vicarius

vRx vs Tenable

Hero Statement

vRx dynamically provides partners and customers with the latest vulnerability data in their environments through real-time reporting. Threat actors won't wait until next quarter's vulnerability scan to start exploiting.

Comparison Paragraph

Tenable is much like Nessus with one key difference being that it is cloud-based. While that does address one issue, many of the same limitations apply.

vRx was built from the ground up for end-to-end vulnerability management. All of the steps in the process have a corresponding feature which we've designed to make each task as simple and time-saving as possible. Real-time vulnerability detection, automatic contextual prioritization, patch management for OS and 3rd party apps, and much more.

Competitive Advantages

1. vRx's continuous vulnerability discovery means your security teams will have the latest vulnerability data at all times allowing them to secure environments much more effectively than with point-in-time scans

2. vRx's Patchless Protection™ provides an additional security layer to ensure you're always protected even when there's no patch or update available.

3. vRx's scripting engine allows for greater flexibility when mitigating configuration-based vulnerabilities, deploying software, or performing any other IT and Security tasks you can dream up

4. vRx's intelligent prioritization takes the context of where each vulnerability exists within the environment along with a multitude of other data points. This automatically assigns a risk-based priority to each app, OS, and asset so your team can focus their efforts where it's needed most and ignore the noise of vulnerabilities less likely to be exploited in your environment.

5. Built-in patch management for both 3rd party apps and all major OS families enables IT teams to remediate vulnerabilities extremely quickly. Having this in the same vulnerability management platform allows for easy tracking of vulnerabilities from detection to remediation.

vicarius

Competitive Advantages Table

Feature	vRx	Tenable.io
Vulnerability Scanning	vRx is continuously detecting and reporting new vulnerabilities in your environment. Using lightweight agents and an intuitive cloud dashboard, you will always be informed of the current active CVEs in your environment at all times.	Tenable provides vulnerability scanning as its core function. It is primarily cloud-based which is its biggest difference from Nessus which is also a Tenable product
Vulnerability Remediation	vRx not only detects vulnerabilities but also has the tools to remediate them. Depending on the nature of the vulnerability, vRx has a corresponding mitigation method available.	Tenable is focused solely on vulnerability detection and does not offer any remediation for these vulnerabilities once detected.
Patchless Software Protection	vRx's Patchless Protection provides a compensating control to monitor and protect the most vulnerable apps where there isn't a patch available otherwise.	Tenable does not offer any advanced mitigation technologies such as Patchless Protection
Contextual Prioritization	vRx goes beyond basic vulnerability detection by analyzing and weighing additional risk factors associated with each vulnerability. From there, the prioritization engine automatically assigns an easy-to-read risk score so you know where your security and IT teams need to spend the most time and energy.	Tenable uses a proprietary vulnerability prioritization score called "VPR". It is largely based on external sources and predictive modeling rather than contextual information about where the vulnerability exists.

Patch Management	vRx makes patch management easy. OS and 3rd party app patches are automatically aggregated in vRx for you and can be installed on endpoints through one time patches as well as through automations.	Tenable does not offer any patch management functionality. This leaves out an integral part of the vulnerability management lifecycle and often results in an overall increase of risk compared to vRx's approach.
Continuous Assessment	vRx's agents report the latest vulnerability data to a cloud dashboard in real time. Vulnerabilities can be introduced into an environment through a new vulnerability being published, a new app being installed, and new devices joining the network. Not having to wait until the next scheduled scan to detect these is an important component in reducing organizational risk.	Tenable requires scans to be scheduled or manually kicked off, resulting in a point-in-time report of vulnerability data. Paired with a vast number of vulnerabilities and complicated patch cycles, this leaves gaps of time where vulnerabilities are undetected, allowing threat actors to exploit them.
Robust Reporting	vRx provides several reporting options so you can choose what works best for your organization. Exporting data to external sources like SIEM, Syslog, and Ticketing systems is possible as well as downloading executive and granular technical reports.	Tenable reports are highly detailed and complex to a fault. They can provide security teams with a great amount of information to triage and IT teams stuck in paralysis by analysis mode.
Great overall value	All of vRxs features are included for one price which is simply based on the number of agents. The reduction in risk and effort required provides partners and end customers with fantastic ROI.	Tenable has a fairly narrow scope and as such requires multiple other tools to match the functionality of vRx. This increases costs and complexity.