[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@67330866d87c49229ac0847c56e4d447?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

reference <https://www.secpod.com/blog/open-source-vs-commercial-vulnerability-scanners/>

**Open-Source Vs. Commercial Vulnerability Management Tools: How a Free Tool Carries Hidden Challenges**

Post author:[Pranav Krishnan](https://www.secpod.com/blog/author/pranavk/)

When vulnerability management started out as a practice 15 years ago, the  process was straightforward and simple in function. An IT admin would  download non-commercial open-source tools for free, scan his environment for the few disclosed vulnerabilities, and mitigate them manually. The  whole process would take months to complete, and that was still okay.

Fast forward to now, vulnerability management is now a full-blown business  process with dedicated resources to handle different aspects of the  program. Since 2015, the number of vulnerabilities disclosed has always  been in the thousands. Each year is setting a new record for the highest number of vulnerabilities disclosed in a year. Cyber-attacks have  increased in number and become more common. To top it off, software  vulnerabilities are now the leading cause of security breaches  worldwide.

If the open-source tools and traditional vulnerability management methods  work well, so many organizations wouldn’t be affected by ransomware and  data theft today. Open-source tools used to work perfectly in the past,  and they still do to some extent today. But it comes at a cost.

**Limitations of free and open source vulnerability Scanners**

Here are the most common limitations of open-source vulnerability management tools and the problems associated with them:

**1. No dedicated technical support**

Lack of timely and dedicated tech support is probably the biggest problem  with open source vulnerability scanners. Open-source scanners are mostly built by developers and testers to develop proofs of concept or to  automate some of their tasks. These tools have become popular among the  community because they are free, and people instantly start using them  out of curiosity.

But these developers/testers don’t invest in providing dedicated technical  support to their users. Users just have to rely on communities to ask  questions/problems or fix them themselves.

In some cases, the tools even get discontinued altogether. They struggle  with numerous bugs and feature limitations making these tools less  reliable in the long run. You cannot afford to spend time trying to fix  the tool when hundreds of vulnerabilities are lurking around in your  environment.

**2. Lack of detection comprehensiveness**

Many free tools are built to detect only specific vulnerabilities (CVEs). They usually don’t have access to a comprehensive vulnerability  database that can detect many publicly disclosed vulnerabilities. They  will also show a lot of false positives. Since they’re not developed and tested with the best technology, they will have bugs and compatibility  errors with some networks.

Some tools support only one or a few platforms like Windows or Linux. To implement vulnerability scanners for all your devices, you might be forced to configure and maintain many other  open-source scanners for your heterogeneous environment. Even though you might get away with no spending, you will lose a lot of time and resources making upgrades and maintaining custom code.

**3. Need for integrations for basic functions**

Open-source scanners can only go so far as to detect vulnerabilities in the  network. But they don’t provide any assistance to execute the steps that follow after detection, such as assessment, prioritization, patching,  etc. To continue the workflow, many security teams choose to manually  integrate their open-source or sometimes even paid scanners with  prioritization and patching tools.

Most organizations assume that integrations for vulnerability scanners are a de facto standard because of these limited functions. Data from the  vulnerability scanner is fed into a patching tool to execute the next  steps of the vulnerability management program. Setting up integrations  increases development and maintenance costs. Instead of focusing on  managing risks, teams spend more time integrating, managing and troubleshooting the tools.

**Advantages of a dedicated vulnerability management tool**

A commercial vulnerability management tool is designed and built with a  specific purpose in mind: to help detect a vulnerability and track it  all the way to mitigation in the most efficient way. Here are the  advantages of a dedicated vulnerability management tool:

**1. Dedicated support, good scalability, and intuitive design**

A commercial vulnerability management tool provides dedicated technical  support for you to resolve issues immediately since time is a crucial  factor in vulnerability mitigation. Technical support specialists who know every corner of the tool would be ready to help you get back on track as soon as possible.

Commercial tools are designed for easy expansion and management. The tool comes  with a graphical user interface to help you visually understand the  exact security posture and make faster and better decisions. As your  organization and the number of devices grows, onboarding new devices and handling more vulnerabilities will still be easy.

**2. Comprehensive and accurate vulnerability detection**

A dedicated vulnerability management tool is more comprehensive in the  number of platforms and devices it supports. All risks across your  environment are shown in one unified view. With a better idea of your  risks, you can derive actionable insights and act on them immediately.

A commercial provider of vulnerability management tools leverages an  up-to-date vulnerability database with all the latest security  intelligence. The scanner will detect all the latest vulnerabilities as  and when they are disclosed for the first time in public. You can feel  safe knowing that the tool actually reflects the true security posture and does not give you a false sense of security.

**3. Core functionalities to strengthen the vulnerability management process**

After a vulnerability is detected, it needs to be remediated by patching  hand-in-hand. In-built patching capabilities in commercial tools  simplify and speed up risk mitigation. Instead of feeding the data into  another tool, or worse, manually downloading and deploying the patches  in each device, you can readily deploy the patches from the same tool.

Compliance is a core part of a vulnerability management program. Industry and  organizational security standards mandate that devices are scanned  periodically for vulnerabilities and remediated effectively. Commercial  vulnerability management tools can detect and display compliant and  non-compliant devices. You can readily generate reports for compliance  audits easily.

**4. Additional features for practical advantage**

After vulnerabilities are detected, the next stage is to assess the risks and prioritize the order of remediation. In many cases, IT admins are left  to prioritize the vulnerabilities manually based on CVSS scores and  exploitation activity. A well-built commercial vulnerability management  tool takes care of this task for them.

All the detected vulnerabilities are smartly prioritized based on their  CVSS scores and multiple other factors. IT admins can be smart in their  remediation process by mitigating the critical vulnerabilities first and averting security breaches.

**The end-to-end vulnerability management tool is here**

An ideal vulnerability management tool should let you focus on fighting  vulnerabilities and not the tool itself. You should be able to handle  the entire workflow starting from detection to mitigation from just one  tool.

[SanerNow Vulnerability Management](https://www.secpod.com/vulnerability-management) is a unified cloud-based tool to handle all stages of your  vulnerability management program right from scanning to patch  deployment. You can:

* perform continuous and periodic scans over all endpoints and network devices in under 5 minutes
* leverage our homegrown, world’s largest vulnerability database with 160,000+ security checks
* assess and prioritize vulnerabilities based on the exact risk levels to your environment
* remediate the detected vulnerabilities with automated and integrated patching

If you’d like to know more about SanerNow, register for a [free demo](https://www.secpod.com/schedule-demo). We’ll show you how your security posture can be strengthened with a unified and improved vulnerability management tool.