PeerPaper Report

Risk-Based Vulnerability Management: Answering the Four Tough Questions

Based on Real User Reviews of Tenable Solutions

2020

IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

The evolution of IT has led to a parallel escalation in the potency of cyberthreats. Digital transformation, APIs, the cloud, mobility, and IoT contribute to a massive expansion in the cyberattack surface area. There is no more perimeter. Malicious actors can exploit vulnerabilities pretty much anywhere in the vast corporate digital ecosystem. Successfully reducing cyber risk means addressing four tough questions: How and where is the organization exposed to risk? What should the priorities be for risk detection and mitigation? What's the best way to operationalize risk remediation and track exposure over time? How does one's organizational risk compare to that of its peers? This paper offers answers, based on reviews of the Tenable Cyber Exposure platform on IT Central Station.

CONTENTS

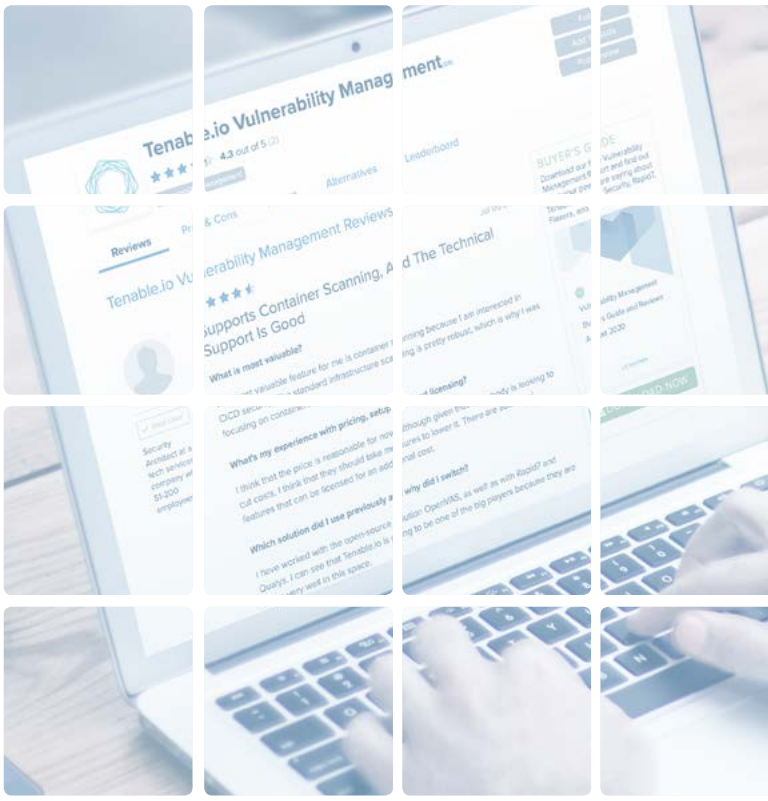
INTRODUCTION

Cyberthreats have grown in sophistication in recent years, exploiting technological advances that increase IT complexity. While innovations like IoT, mobility, and digital transformation are good for business, they contribute to a bigger attack surface area. The perimeter, once a bulwark of cyber defense, has more or less disappeared. Cyber risks abound, with vulnerabilities found on endpoints and infrastructure that span the globe.

It is possible to reduce these risks, but success involves addressing four tough questions: How and where is the organization exposed to risk? What should the priorities be for risk detection and mitigation? What's the best way to operationalize risk remediation and track exposure over time? How does one's organizational risk compare to that of its peers? This paper answers these questions, based on reviews of the Tenable Cyber Exposure platform on IT Central Station.

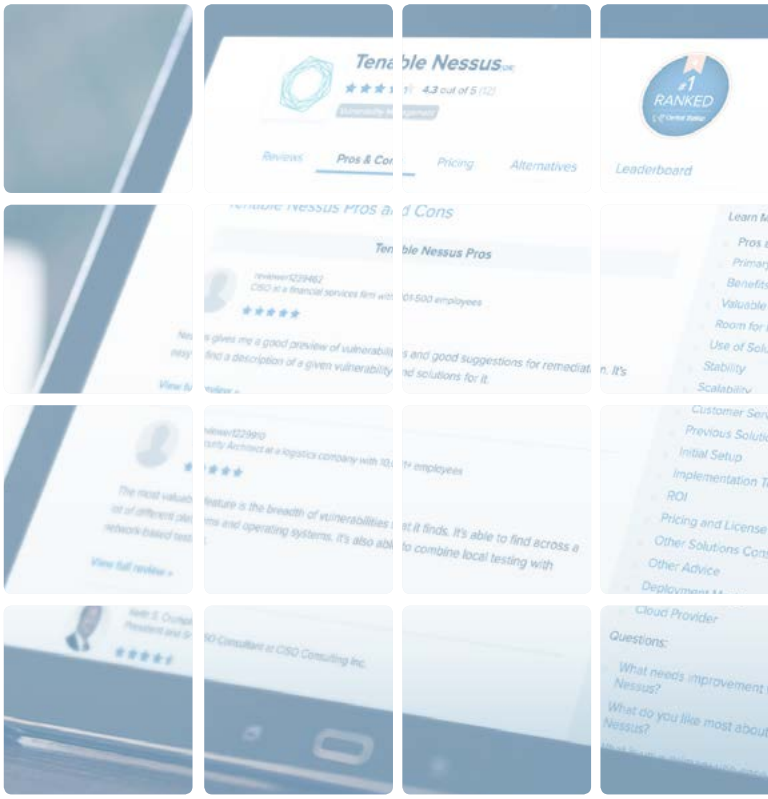
Cyber Risk: A Brief Overview

Information Security (InfoSec) is a familiar subject for most IT professionals. InfoSec is now cybersecurity, though IT departments and Security Operations (SecOps) teams are confronted with a far broader range of cyberthreats than ever before. These include highly sophisticated attacks from nation state actors and increasingly brazen cyber criminals. At the same time, the number of systems, environments, and endpoints — the attack surface — has widened considerably. Attackers can target mobile devices, servers, laptops, and WiFi network routers. They can try to disrupt operational technology (OT), such as industrial controls. Container environments (e.g. Docker) and cloud-hosted digital assets are also vulnerable to threats.



Answering the Four Tough Questions

Legacy risk reduction techniques cannot keep up with this sharp escalation in the number of new vulnerabilities discovered each year, coupled with the widening attack surface. Most legacy methods use the industry open standard Common Vulnerability Scoring System (CVSS) as their sole method for determining which vulnerabilities warrant attention. The most common approach is to prioritize remediation of every vulnerability with a CVSS base score of 7.0 and above.



This is a deficient practice, however. It is a waste of time because over half of all vulnerabilities fall into the 7.0+ category, and the overwhelming majority don't pose any risk. CVSS doesn't reduce the number sufficiently, causing security team workloads to quickly spiral out of control.

In contrast, a better risk-based approach to vulnerability management, as exemplified by the Tenable portfolio, solves these problems and enables security teams to focus on the vulnerabilities and assets that matter most. When combined with rigorous processes, this risk-based approach reduces the priority of vulnerabilities that are unlikely to be exploited. To implement such solutions effectively, though, it's necessary to address four challenging questions.

> **"... it's all out in the cloud so you don't have any infrastructure cost.**

How and Where is the Organization Exposed to Risk?

To reduce risk, one must first know where risk is present in the organization. This may sound obvious, but the complexity of modern IT infrastructure makes the task anything but easy. IT Central Station members have found a solution in Tenable products. A Director of Information Risk Management at a consultancy with over 1,000 employees uses Tenable.io "to perform truly continuous - in the sense that it never stops - unauthenticated scanning at the perimeter." Figure 1 depicts this process.

As he put it, "We use Tenable to monitor many dozens of technologies. For the most part, any database technology you can think of: multiple versions of Windows Server, Windows 10 on the workstation, High Sierra and Mojave for macOS, a bunch of different networking technologies. The list goes on." He also employs Tenable.io as part of his company's PCI controls, praising it because "it's all out in the cloud so you don't have any infrastructure cost."

A Senior Security Analyst at a tech services company with over 1,000 employees uses Tenable.io Container Security and Nessus Scanner for internal and external penetration testing activities. For him, Tenable has enabled pentesters to cut their testing time in half. According to a Senior Manager, IT Security at a financial services firm with more than 5,000 employees, "It reviews our threat landscape vulnerability. The key is to make sure that we are not exposed to vulnerabilities that can be exploited."

An Information Security Expert at a comms service provider with more than 5,000 employees "loves" the Tenable.sc (formerly Tenable Security Center) dashboard in this context because it performs vulnerability scanning and then outputs vulnerability data. A Senior Information Security Analyst at a financial services firm with over 1,000 employees remarked, "This solution has given us

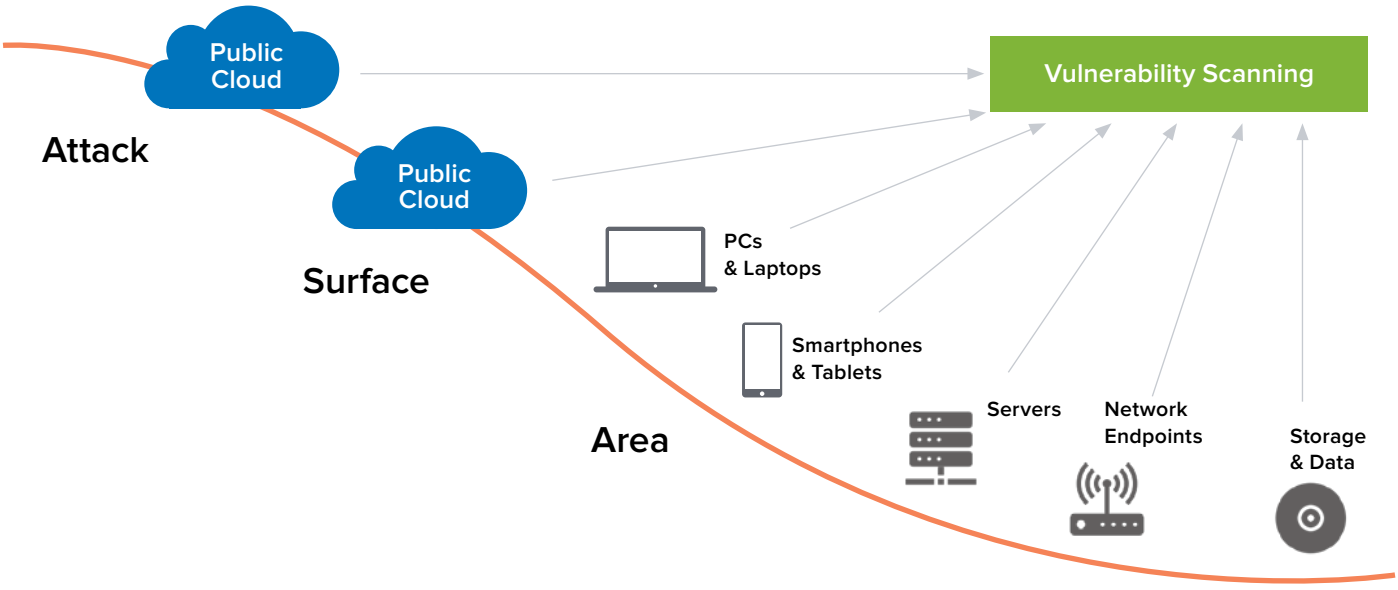


Figure 1 - The broad, never-ending attack surface area in today's organizations requires continuous vulnerability scanning

visibility of the vulnerability in our network."

For a Medical Device Cybersecurity Analyst at a large healthcare company, Tenable "helps to limit our organization's cyber exposure." He further stated, "In our environment there is a lot of stuff we can't deal with in terms of endpoints, but it has definitely helped in identifying the devices we have out there which haven't had Microsoft updates applied in years, potentially. It's really helped identify those, the low-hanging fruit. But then, you get into the devices that are relatively up-to-date but their vendor application has been the same for however many years. In the least, we're able to identify and understand which devices those are and what the risks are, even if we can't immediately address it."

> **It also shows what needs to be done to negate the vulnerabilities by providing links to the solution for those issues.**

An IT Security Specialist at a consultancy with over 1,000 employees shared that Tenable "helps us to understand our cyber-exposure. At the end of the day, if you don't know what you have, then you cannot defend against it. Understanding what services, what technologies, and all those components will also give us an idea about how to predict what kinds of attacks are the things that we need to guard against in the future."
A Sr. Principal IT Architect at a manufacturing company with over 10,000 employees similarly noted, "We are monitoring our infrastructure: servers, switches, storage, routers, SAN storage, operating systems and applications to the extent that the tool is able to see into them."

What Should the Priorities be for Risk Detection and Mitigation?

Awareness is a first step in managing and remediating vulnerabilities. Invariably, scans turn up more vulnerabilities than can be managed by the security team. As a result, one needs to prioritize remediation efforts by focusing on the vulnerabilities and assets that matter most. As the information security expert put it, "When you are working with one, two, three, up to 10 IT pieces of equipment, managing the vulnerability data would just be fine, but when you are managing assets across an organization of 10,000+ employees, you have a really hard time normalizing all that vulnerability data. The [Tenable] dashboard helps us out to map what things need to be prioritized, what is our current threat landscape and what would be the latest threats that we have in our network."

The financial services Senior Information Security Analyst further put the prioritization issue in perspective, saying, "It also shows what needs to be done to negate the vulnerabilities by providing links to the solution for those issues. Generally, we are now able to manage our vulnerabilities better. We can identify them, prioritize them, and

> **The dashboard helps us out to map what things need to be prioritized, what is our current threat landscape and what would be the latest threats that we have in our network.**

then negate them. It has improved our security posture." The IT Security Specialist added, "It also helps us focus resources on the vulnerabilities

that are most likely to be exploited. Looking at what actually has an exploit available along with consideration of other things such as network proximity times and information about the threat - either VPR [vulnerability priority rating] or CVSS - pulling all that together does allow us to identify pretty quickly what are the high-priority targets that we should work on."

> **It's good in that we see how each of these stacks up and where our priorities should be.**

Tenable.sc's Vulnerability Priority Rating stood out for the Sr. Principal IT Architect. He said, "It's a much more holistic view, instead of being very binary, which we tend to see. It lets us focus on what's most important to us, especially because it goes across many products that we have. It's good in that we see how each of these stacks up and where our priorities should be. Should they be in Cisco, should they be in Microsoft, should they be in Linux? That's very useful to us as well." He framed the issue by noting, "We'd love to do all the work right now, but we have to pick some type of priority in terms of what we're going to focus on, before we focus on the less vulnerable items."

The Medical Device Cybersecurity Analyst also praised Tenable's Vulnerability Priority Rating. He shared, "I run scans on all of our medical equipment and we have stuff that's still Windows 2000. Equipment is so expensive to upgrade and replace. I find a lot of it shows up red for vulnerabilities that we really can't do anything about. The predictive stuff helps prioritize some of those risks." Figure 2 shows the progression from scanning to prioritization, followed by operationalization of remediation.

What's the Best Way to Operationalize Risk Remediation and Track Exposure Over Time?

Once vulnerabilities have been discovered, assessed, and prioritized, it is then time to remediate those that pose the most risk to the organization. This is an operational issue. According to real user reviews on IT Central Station, Tenable products help with this challenging process. According to a Senior Information Technology Security Engineer at a large insurance company, "After the scans are done it goes out to a prioritization tool which applies some additional context and additional data to drive a risk score. Based on a threshold there, it's sent into ServiceNow where the team which owns the asset or the device will do the remediation. Most of the data they get comes directly from Tenable. It's just removed a couple of steps by going through those other platforms."

> **This solution provides a good reporting system and with a reasonably good level of third-party integration.**

A Network Security Analyst at a government agency shared, "I use Security Center currently to investigate daily network security events from reports I receive. Our network support team uses it to track, manage, and remediate system vulnerabilities." The Sr. Principal IT Architect also uses Tenable.sc's reports or the remediation recommendations for making changes to his organization's environment.

Setting the remediation process into motion is only one step in a bigger process. It's also necessary to track and report on risk exposure over time. A Tech Specialist put it like this: "This solution provides a good reporting system

and with a reasonably good level of third-party integration. McAfee has leveraged this capability beautifully in its Policy Orchestrator." The Medical Device Cybersecurity Analyst added, "For me, another useful feature of the tool is the dashboard and reporting. That is a big piece for me. The reporting covers most of my needs."

"The ability to trend data back as far back as we have disk space for, is helpful," said the IT Security Specialist. He then relayed "we've seen return on investment through visibility, scan stability, ensuring that we're able to assess our environment. Also, ensuring that we are able to have good confidence in the data, and that we're able to do out-of-the-box reporting and various other dashboards that really help us drive our program and help sell our case."

How Does One's Organizational Risk Compare to that of its Peers?

Benchmarking is an essential element of a mature vulnerability remediation program. Security professionals like to know how their results compare with those of peer organizations. Tenable enables such peer comparison. The Sr. Principal IT Architect framed the issue by saying, "They [Tenable] do a lot of research and we trust the research that they do internally. They have knowledge of what's going on with many companies, where we only get a view into what's going on here."

> **"... it allows us to reevaluate quickly if there are new vulnerabilities found.**

He then went on to explain that "we use it as a third-party — I don't want to say settle arguments — but as an expert opinion as to what is a true vulnerability, versus what is something that isn't as high of a priority. It takes opinion — if two cybersecurity people are arguing or discussing if this thing is more important than that thing — and, since Tenable is not invested in our company, it gives the best practice. It is very valuable in that sense."

This matters because "Tenable also helps us to focus resources on the vulnerabilities that are most likely to be exploited. And since it is continuously updated, it allows us to reevaluate quickly if there are new vulnerabilities found, versus ones that we're already working off and are already known to us." A managing partner at a small tech services company spoke further to this point, noting that Tenable is "something that allows us to quickly get a really important information context."

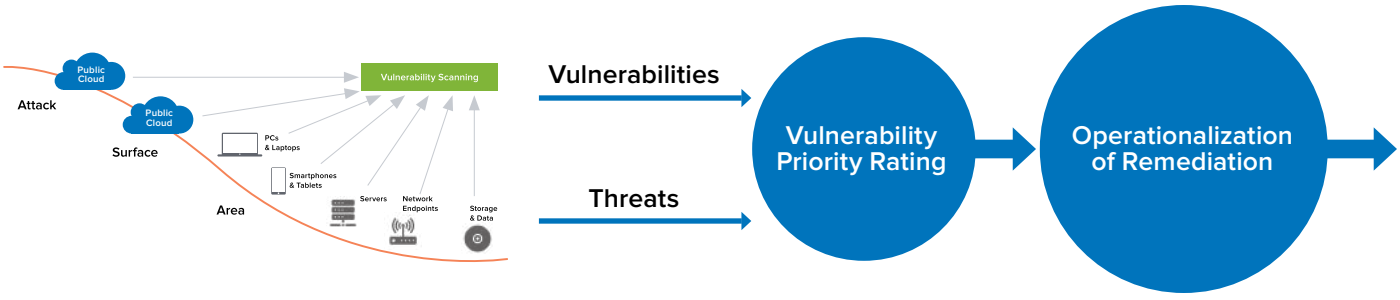


Figure 2 - Vulnerability scanning leads to the prioritization of risks to be remediated, followed by remediation processes, often executed with IT service management tools.

CONCLUSION

Answering the tough questions gives security professionals the ability to focus their time and efforts on the vulnerabilities that pose the most risk to the organization while deprioritizing those that are unlikely to ever be exploited. It starts with simply understanding how and where the organization is exposed, and correlating that information with what's most important to the business. This alone can be a significant achievement, given the complex and distributed nature of today's infrastructure. Then, it's about setting a priority for which vulnerabilities to remediate first.

With those priorities in hand, it is then possible to operationalize the vulnerability remediation process. Using a rich set of reporting and analysis tools, one can effectively communicate the team's efficiency – to gain and maintain management's confidence in the team's abilities. And, having the ability to compare the organization's level of risk against that of industry peers delivers a degree of context that helps security teams truly understand how they're doing. IT Central Station members who use the Tenable product portfolio have found that they can tackle these four challenging issues and emerge from the process with a stronger overall security posture.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform.

Tenable delivers the most comprehensive risk-based vulnerability management solution available to help organizations prioritize their remediation efforts to focus on the vulnerabilities and assets that matter most. We help organizations of all sizes make the most efficient use of their limited security resources by making the biggest impact on risk with the least amount of effort.

Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.