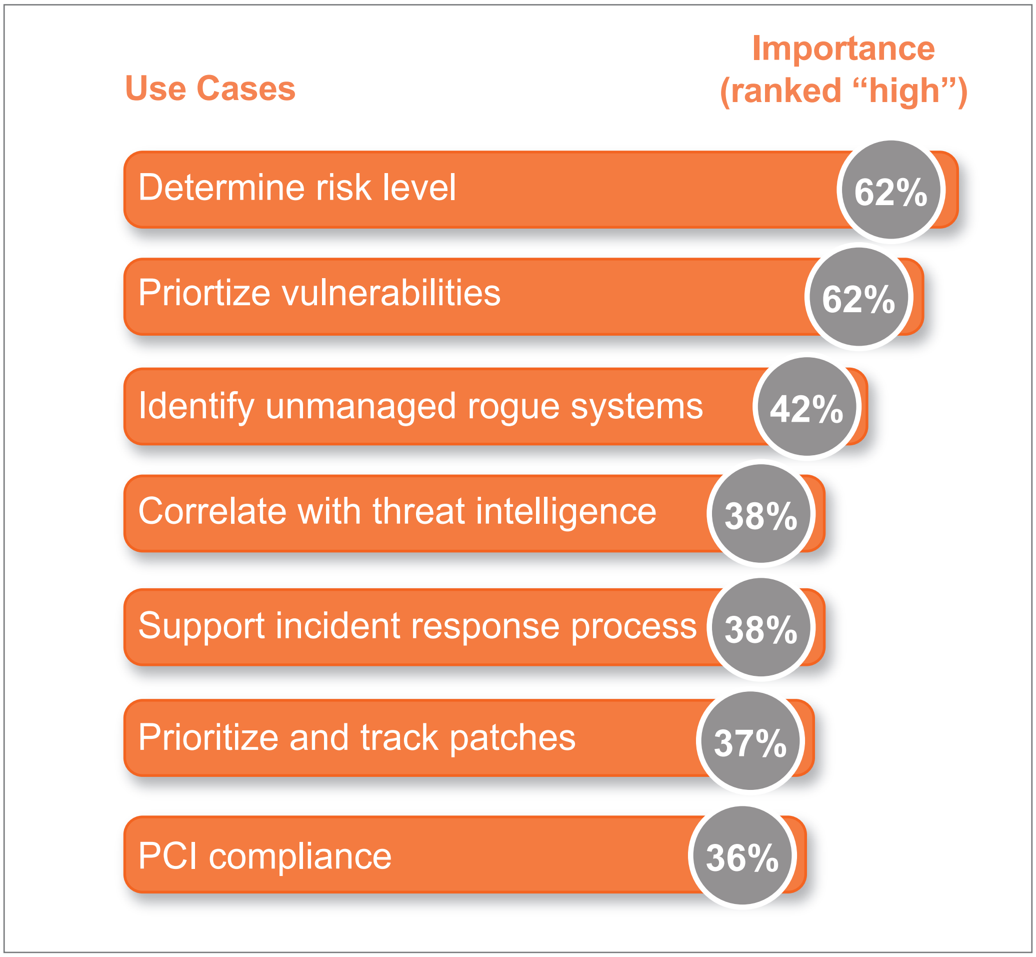


Figure 6

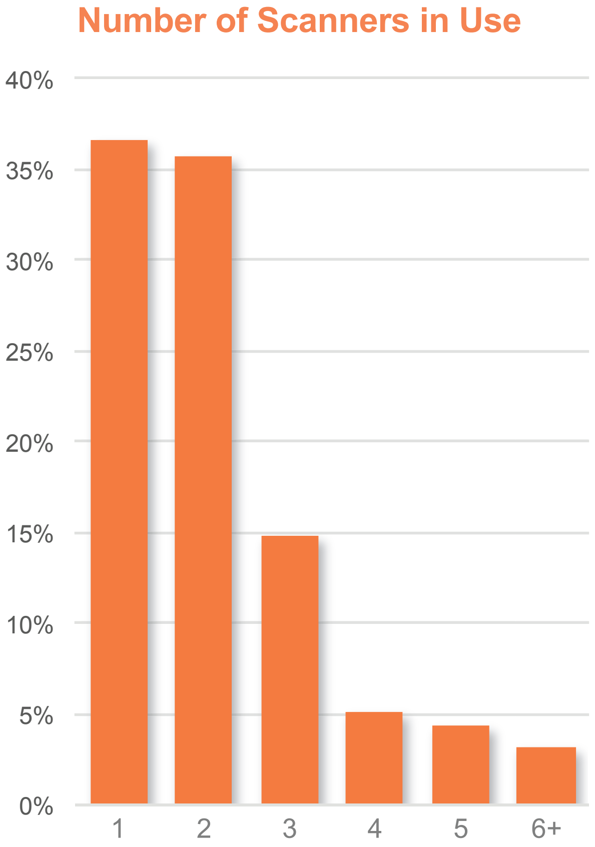
It's interesting to see PCI compliance fall toward the bottom of the use cases. This indicates that security and operational efficiency has a larger mindshare for vulnerability management programs. PCI is no longer the purchase driver it was a few years ago.

Tools Used in Vulnerability Assessment Process

The survey shows a variety of vulnerability scanners currently in use: 14 commonly known brands of vulnerability scanners, other lesser-known scanning tools, and even custom solutions.[2] The chart below highlights the 10 most popular scanners used by respondents.

How many vulnerability assessment tools does your organization use?

Top 10 Scanners	In Use	Primary*
Tenable/Nessus	42%	66%
McAfee	30%	54%
Qualys	28%	62%
Rapid7	20%	66%
Tripwire/nCircle	19%	29%
OpenVAS	10%	14%
GFI	10%	25%
Trustwave	9%	12%
Lumension	8%	5%
BeyondSecurity	7%	39%


Number of Scanners in Use

** Respondents using scanner indicated that it was their primary tool for vulnerability discovery.*

Figure 7

Use of multiple scanning tools appears to be standard practice at most organizations, with 63 percent of respondents using more than one vulnerability scanner. The top four scanners in use by respondents—Tenable, McAfee, Qualys, and Rapid7—are also used the majority of the time as the main scanning tool in a particular environment.

There is a large set of secondary scanners in use in many environments. In separate interviews conducted by Skybox Security, end-users indicated various reasons for using multiple scanners, such as the desire to expand vulnerability assessment coverage, reduce costs by using a lower-price or open source solution in parts of the network, or to reduce false positives.

Tools for Vulnerability Analysis and Prioritization

We also asked about other tools that security professionals use to analyze vulnerability data. It's a common practice to use data analysis tools to correlate multiple sources of data, allow querying of results, or feed vulnerability data into other systems like SIEM or GRC solutions.

Splunk was the most frequently noted data analysis tool, followed by Excel and then a host of other analysis solutions including Skybox, Arcsight, homegrown solutions, and old-fashioned "brainpower."

[2] 11.2 percent of respondents indicated they were using Skybox, but we removed this data to eliminate vendor bias.

Scanning Frequency

Vulnerability scanning occurs frequently in most organizations. 33 percent of respondents scan monthly, and 41 percent of respondents report scanning weekly or more often.[3]

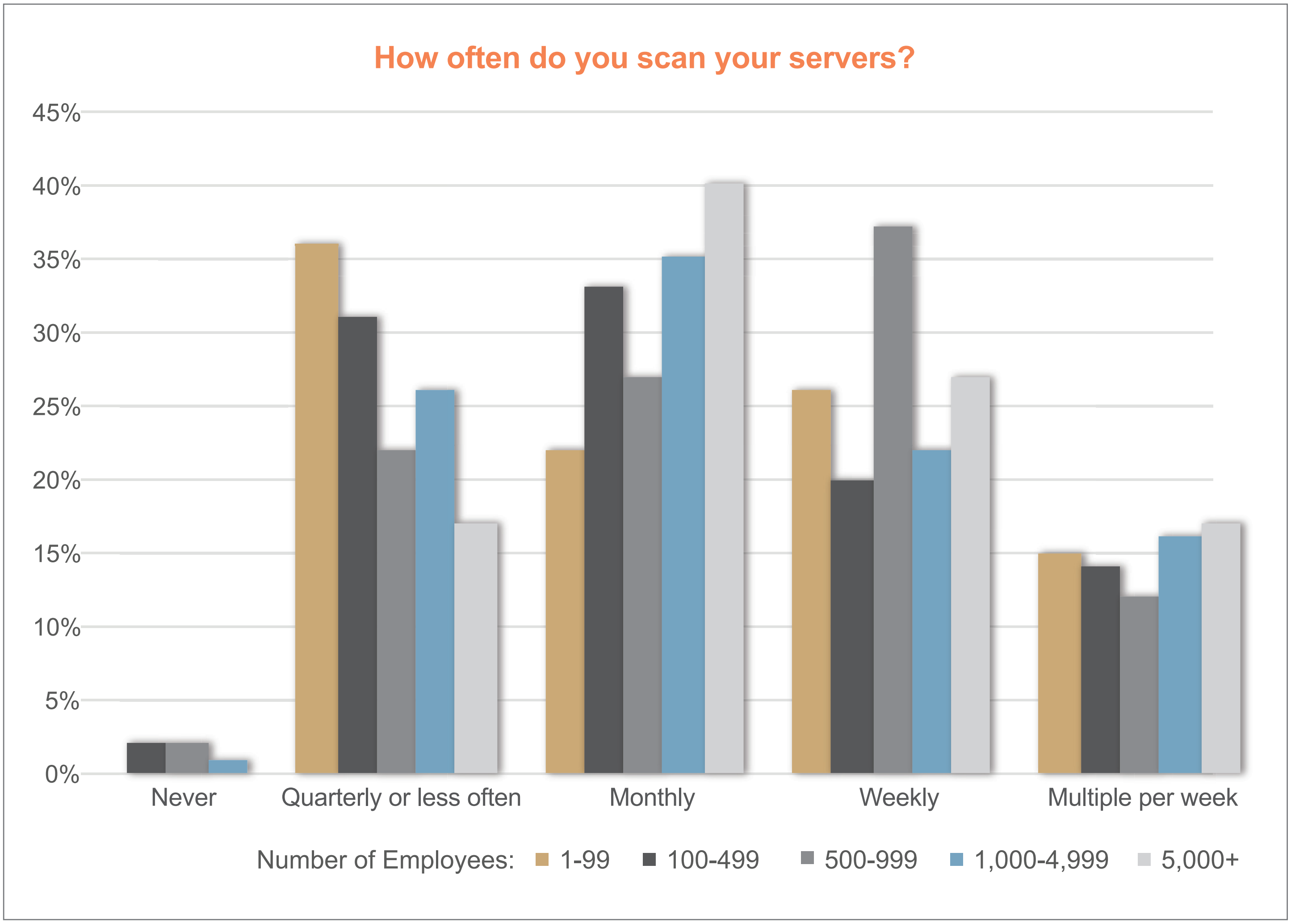


Figure 8

As expected, the frequency of scan cycles directly correlates with size of the organization. 36 percent of SMB respondents (1-99 employees) scan quarterly or less often. By contrast, 17 percent of enterprises with 5,000 and more employees scan quarterly or less frequently.

Although there is a clear connection between company size and quarterly or monthly scan frequencies, this connection does not apply when examining companies that scan weekly or more frequently. “Frequent scanning” accounted for approximately 40 percent of those surveyed. More investigation is needed to see if this “frequent scanning” category stems from security conscious industries such as financial services and other critical infrastructure organizations.

[3] A Skybox Security Vulnerability Management Survey from 2012 found that 24 percent of respondents scanned the DMZ weekly and 37 percent scanned monthly.

Ideal Scanning Frequency

Despite successes in improving scan frequency, there still exists a desire to scan more regularly across the board. Respondents who scan quarterly want to scan monthly; respondents who scan monthly want to scan weekly, etc. This is likely a symptom of increased threat levels fueled by big-name breaches and a growing prevalence of sophisticated attacks; security personnel are still concerned something may slip through the cracks.

This puts the pressure on vulnerability management solution providers to ensure that scanning can scale to the demand for faster cycles of data collection, analysis, and remediation.

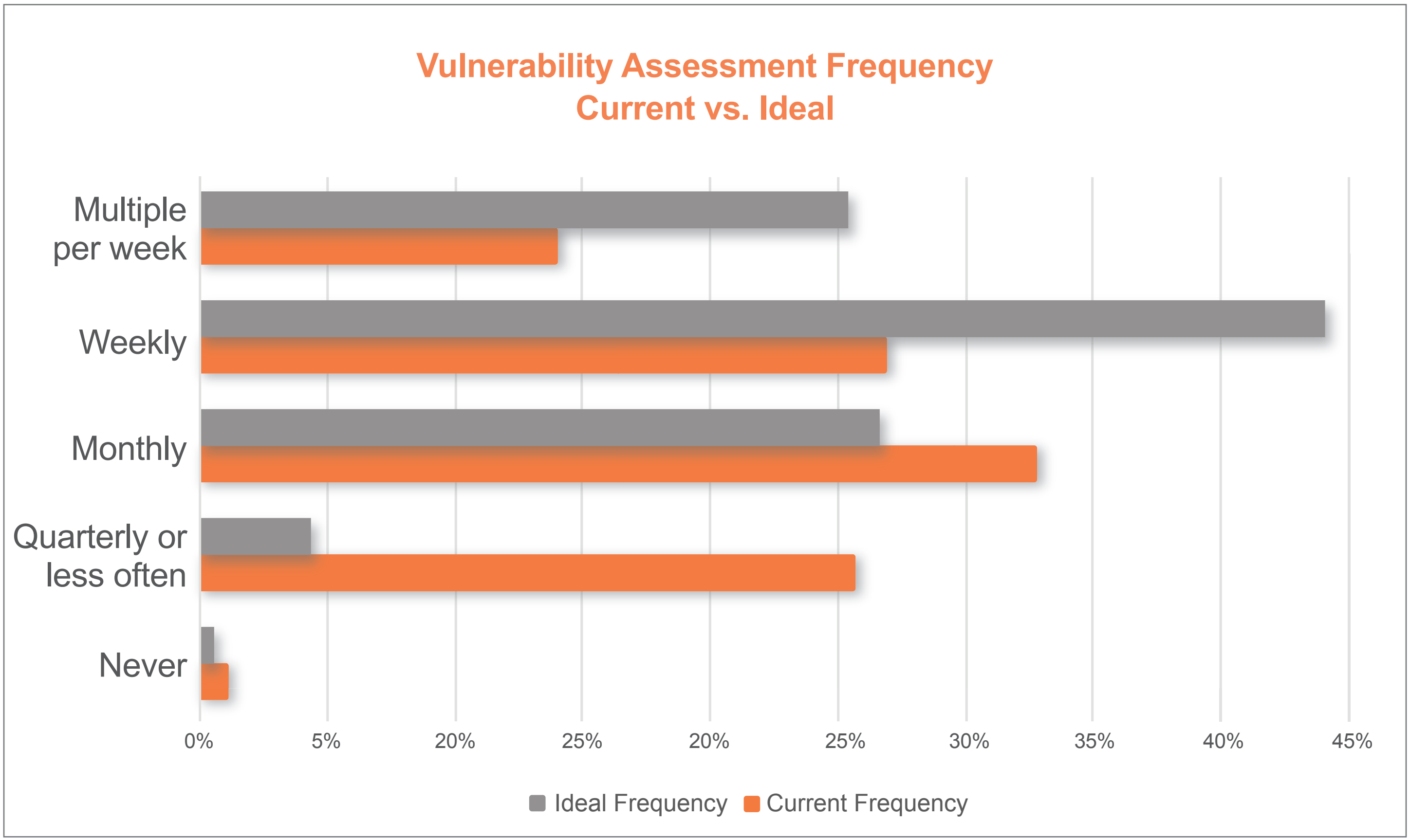


Figure 9

Satisfaction with the Vulnerability Assessment

We sought to find out whether end-users were satisfied with their existing vulnerability management program.[4] Because vulnerability management programs involve different tools, people, and processes in the different stages of the vulnerability management workflow, we asked separate questions for scanning (vulnerability assessment), data analysis and prioritization, and remediation steps.

[4] Data Filter: To avoid vendor bias in the satisfaction measurement, we excluded those respondents who use Skybox Security solutions. Additionally, we included only respondents who had responsibility for vulnerability assessment and represented enterprises with more than 500 employees. All levels of vulnerability management policies (formal, informal, and none) were included, for a total sample of 215 respondents.

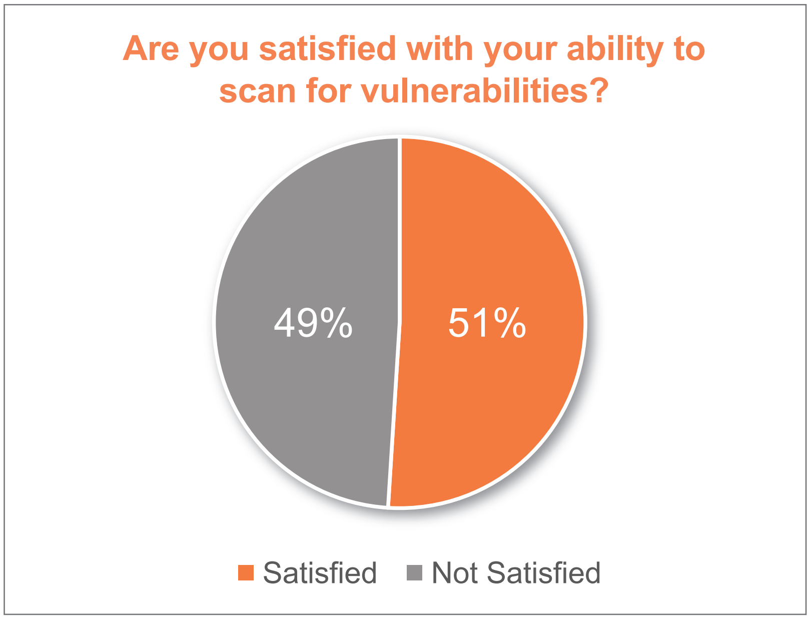


Figure 10

51 percent of respondents are generally satisfied with their ability to scan for vulnerabilities, while 49 percent are dissatisfied. This is a concerning number of dissatisfied security professionals, indicating considerable room for improvement in vulnerability assessment processes or solutions.

Satisfaction Varies by Role

When we filtered the data by level of responsibility in the vulnerability management processes, we found an inverse correlation between seniority and level of satisfaction. We interpret this as an indication that C-level executives have high expectations from the vulnerability management program, and high accountability for the results.

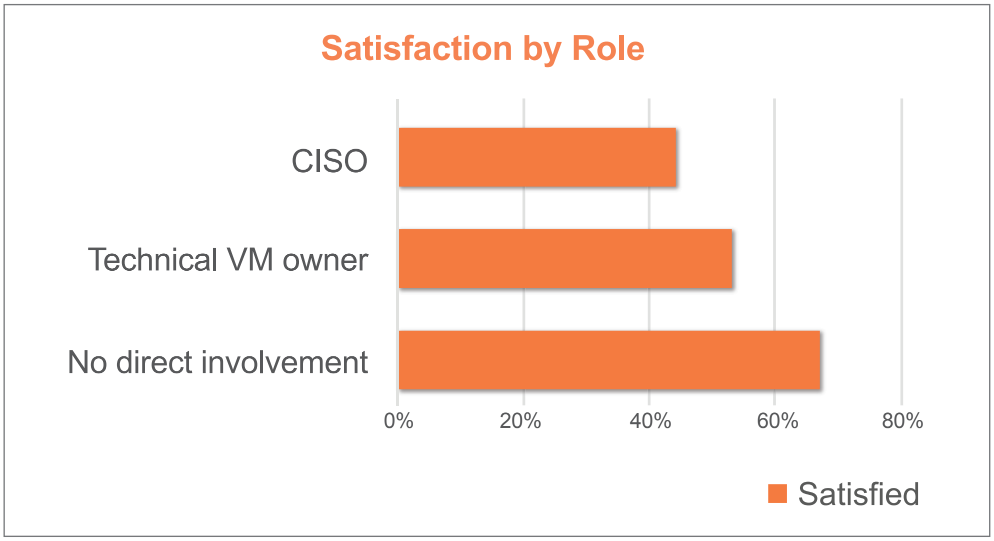


Figure 11

CISOs had the lowest level of satisfaction with vulnerability assessment processes, reporting 44 percent satisfaction. In comparison, 53 percent of the technical vulnerability management program managers indicated they were satisfied with the organizations ability to scan for vulnerabilities.

Interestingly, IT managers who did not have direct daily responsibilities in the scanning processes reported the highest levels of satisfaction with all vulnerability management activities. Apparently, those outside the vulnerability management trenches may be largely unaware of the challenges that the vulnerability management team faces every day—out of sight, out of mind.

Vulnerability Management Policy Influences Satisfaction

In order to drill deeper into these differing levels of satisfaction with vulnerability management activities, we excluded the outside observers with no vulnerability management responsibilities and focused our analysis on the "day in, day out" vulnerability management team.

When examining the relationship between various aspects of vulnerability management programs and levels of satisfaction, we noted a strong correlation between vulnerability management policy maturity and satisfaction.

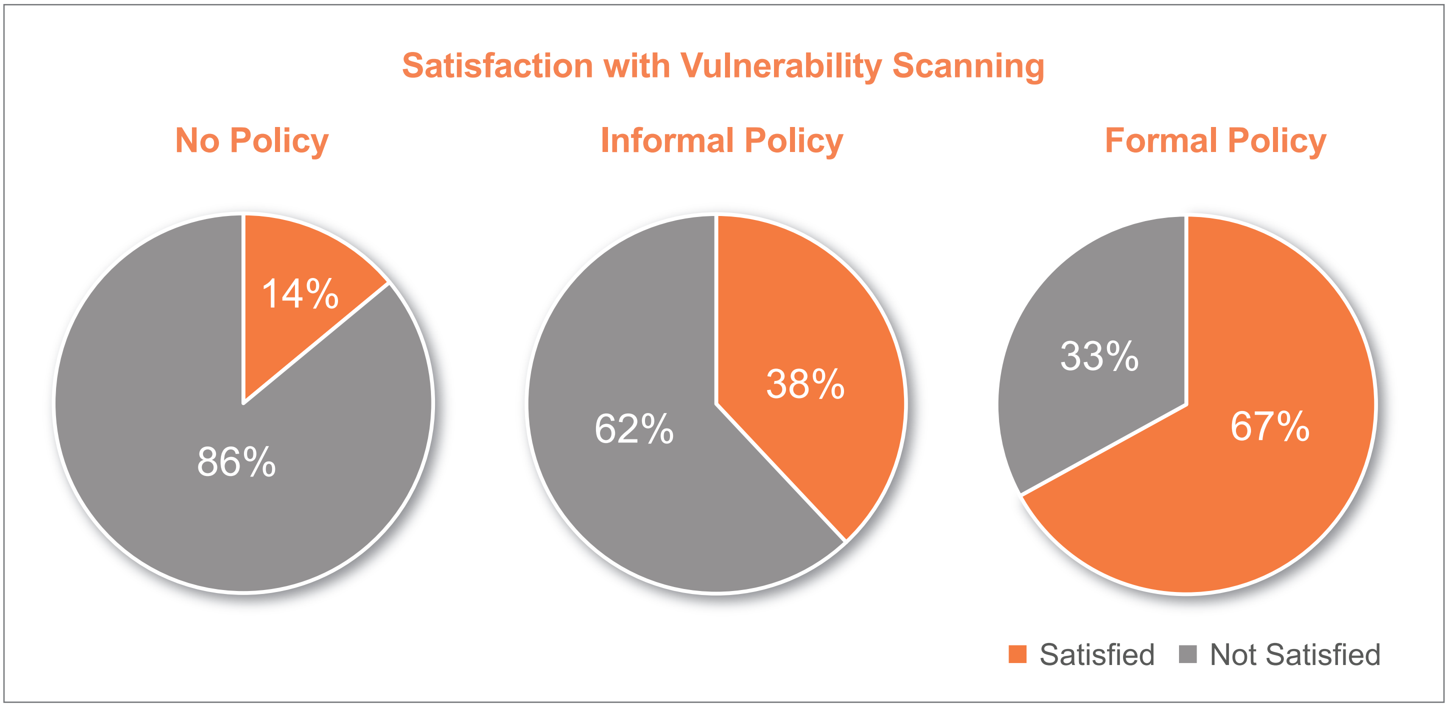


Figure 12

Only 14 percent of respondents from organizations without a defined vulnerability management program (i.e., ad-hoc scanning only) stated they were satisfied with their ability to scan for vulnerabilities. With an informal vulnerability management policy in place, that level of satisfaction rose to 38 percent, and up to a high of 67 percent with a formal, documented, and audited vulnerability management program.

This indicates the management time required to develop a formal policy, document procedures, and audit results will yield a strong, positive return. We conclude that although security managers complain about the headaches involved in establishing repeatable processes and performing regular audits, the data supports that this standard practice offers considerable value and fewer management headaches in the long run.

Satisfaction with the Vulnerability Analysis/Prioritization and Remediation

Analysis and prioritization activities present more challenges to the security staff, with reported satisfaction levels dropping from 51 percent for vulnerability scanning to 44 percent for analysis and prioritization and 45 percent for remediation tasks.

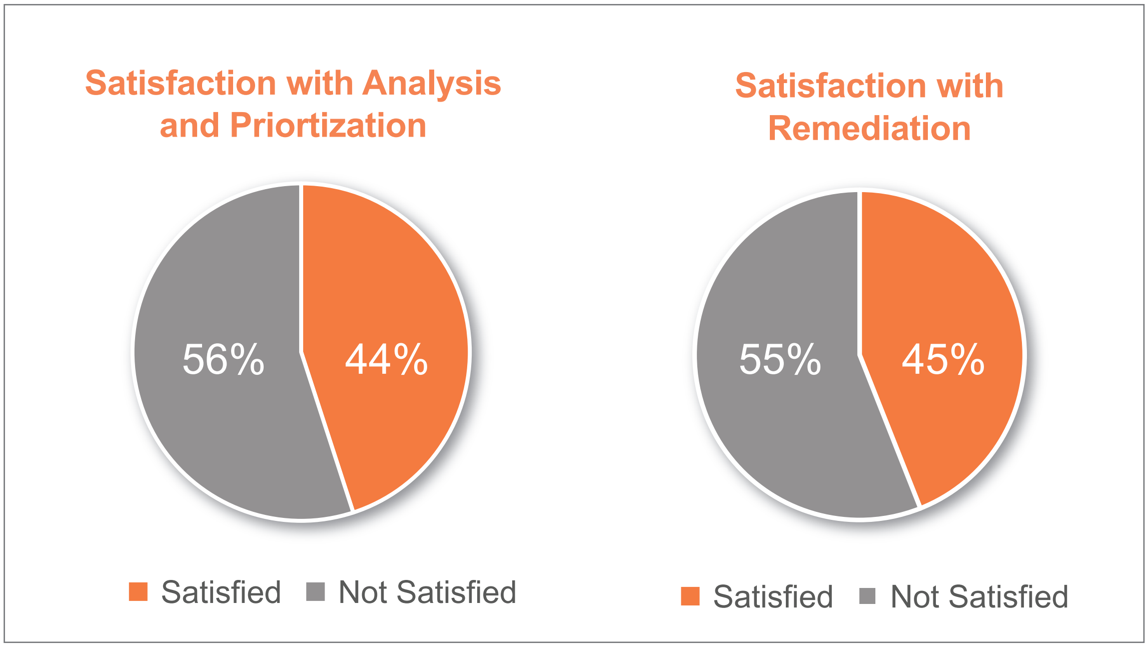


Figure 13

The relationship of seniority level and policy maturity to satisfaction levels holds true for analysis and prioritization and remediation activities as well. Consistently, managers with higher level of seniority and a higher level of accountability reported lower satisfaction with all steps in the vulnerability management process. Respondents in organizations with a formal or mature vulnerability management policy in place reported higher levels of satisfaction.

Those respondents working with a formal vulnerability management policy reported higher levels of satisfaction with the entire chain of activities.

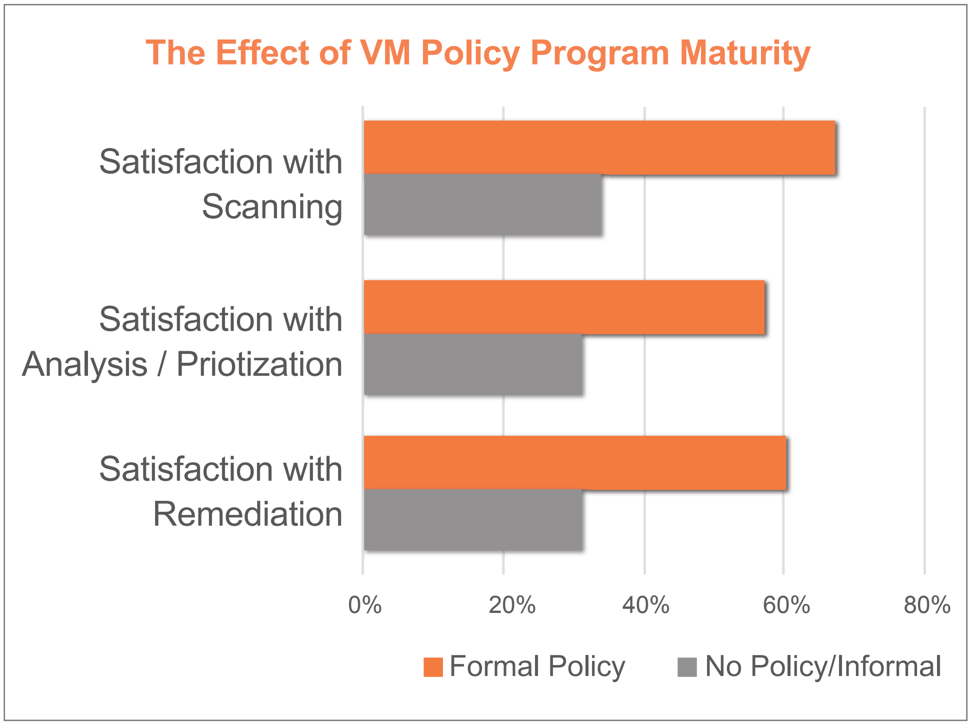
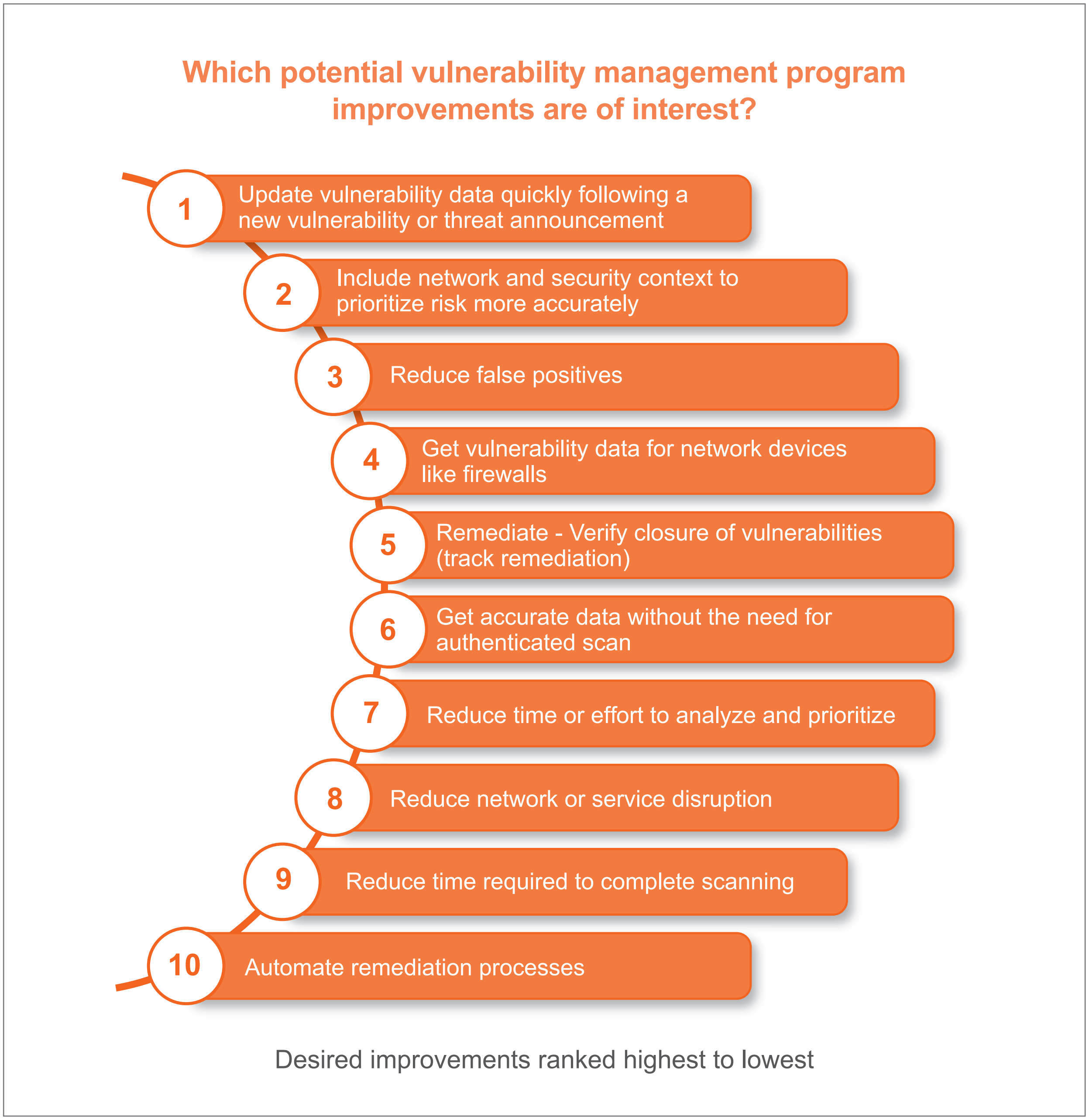


Figure 14

Security managers frustrated with the vulnerability management program should start by defining that process including responsibilities, tools, and audit requirements. A clearly defined process has a strong influence on satisfactory results.

Desired Improvements with Vulnerability Management Processes

Regardless of their level of satisfaction with current vulnerability management program, all respondents were asked about their interest in potential improvements. The Skybox Security Vulnerability Management Survey included a list of 16 potential improvements to vulnerability assessment, analysis and prioritization, and remediation activities. Respondents ranked their interest level from “no interest” to “high interest.” The 10 highest ranking improvements are listed below.



Which potential vulnerability management program improvements are of interest?

1 Update vulnerability data quickly following a new vulnerability or threat announcement

2 Include network and security context to prioritize risk more accurately

3 Reduce false positives

4 Get vulnerability data for network devices like firewalls

5 Remediate - Verify closure of vulnerabilities (track remediation)

6 Get accurate data without the need for authenticated scan

7 Reduce time or effort to analyze and prioritize

8 Reduce network or service disruption

9 Reduce time required to complete scanning

10 Automate remediation processes

Desired improvements ranked highest to lowest

Figure 15

The Most Desired Improvements

The two highest ranking potential improvements focus on obtaining accurate information and the ability to respond quickly to new threats. This is no surprise. New vulnerabilities and threat alerts occur daily, but it can take weeks for a vulnerability management team to run through the cycle to scan, prioritize, and remediate vulnerabilities. For example, when the Heartbleed vulnerability was disclosed, it took weeks for many organizations to generate an accurate list of vulnerable systems.

Moreover, each vulnerability assessment cycle generates thousands of vulnerabilities which can take extended periods to review and develop remediation plans. Such plans and the tools to help create them must consider the surrounding context of the network topology and existing security controls. According to Gartner, “A set of dedicated products has evolved to provide a better context or environment for a vulnerability by examining network and security devices (for example, firewalls and routers) and combining this information with vulnerabilities that are identified elsewhere. Such simulation or modeling products examine vulnerabilities in light of the entire computing environment.”[5] Context helps IT security teams prioritize those vulnerabilities that can impact critical assets over those where an existing security control offers protection. Making these improvements would allow organizations to access and analyze vulnerability data faster, which could shorten response times to new vulnerability announcements and lower risk of attack.

Reducing false positives (ranked third) is a related concern, indicating that respondents may feel they are spending valuable time on false positives instead of risks which can truly impact their network. Getting vulnerability data for network devices like firewalls (ranked fourth) indicates an interest in extending vulnerability data to systems not covered by traditional active scanners today.

The next six improvements are largely about operational improvements to vulnerability management processes—tracking closure of vulnerabilities, automating process steps, removing task roadblocks like system authentication requirements, and potential service disruptions.

[5] Gartner Vulnerability Assessment Technology and Vulnerability Management Practices – Feb. 2014, refreshed May 2015

Conclusions

Organizations intend to use vulnerability management as a mean to reduce risk level. This is supported by the top use cases (determine risk level and prioritize vulnerabilities) and the top desired improvements (access to accurate vulnerability data and network context), as well as past surveys conducted by Skybox.

Are they successful in meeting this goal? Judging by the satisfaction numbers, it’s a coin toss. For every security manager who is happy with their vulnerability management program results, there is another security professional who is unhappy.

The rankings of desired improvements to the vulnerability management programs points to some likely hidden pain points.

- Difficulty getting current vulnerability data when it’s needed for threat response
- Accurate prioritization of vulnerabilities that are critical risks to the network
- False positives draining limited resources and extending the vulnerability management process

Aspiring to a higher level of process maturity, better verification of closed vulnerabilities, less disruption to other processes, and reduction in the time spent from scanning through remediation will improve vulnerability management and result in higher satisfaction.

For CISOs and other security leaders, these results point to a need to evaluate their vulnerability management program on many levels. Using a program scorecard on an annual basis would allow CISOs to identify productivity concerns, solutions that are underperforming, weak points in the process, and tune their program for maximum effectiveness in reducing risks.

For technical managers, it’s a good idea to think of a vulnerability management program as a leading defense against attacks. A mediocre program is not enough to manage vulnerability risks against a legion of determined attackers. Security demands strong set of consistently applied tools. If an organization uses a patchwork of different scanners and add-on tools and takes weeks to evaluate vulnerabilities, it will be in poor position when the next vulnerability or threat is announced. Without a solid foundation of vulnerability management processes, a network is an easy target to knock down.

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.

Skybox Security's Vulnerability Management solution automates and integrates continuous vulnerability assessment, analysis, and remediation, enabling same-day attention to critical cyber risks. Skybox Security uniquely combines network modeling, non-disruptive vulnerability detection, risk analytics, performance metrics and attack simulation to prioritize and eliminate security risks.

Skybox challenges the assumption that scanning is the best way to discover vulnerabilities. Skybox uses non-disruptive, scanless technology that analyzes information repositories available in every enterprise—typically patch management and asset management systems—to automatically and accurately deduce vulnerability data on all network nodes. Additionally, Skybox Vulnerability Control seamlessly integrates with every major vulnerability scanner, and scanner results can augment Skybox's scanless vulnerability discovery.

Skybox looks beyond a vulnerability's severity rating, asserting that the criticality of a vulnerability depends on several factors, including existing security controls, the business asset, and the impact of a potential attack. Taking into consideration the network infrastructure and threat data, Skybox Vulnerability Control automates the analysis of the vulnerabilities, eliminating vulnerabilities that are not exploitable and prioritizing remediation based on business impact and exploitability. Skybox Security uses two approaches for prioritization:

- **Hot Spots Analysis:** Finds groups of hosts on the attack surface with a high density of severe vulnerabilities, which can be fixed en masse by broad action items, such as patching.
- **Attack Vectors Analysis:** A surgical approach that finds specific, high-risk attack vectors around one or a few hosts that would require quick remediation (patching, shielding, network configuration) to eliminate exposure of specific targeted assets.

Once a short list of action items is available, Skybox Vulnerability Control provides context-aware remediation recommendations that consider a variety of remedial actions, such as IPS signature activation, firewall configuration changes, patching, system configuration, and more. Further, Skybox Vulnerability Control enables effective communication with the relevant IT operations team, and integrated workflow generates and tracks remediation actions.

Skybox Security, Inc. provides security management and operations the tools they need to eliminate attack vectors and safeguard business data and services. Skybox solutions provide a context-aware view of the network and risks that drives effective vulnerability and threat management, firewall management, and continuous compliance monitoring. Organizations in financial services, government, energy, defense, retail, and telecommunications rely on Skybox Security every day for automated, integrated security management solutions that lower risk exposure and optimize security management processes. For more information visit www.skyboxsecurity.com.

VMSurvey_EN_04292015