FORTRA™

GUIDE (DIGITAL DEFENSE)

The Case for Enterprise-Grade, Risk-Based Vulnerability Management

Maybe you've heard that you need vulnerability management. Maybe you already have some sort of legacy system in place. But will that system be able to handle all that today's threat landscape will throw at it and can it keep up with your dynamic infrastructure? With so much at stake - IBM says the average cost of a data breach was $4.35 million in 2022 - it's more important than ever to know your organization is taking all the steps it can to manage risk. In short, you need the capabilities and efficiencies that enterprise-grade, risk-based vulnerability management provides. This guide explains why that is so crucial.

Why Vulnerability Management?

A vulnerability management program is far more than just a vulnerability assessment or vulnerability scanner. Everyone who has a computer on a network needs vulnerability management (VM) whether there are two devices on a local system or 10,000 on a global network. VM is a cornerstone, foundational activity for the security of any organization; it's at the core of all the layers that make up solid cybersecurity. The best VM programs use an ongoing process to regularly identify, evaluate, report, and prioritize vulnerabilities in network systems and software in dynamic environments. Organizations have evolving infrastructures and an ever-expanding number of endpoints. It's important to continuously assess weaknesses and remediate them so cyberattacks can be thwarted or at least their impact can be limited.

Why Enterprise-Grade?

Regardless of your network's complexity and composition, it's important to have a centralized, comprehensive view of it all, without having to manually cobble together a variety of reports yourself. An enterprise VM system will have the flexibility to handle all the permutations of modern organizations, including on-premise, cloud, or hybrid assets.

Enterprise-grade VM can:

- Scan local systems as well as the entire global network
- Segment reports into different locations, specific IT teams, departments across locations, and more
- Correlate data on dynamic assets
- Connect and integrate with other enterprise-level systems and tools
- Create efficiencies by being simple to deploy, learn, and maintain

Basic vulnerability scanners are outmatched by today's complicated threat landscape. Additionally, the shortage of cybersecurity professionals and the expertise gaps that result make it even more essential that your VM solution offer a robust set of features and produce prioritized, actionable results. This enables you to adequately optimize the resources you do have by focusing on the risks that matter.

Why Risk-Based?

Every system has vulnerabilities. Risk-based vulnerability management (VM) shows which ones really matter and helps you prioritize the most important remediation. One reason why critical vulnerabilities aren't being addressed consistently is the sheer volume of work heaped on IT departments. This is only compounded by basic vulnerability scanners that don't offer customized prioritization – the ability to prioritize by risk context specific to your business' infrastructure. . When it comes to vulnerability management, you need a system that can do more than tell you whether a security alert actually represents a threat or not. You need a system that can help you understand the level of risk to your unique network.

A good risk-based system will help you use the three pillars of information security - confidentiality, integrity, and availability - to gauge how much risk you can assume based on your risk tolerance. It does this by looking at how exploitable a vulnerability is and how important the exposed device or system is to your business. Quality VM systems combine this intelligence with real-world threat activity and industry-standard severity scores to rank threats and vulnerabilities. These provide additional metrics to help you evaluate exposure and prioritize remediation activities.

Other Functionality to Consider

Now that you understand the importance of an enterprise-grade, risk-based vulnerability management system, you may be wondering what else you look for when choosing the right VM system. Here are a few ideas.

✔ Platform Interface

While scans can be automated, not all fixes can. Technicians still need to do the work to address the vulnerabilities. That's why a prebuilt, intuitive interface is important. Plenty of scanners and other products can find vulnerabilities in your system. But a good interface is easy to use and helps your IT team create repeatable scans that deliver consistent results. As IT departments face turnover and staff shortages, there's no time to waste learning or trying to use a complicated, temperamental tool that could damage the network in the hands of an inexperienced tech.

✔ Historical Data

A good system will also deliver far more than just the current state of your network. For example, **historical data** isn't available on many VM tools in the marketplace. But knowing what assets have been impacted by a vulnerability, for how long, and what fixes have been attempted is key to accurate ongoing management. The length of the impact may also help other parts of the business assess impacts to customers, vendors, or other third parties. Historical data can also be useful when correlating assets that might have been masked by malware.

✔ Automated and On-Demand Scanning

Scanning is a key part of any VM tool. Best practice says scans should be run monthly at a minimum, or any time there's a change on the system. And systems are always changing. New vulnerabilities could be identified daily but they may or may not actually impact your network. Checking every vulnerability every day is time consuming and can bog down the network and operations but it can be automated with the right system. Sometimes it makes sense to automate, especially with a system that takes the additional step of assigning a remediation ticket to an IT team member. Other times, you need on-demand scanning to validate issues have been addressed, or demonstrate how long vulnerabilities were on the system, track certain KPIs, and more. This feature helps you respond to developing issues and maintain a level of control while also benefiting from the advantages of automation.

✔ Accuracy and Asset Correlation

Scans results need to be accurate and actionable. Enterprise VM solutions have the ability to distill results, **reducing false positives** that could otherwise waste your team's time. They also have the built in technology to match devices from scan to scan to properly gauge risk. Networks are dynamic and devices don't always have the same IP address, which is the easiest way to track devices over repeated scans. That's where **asset data correlation** comes in because it automatically tracks a device through the network and across changes without anyone having to manually match up devices each time. Without the consistency of scan-to-scan identification, machines that need fixing may be overlooked and fix attempts could be made on machines that don't need it. IT teams don't have time for that sort of inefficiency. A good VM system will also offer a variety of criteria for matching machines as well as sorting and searching results, so customers with unique needs can make manual overrides as needed.

✔ Data Management

Once the scans have been run and vulnerabilities found, the best systems will provide **data management** capabilities with a variety of ways to slice and dice the data. You should be able to **customize reports** and see actionable results anytime. The system should let you query against all scanned assets, see which devices haven't been scanned in a certain period of time, devices where fix attempts have been made, and more. This will give you the flexibility to manage and parse data so you can understand what needs to be done. Data management makes the scan results more valuable because it's easier and more efficient to work with them. While some systems require you to compile data from various reports and figure out how to create a spreadsheet or other report to pull all the data together, an enterprise-grade VM system will let you tag and label devices as well as reports so you can search and sort to deliver exactly the results you need.

✔ API

Systems that are **available via API** are even more beneficial, integrating into the broader security ecosystem. VM data can help enrich SIEM, SOAR, NAC and more. Integration with ticketing would allow a manager to apply a filter to return vulnerabilities that meet certain criteria and auto assign a certain tech to fix them then follow-up with automated validation activities. The manager can schedule a report for each tech to see what's been done and have near real-time visibility. Those filters should be saveable and the results deliverable in a variety of ways.

Overall, this is a good checklist when shopping for a VM tool. It may seem like a lot but there are systems out there ready to deliver all this and more for your IT team.

"Enterprise VM solutions have the ability to distill results, reducing false positives that could otherwise waste your team's time. "

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.