KENNA Security

whitepaper

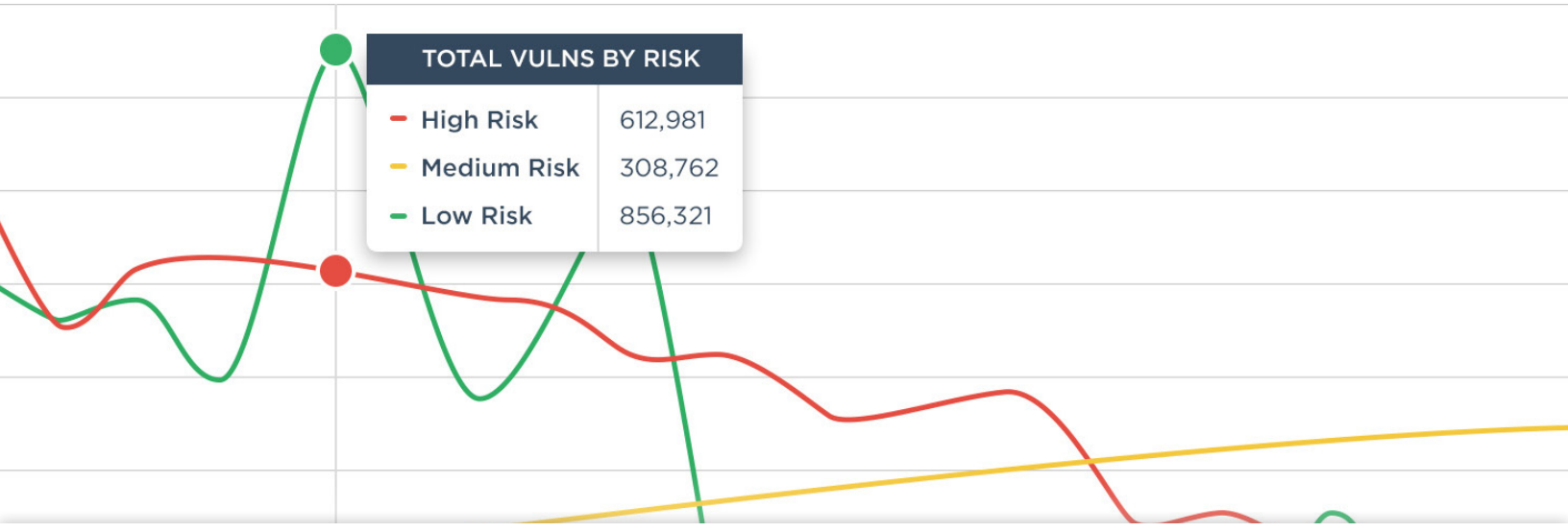
Close What Matters: 5 Requirements for Reducing Vulnerability Risk

Identify high-risk vulnerabilities and prioritize remediation efforts

Introduction

It only takes one exploited vulnerability to bring down a large enterprise. And it doesn't have to be a zero-day; according to Gartner, zero-day vulnerabilities will play a role in less than 0.1% of attacks, excluding sensitive government targets, through 2020. That means in most cyber attacks a patch will be available, and security tools will trigger alerts. But still the vulnerabilities will remain open, enabling attackers to access business-critical systems and sensitive data.

The problem isn't a lack of security controls—it's too many alerts. For security teams that lack the resources to analyze, correlate, and prioritize vulnerabilities, remediation is a game of Russian roulette. The good news is, vulnerability management doesn't have to be fraught with risk. You can prioritize high-risk vulnerabilities. You can significantly reduce the risk of leaving a targeted vulnerability open. Here's how.



Requirement #1: Know Your Assets

The first step to prioritizing your remediation efforts is understanding what it is you're protecting. This means taking a complete inventory of all organizational assets—both on-premises and in the cloud.

Performing an asset inventory can be a daunting task for many organizations. To make it more palatable, treat your asset inventory as an objective with specific goals and metrics such as:

1. External scanner coverage (known assets/ scanned assets)

2. Internal scanner coverage (known assets/ scanned assets)

3. Time to discover (lower is better)

Use An Automated Discovery Process To

- Understand your DNS and WHOIS records
- Identify IP address ranges and domains you own
- Recognize what ports, applications and services are running on them
- Clarify your processes for discovering new assets, services and DNS records
- Understand how you feed these assets into your assessment and scanning processes

Requirement #2: Know Your Business

Successfully understanding the most pertinent threats – and measuring the likelihood of an exploit – requires business context. A great way to apply this knowledge to security is through threat modeling. Threat modeling can get quite sophisticated, but even a basic approach will help you identify the assets most in need of protection.

A few key areas to consider include:

- Your organization's broad metadata including industry vertical, size and geography
- The valuable and/or regulated information your applications or assets are processing
- How many people use an application
- The critical controls in place to protect confidentiality, integrity and availability of key assets
- Your adversaries and their capabilities

As an example of how this information can provide valuable business context, consider the following two applications. The first, used internally for HR, contains sensitive information such as social security numbers, health care information, etc. The second is a public-facing application that only contains public data.

Without evaluating the size of the user base, the internal application processing sensitive data seemingly outweighs the risk of the public application. However, if the public application exposes each of its 100 million users to a persistent cross-site scripting vulnerability, you might think differently

Useful Metrics

1. System Susceptibility
- Value to attackers
- Vulnerabilities

2. Time to Compromise
The time it would take hackers to compromise any of the key controls for these assets and applications

3. Threat Accessibility
Access Points and Attack Surface

4. Threat Capability
- Tools
- Resources
- Techniques

Requirement #3: Know Your Current Risk Posture

Knowing your organization's risk posture requires understanding the likelihood and impact of threats. Numerous factors go into understanding both factors. Consider the following:

1. Asset Metadata:

- Who owns the asset?
- What is the asset's function, and how is it used?
- Based on the asset's function, which is the most important: confidentiality, integrity, or availability?
- What's the impact of losing the confidentiality, integrity, or availability of the asset?

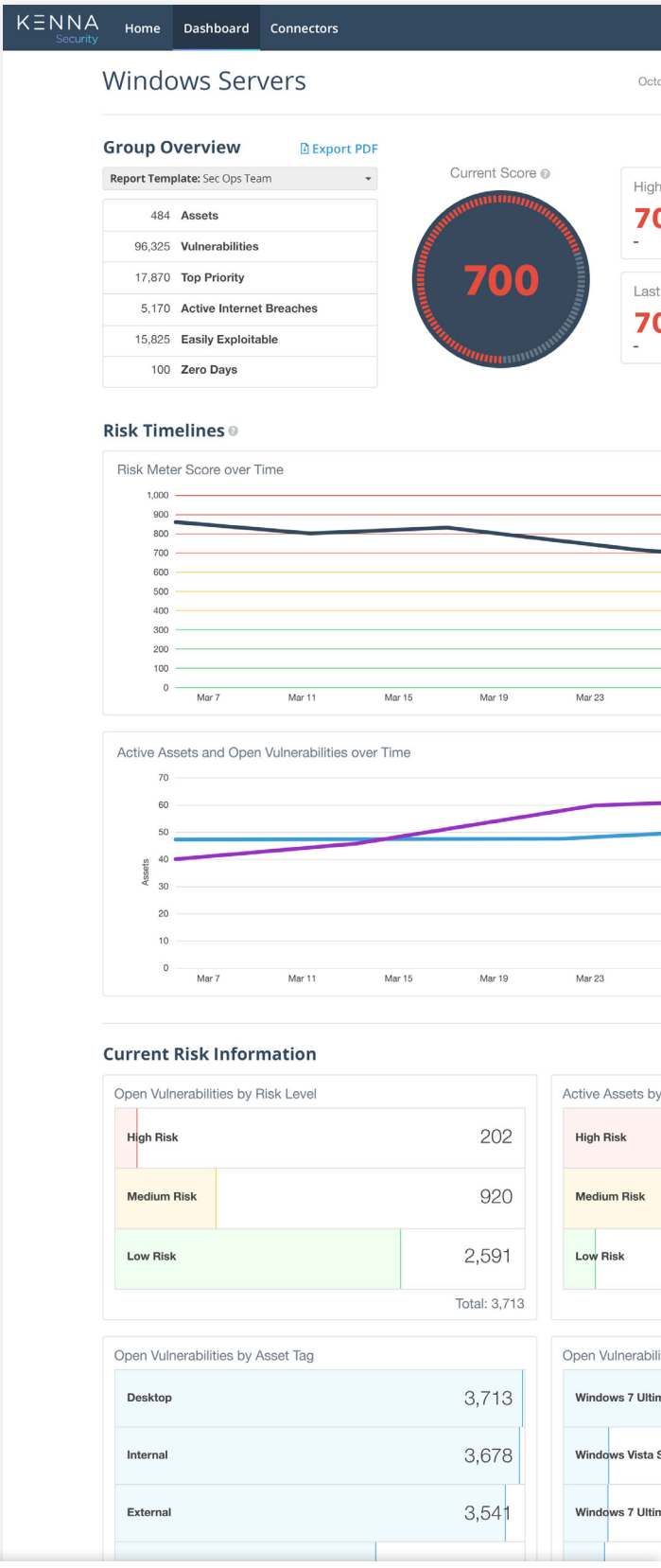
2. Vulnerabilities:

- What are the weaknesses and vulnerabilities tied to this asset or group of assets?
- How easy or difficult is it to exploit these weaknesses?

3. Threats:

- What are the threats associated with the security holes, as well as to your business?
- How skilled are your adversaries, and what skills are required to exploit your weaknesses?
- Are these vulnerabilities being exploited in the wild? How prevalent are they?
- Are you likely to be hit by a "drive by" attack?

Once you have a handle on this information, you can assign a single risk score to the environment. You can then drill down and assign scores to other important asset groups and categories. These scores will allow you to measure and monitor risk exposure over time. They can also serve as a valuable proof point when demonstrating efficiency, ability, and the need for additional budget and headcount.



Requirement #4: Know Your Resource Constraints

Once you understand the business, as well as its assets and security risks, you can begin to determine how you'll leverage your available resources (people, money, and time) to eliminate risks. Every organization has resource constraints. Understanding the resources at your disposal will help you prioritize your team's efforts.

Identify:

- What areas are most crucial for risk reduction within your business?
- What security risks are you carrying within those areas?
- What types and how many resources do you need to remove risk?

The goal is to optimize resource utilization to efficiently reduce risk.

Requirement #5: Know Your Direction

Continuously measuring against the metrics you've previously defined empowers you to understand the organization's direction and set meaningful goals to reduce risk over time and support business objectives. Establishing baselines will allow you to target areas of risk across the organization that are not within an acceptable range.

You can also quantitatively demonstrate to management what a reasonable risk reduction goal looks like and, if necessary, make the case for additional resources based on your organization's risk tolerance.

When tracking progress, avoid simply counting closed vulnerabilities. While these wins are important, the goal is to focus on reducing overall risk by optimizing available resources.

Useful Goal Metrics

1. Risk reduction by asset group over time
2. Risk goal by asset group
3. Cumulative risk accepted over time

Bonus: Know What's Coming

The goal of any vulnerability risk management strategy is to proactively close vulnerabilities. But once you meet the previous five requirements, you can take it a step further. You can go from being proactive to predictive. New vulnerabilities surface daily, each with differing threat levels. And, unfortunately, no organization has the resources to react to each vulnerability as it appears. Data-driven, reality-based predictive analytics can help you identify and close vulnerabilities that have a high likelihood of becoming future zero-day vulnerabilities.

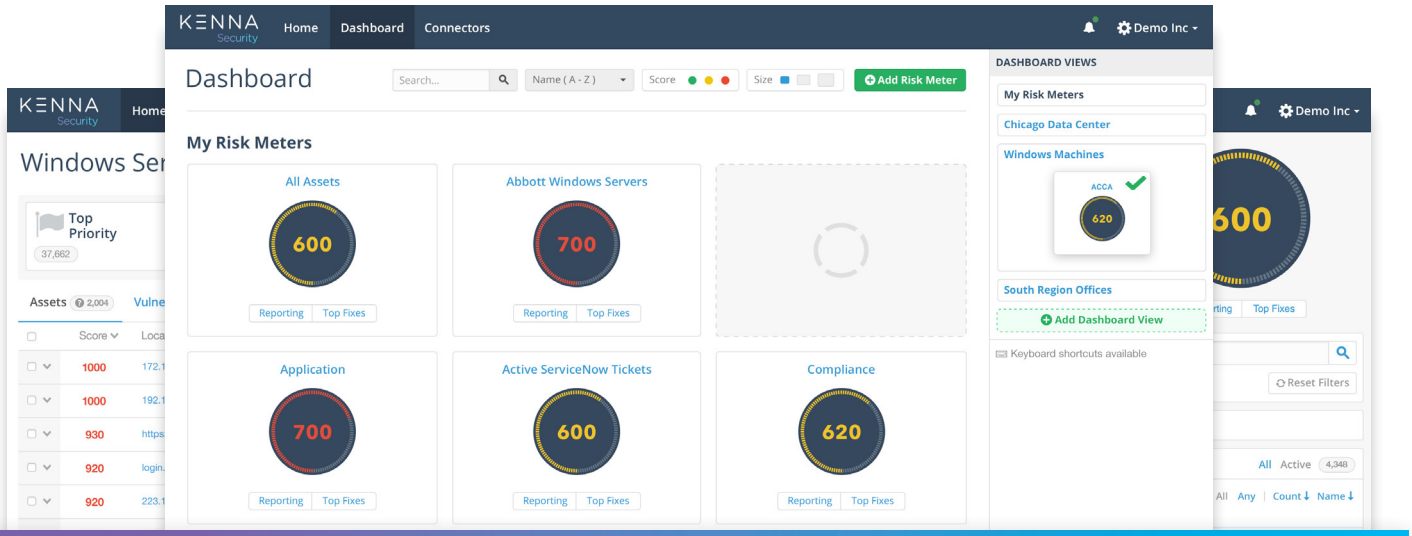
Focus on Patching the Right Vulnerabilities, Not Counting Them

It doesn't matter how many vulnerabilities you close at the end of the month if you're not closing the right ones. The Kenna Security Platform can play a key role in helping your organization analyze, correlate, and prioritize vulnerabilities so that you're closing the right ones at the right time.

At the center of the Kenna platform is a single risk score, calculated with advanced technology and real-world data, that serves as a compass for all risk operations. This score helps provide organizations with the steps required to reduce risk and understand the quantifiable impact each action makes on the overall risk score. With its data-based framework to rank vulnerabilities in order of urgency, Kenna offers security managers a mechanism to proactively manage and mitigate cyber risk operations.

Benefits of the Kenna Security Platform

- ✓ Reduce cyber risk by proactively focusing on high-risk vulnerabilities
- ✓ Increase IT efficiency by automating vulnerability analysis, correlation, and prioritization
- ✓ Obtain continuous, real-time visibility into the organization's risk posture
- ✓ Make data-driven investment decisions based on objective risk metrics
- ✓ Eliminate spreadsheets and home-grown apps with automated reports
- ✓ Monitor risk and measure improvement over time



To learn more about aligning your organization around risk
visit https://www.cyberbusinesssupport.com/
or email info@cyberbusinesssupport.com