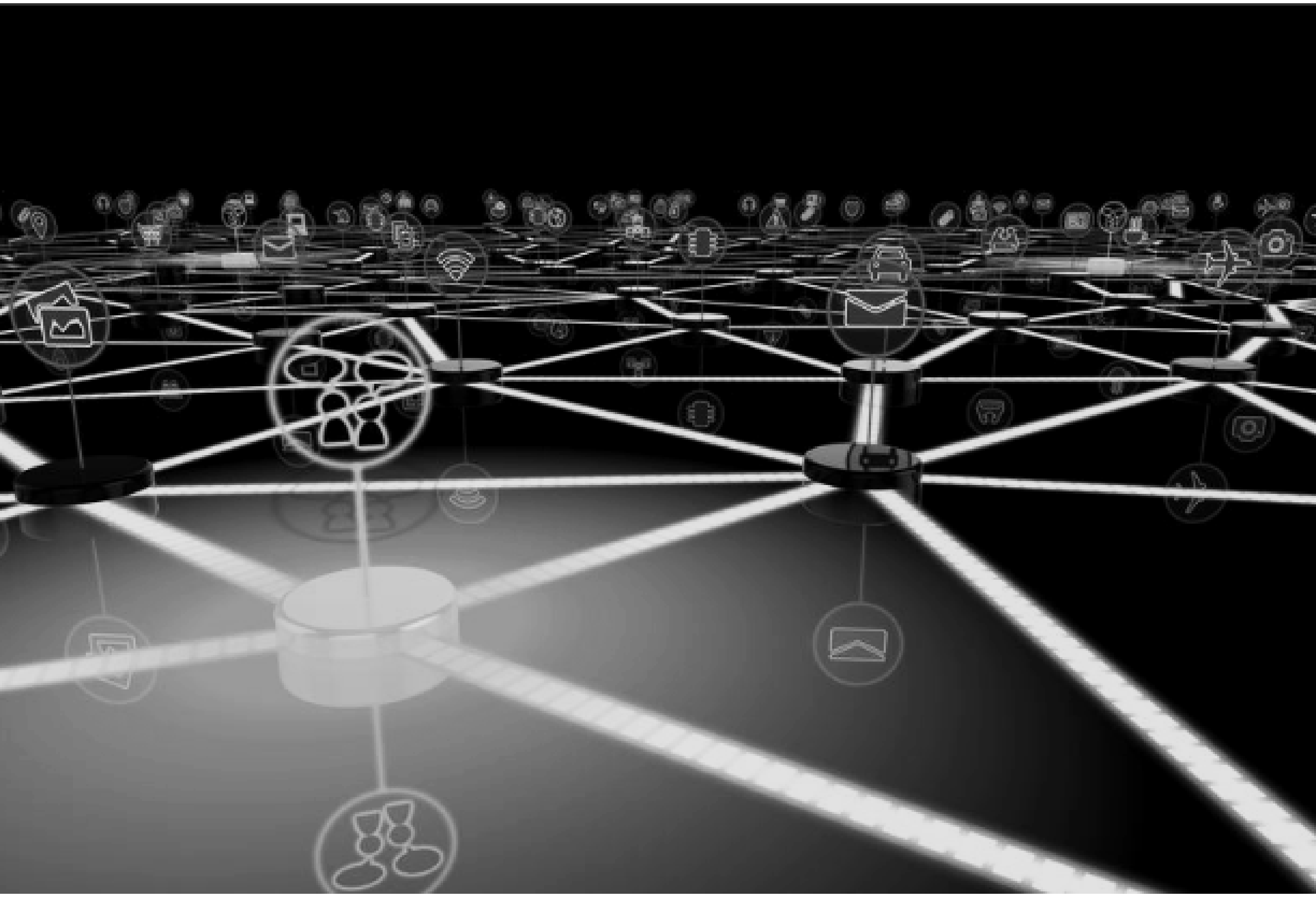
WHITE PAPER

Improving Business Outcomes With Vulnerability Risk Management

The Business Case for the Right VRM Technology

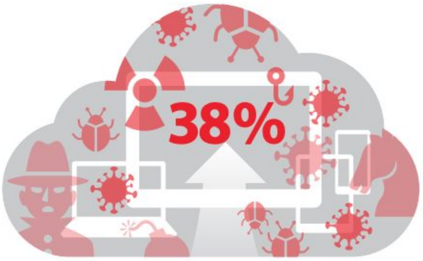


NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction



The value of an effective information security (infosec) program is intuitive to any business leader. In one survey, organizations reported 38% more detected security incidents in 2015 compared to 20141 , and high-profile data breaches remind us just how far-reaching a security failure's implications can be. From protecting customer data to securing intellectual property to meeting regulatory standards, companies rely on infosec not only to stay compliant, but to stay in business.

Despite their intuitive understanding, many company leaders find themselves investing in vulnerability risk management (VRM) solutions and then wondering whether the time, money and resources put into VRM implementation are delivering on the promised value. Often, businesses feel burned by unrealized promises for better security, cost savings, and a lightened employee workload. It doesn't have to be this way. VRM is a vital piece of a comprehensive infosec program that, when done right, can drive improvements to your broader business objectives. Successful VRM is a strategic program backed by the right technology that proactively informs teams about their security risks, helps them prioritize risk remediation, and helps them continue to operate efficiently as the company grows.

The following explains the most common reasons businesses struggle to derive value from VRM technology. We proceed to share key components for VRM success and explain how to align VRM and business outcomes.

Challenges to Getting Maximum Value from VRM Technology

Even with expensive scanning and VRM technology, infosec teams may still be dealing with overloaded employees and more vulnerability data than they can handle. Add to this the difficulty of calculating the return on investment (how do you measure the value of a data breach or downtime that didn't happen?), and infosec leaders may find themselves in a difficult position when it's time to make the case for the VRM technology budget. These are the most common reasons that businesses find themselves in this position when it comes to their VRM solution.

1. Leadership Doesn't Understand the Full Scope of VRM and Its Impact

Many business leaders outside of the security organization hear "vulnerability risk management" and confuse it with specific VRM steps like vulnerability scanning and penetration testing (pen testing). However, the infosec team knows that scanning and pen testing only give you limited information about your security posture - by themselves, they won't keep your business secure. In order to do that, you need VRM: an ongoing practice that is as much about people and processes as it is about technology. VRM encompasses the full scope of detecting, classifying, prioritizing, and remediating security vulnerabilities, as well as managing workflow and communicating within and across teams.

To understand the difference, compare scanning and VRM to the process that occurs when a patient goes to the doctor for a physical examination. Think of your organization's overall infosec posture as the patient's health. The vulnerability scan is like the exam, and VRM is all of the people, processes, and technology applied before, during, and after the exam that actually keep the patient healthy.

For example, in a physical exam, the doctor will weigh the patient, take their blood pressure, and listen to their heart. This is like running a vulnerability scan. It provides data, but it doesn't tell the patient if they're at risk of getting sick, nor what to do about it if they are. In the same way, the report output from a vulnerability scan gives you data, but by itself, it won't help you prioritize nor remediate threats without additional steps.

Many businesses choosing a VRM solution miss an essential stage in the decision-making process: connecting the technology to their business needs.

VRM, on the other hand, encompasses not only the exam (the scan), but also a full suite of activities and technology that turn the results into something useful: from hiring qualified staff (the infosec team); to investing in diagnostic technology (the scanner); to interpreting the test results (prioritizing threats); to treating the patient (remediation); to communicating and managing the process (workflow, communication, and reporting).

2. The VRM Technology Isn't a Fit for the Business's Needs

Many businesses choosing a VRM solution miss an essential stage in the decision-making process: connecting the technology to their business needs. The decision usually begins with a vague sense that technology is needed to improve VRM practices. It ends with selecting the platform that checks the most boxes. In between, the deciders fail to define and prioritize the business issues that they wanted to address in the first place.

Similarly, businesses may find themselves layering on point solutions throughout the environment prior to assessing the overall business requirements driving their selection. More often than not, these point solutions end up poorly integrated and add friction even if they succeed at addressing the old problems.

Whatever their approach, many companies implement solutions that don't solve the underlying issues they were intended to address. For example, if cost control was one of your drivers, but you now find yourself paying for features that you don't need, are you meeting your goal? Or perhaps one of your biggest frustrations was managing remediation workflow efficiently, but you're now finding that workflow is not a strength of your VRM platform. Companies that do not take a moment to establish these business needs early in the buying process may find themselves going through a box-checking exercise without sufficiently evaluating a solution's true capabilities in critical areas – resulting in a lot of time and money invested in technology that is not a fit.

3. The Technology Lacks Innovation and Fails to Keep Up With Security Trends

Not all VRM technology is created equal. Many solutions fail to innovate sufficiently and therefore cannot deliver on their promises to make the infosec team's lives easier. A vendor may tout their platform's ability to prioritize vulnerabilities. But in reality, the technology does little to eliminate false positives or to score risks using inputs beyond the Common Vulnerability Scoring System (CVSS) and asset classification.

The result is a team that has a technology solution but is still overloaded by data and lacking trust in the threat reporting. The platform may also fail to solve the more people-driven challenges of VRM, like workflow and communication issues that slow down time to remediation. Inadequacies like these lead to frustrated infosec staff, unremediated threats, and an incomplete picture of the true risks the business faces.

4. The Company Has Difficulty Hiring Skilled Resources

It's a story most small and medium-sized companies know well: they simply cannot afford to hire the number of skilled security professionals they need. For the business leader responsible for infosec, these budget realities can be the most frustrating part of the job. Even if the business possesses effective technology for reporting on vulnerabilities, the head count is not there to keep up with external security trends and internal workload. Alternatively, even when the head count is there, the staff may still lack the right technical skills, further overloading employees or keeping important tasks from getting done right if at all.

5. Competing Operational Demands Get In the Way

Chances are good that infosec is not the only responsibility of the IT staff. Small IT teams typically wear many hats, balancing security with support, operations, development, and more. Pulled in many directions at once, operational necessities mean VRM gets put on the backburner, putting the business at risk.

Small IT teams typically wear many hats. Pulled in many directions at once, operational necessities mean VRM gets put on the backburner.

> *"Attackers have a tendency to follow the easiest path, and organizations are still consistently failing to patch well-known vulnerabilities in a reasonable timeframe. There are two key trends addressing this issue: First, organizations need the ability to prioritize threats based on a mix of the attacker's perspective and the academic/researcher perspective, not just the latter. Second, workflow optimization can also significantly reduce the time from awareness to issue resolution with respect to flaws that attackers will quickly identify and exploit."*

- **Adrian Sanabria, Senior Security Analyst, 451 Research**

Bridging the Gap: The Right VRM Technology

These steps will help you overcome the most common hurdles to deriving maximum value from your VRM technology and assist you in selecting the right solution for your business's requirements.

1. Understand the Scope of Full-Scale VRM

VRM goes beyond vulnerability scanning and pen testing. The first step to making the business case for VRM is understanding all the pieces that go into an effective program and what they mean to the overall security posture of your business. From risk detection to prioritization, remediation, reporting, workflow, and communication, every decision-maker must have a grasp of VRM's scope in order to be confident that you have the right solution for your unique needs.

2. Align Technology and Resources with your Business Objectives

Once you're confident that the leadership team has a complete understanding of what VRM entails, it's time to take a step back and look at the big business picture. Start by listing the business demands that drive your need for a VRM solution in the first place. What's most important to your business strategy?

When you know what your business priorities are, you can make a more realistic assessment of whether a platform will solve your most important problems. Say resource efficiency is at the top of your list. Does your solution's risk scoring apply enough data to narrow down vulnerabilities to the critical few that present the most risk so the team does not waste time prioritizing? If cost control is your priority, does the technology reduce the need to hire additional people or pay the ones you have to spend overtime on manual processes? If the answers to questions like these are “No,” then it is time to consider your alternatives.

3. Look to a SaaS solution to Augment Resources and Keep Up with the Changing Threat Landscape

Seek a VRM vendor that can serve the business objectives you identified in step two. While a checklist is a great tool to evaluate different options, make sure that each criterion on your list maps clearly back to business needs. A software-as-a-service (SaaS) vendor may be in a better position than an on-premise solution to provide the customization and benefits that are most frequently needed.

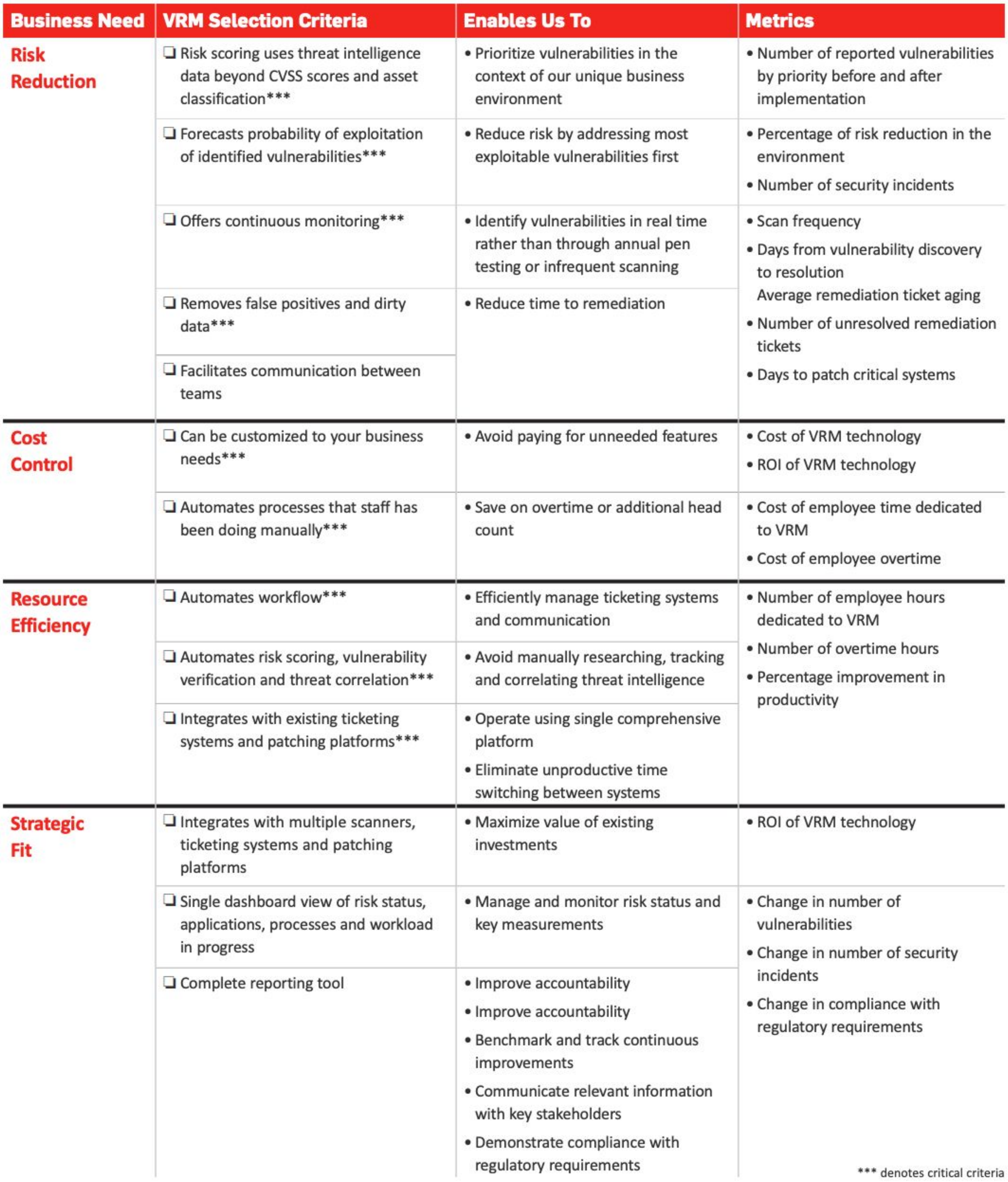
The sample checklist here outlines common business objectives, VRM technology benefits that can serve them, and areas where SaaS solutions tend to stand out.

4. Define and Measure VRM Success

Finally, a successful VRM strategy will lead to measurable improvements in the factors that you defined at the outset. Without question, it should improve speed to remediation, showing a significant reduction in the time it takes to remediate identified vulnerabilities. You should also see measurable improvements in the other business objectives that you identified as most important. Establish baseline measurements of your costs, resource efficiency, and risk posture. As you evaluate solutions, look for proof that they can drive measurable improvements in these areas.

Your infosec program is incomplete without quality VRM that helps protect your business's operations and reputation. The most common VRM challenges can become a thing of the past with the right technology. Align your VRM program with your business goals, and prepare to see measurable improvements to your broader business objectives.

Vulnerability Risk Management Solution Cheat Sheet



Business Need	VRM Selection Criteria	Enables Us To	Metrics
Risk Reduction	❑ Risk scoring uses threat intelligence data beyond CVSS scores and asset classification***	• Prioritize vulnerabilities in the context of our unique business environment	• Number of reported vulnerabilities by priority before and after implementation
	❑ Forecasts probability of exploitation of identified vulnerabilities***	• Reduce risk by addressing most exploitable vulnerabilities first	• Percentage of risk reduction in the environment • Number of security incidents
	❑ Offers continuous monitoring***	• Identify vulnerabilities in real time rather than through annual pen testing or infrequent scanning	• Scan frequency • Days from vulnerability discovery to resolution Average remediation ticket aging • Number of unresolved remediation tickets • Days to patch critical systems
	❑ Removes false positives and dirty data***	• Reduce time to remediation	
	❑ Facilitates communication between teams		
Cost Control	❑ Can be customized to your business needs***	• Avoid paying for unneeded features	• Cost of VRM technology • ROI of VRM technology
	❑ Automates processes that staff has been doing manually***	• Save on overtime or additional head count	• Cost of employee time dedicated to VRM • Cost of employee overtime
Resource Efficiency	❑ Automates workflow***	• Efficiently manage ticketing systems and communication	• Number of employee hours dedicated to VRM • Number of overtime hours • Percentage improvement in productivity
	❑ Automates risk scoring, vulnerability verification and threat correlation***	• Avoid manually researching, tracking and correlating threat intelligence	
	❑ Integrates with existing ticketing systems and patching platforms***	• Operate using single comprehensive platform • Eliminate unproductive time switching between systems	
Strategic Fit	❑ Integrates with multiple scanners, ticketing systems and patching platforms	• Maximize value of existing investments	• ROI of VRM technology
	❑ Single dashboard view of risk status, applications, processes and workload in progress	• Manage and monitor risk status and key measurements	• Change in number of vulnerabilities • Change in number of security incidents • Change in compliance with regulatory requirements
	❑ Complete reporting tool	• Improve accountability • Improve accountability • Benchmark and track continuous improvements • Communicate relevant information with key stakeholders • Demonstrate compliance with regulatory requirements	

*** denotes critical criteria

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.