vicarius

vRx vs SentinelOne Ranger

Description

Vulnerabilities happen fast and you need a vulnerability management platform that can keep up, point-in-time network scanning alone is not enough. vRx continuously scans your environment and dynamically prioritizes based on context and predictive factors so you can respond rapidly and efficiently. Tie it all together with vRx's native patch management, automation, and patchless protection for a complete end-to-end solution and remove risks from your environment today.

Comparison

vRx is a real-time system, meaning you are always aware of the risks in your environment at any given moment. IT teams may read that and think "great, more time patching" but vRx has you covered - our dynamic prioritization takes known vulnerabilities, environmental context, threat intel feeds, and predictive analysis into account to prioritize risks so you are spending efforts where they are needed most. What's more, vRx has native patch management which can be automated to deploy patches on the frequency of your choosing, saving a ton of time and making you more secure.

Comparatively, Ranger is a point-in-time scan-based solution that is an add-on to the SentinelOne EDR agent. It allows for the discovery and visibility of networked devices and some risks they may have but lacks in prioritization and actionable remediation steps. To match vRx's capabilities with Ranger you would need multiple tools which increases cost, complexity, and risk.

Features and Use Cases

- **Vulnerability Discovery**

    a. **Inventory -** Before you can start removing vulnerabilities from your organization you must have a clear understanding of where the risks can exist in your environment. Having a dynamic app and asset inventory is a best practice in achieving this.

    How vRx handles it - vRx's agents take an application and OS inventory on every device it is installed on. This inventory is presented in our cloud dashboard where you can easily track which assets have which OS, 3rd party app, and which versions are present. This provides a great deal of insight to where specific versions of apps exist in your environment at any given time and when paired with the grouping and remediation mechanisms, it can lead to an efficient means of managing the remediation process.

Where Ranger falls short - Ranger is focused on a combination of active and passive network scans and while it can provide some visibility into networked devices and the traffic they are sending it does not include any inventory capabilities. This gap means that with Ranger, you will be lacking one of the most efficient ways to go from detection to remediation in your environment and you will also be lacking the wealth of insight that this inventory can provide your security and IT teams.

b. **Vulnerability Detection**

OS and App vulnerabilities - Vulnerabilities that exist in OS and applications make up a large portion of the vulnerabilities disclosed and exploited in the wild. This can prove to be one of the most common attack vectors due to user interaction and the fact that they are often desired targets by threat actors.

How vRx handles it - Once vRx's agents have taken a device inventory it correlates the detected OS and App version with leading vulnerability databases like the NVD. vRx agents are running scans continuously for any changes made on the host such as new applications being installed. These continuous scans paired with a feed from the most recognized vulnerability databases results in an almost unparalleled, real-time understanding of the vulnerabilities that exist in your environment at an given time. Additionally, because vRx is agent based it checks various data points to confirm the existence of a vulnerability offering a great deal more accuracy than a network scanner approach.

Where Ranger falls short - Ranger's scans are performed on a periodic point-in-time basis. This approach, when not paired with other methods leaves many gaps in a modern vulnerability management system.
More specifically, the gaps between scans can leave blindspots or openings for attacks - if a critical vulnerability is disclosed and your next scan is not scheduled for another week or more this leaves you vulnerable to exploitation. This approach lacks accuracy as it is based on network traffic for passive scans and active scans are looking "outside in" which is known to be less accurate than "inside out" scans from the hosts themselves. Hybrid, work from home, and cloud models have also decreased the effectiveness of a scan-focused approach and can leave more blindspots when compared to vRx.

- **Vulnerability Prioritization**

a. **Severity and Risk -** With over 22,000 CVEs last year and the distributed nature of workloads today prioritizing remediation efforts by CVSS and other external metrics alone is not enough. Using such dated methods leaves IT teams struggling to keep up with the sheer amount of remediations, it's not uncommon to see more vulnerabilities present in the next scan even after spending 10-20 hours a week patching with traditional toolsets and processes.

   How vRx handles it - Now that we have our inventory, asset list, and active CVEs vRx analyzes where the vulnerability exists in your environment in order to determine the likelihood of exploit. This contextual analysis based prioritization is the most effective for understanding the true risk of a given vulnerability, app, and asset which greatly helps IT teams "move the security posture needle" in a way that removes the need for manual effort. Our agents are detecting and analyzing these contextual factors dynamically - vulnerable app exists on a public facing web server? Likelihood of exploit, and thus risk, goes up. In calculating the risk score we also analyze the components of the applications to see if there are any components of the file structure, dlls, processes, etc that are common with Zero Day families or Common Weakness Enumerations which provides a predictive risk analysis.

   Where Ranger falls short - Ranger's prioritization is focused primarily on external factors which may not apply in your environment if compensating controls have been applied or if the asset is in a low risk VLAN that has very limited traffic for example. This approach creates a disjointed process and leaves both the security and IT teams with a lot more manual effort which not only increases cost but most importantly, risk.

- **Vulnerability Remediation**

a. **Patching -** The goal of any vulnerability management program is to remove risks from the environment. Many traditional approaches required multiple tools to handle the different stages of the Vulnerability Management lifecycle creating a siloed and disjointed process. Today we work with more OS's and 3rd party apps than ever before and patches are being released by these vendors more rapidly than before - due to this, having patch management as a native component of your vulnerability management toolset is more important than ever.

   How vRx handles it - vRx uses the application and OS inventory discussed earlier and compares that against the available patches from the vendor. In our dashboard, you see the patches needed in your environment, what assets they are needed on, and you can apply them. This capability is completely native to vRx and does not require any additional tooling or local services like Windows Update Service meaning you have complete control over this process and it is easier than ever to do so. Seamlessly go from viewing which patches are

available, selecting which ones you'd like to apply, where, and when and you're done - you'll no longer need to go to the vendor site, download the patch, create packages and push them out with outdated tools - it's all handled for you. Amplify the ease of use, reduce manual effort, and increase security further by doing this process with our Auto-Actions which are policy based automations to apply patches on the frequency of your choosing.

Where Ranger falls short - Ranger does not have any native patch management nor any remediation capabilities for that matter. Additionally, it does not integrate directly with any other patch management tools furthering the issues that are all too common with siloed, disjointed vulnerability management processes.

b. **Configuration based vulnerabilities and non-patchable vulnerabilities -** Another trend we have seen increasing over the past several years is configuration based vulnerabilities and also delays in vendors deploying patches to critical, named vulnerabilities.

How vRx handles it - vRx includes the ability to apply configuration changes via our scripting engine to mitigate vulnerabilities that are configuration based. Recently, we saw the 3CX supply chain attack exploit a vulnerability from 2013 that Microsoft had just re-issued an advisory on, this affects almost all versions of Windows and does not have any patch available - through our scripting engine we were able to detect the vulnerabile registry entry and mitigate it using the official recommendation from Microsoft, a DWORD entry in HKLM, if the vulnerable configuration exists and finally restarting the associated services to apply the fix without requiring a reboot. In cases where we want to apply a more dynamic mitigation, for example with end of life applications, we have our Patchless Protection. This is something we can apply in various intensity modes (Analyze, Monitor, or Protect) to monitor and stop malicious system calls being made against the application while maintaining its business function. This capability is extremely unique in Vulnerability Management platforms and provides a way to reduce risk via a compensating control when we would otherwise need to accept it.

Where Ranger falls short - As with the lack of patch management, Ranger does not include any ability to address configuration based vulnerabilities, nor reduce the risk around applications that may be end of life or not have a patch readily available.

Top 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 engine 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 capability in the same vulnerability management platform allows for easy tracking of vulnerabilities from detection to remediation.

Competitive Advantages Table

Feature	vRx	Ranger
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 on the current active CVEs in your environment at all times. In addition to the continuous scan performed by the agents, we also sync with NIST NVD continuously so you always know if the latest vulnerabilities exist in your organization. vRx is able to detect vulnerabilities across all major OS's (Windows, MacOS,	Ranger uses an existing S1 EDR to perform network scans primarily searching for rogue devices. Because the scan is periodic, you are susceptible to attack vectors that may be created in between scans like a new vulnerability or a user installing a vulnerable app as well as situations when a device may be offline during a scan. Because this uses existing nodes to scan for other networked devices it would only classify as an "outside-in" scan which can be less accurate and informative

	and Linux) as well as thousands of third party apps and	when compared to an inside-out scan.
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.	Ranger does not have any remediation capabilities, nor does it integrate with any remediation platform causing remediation processes to be siloed and potentially disjointed.
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 or mitigation available otherwise.	Ranger does not include any compensating controls to reduce risks.
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.	Ranger is able to display some severity factors for detected vulnerabilities.
Patch Management	vRx makes patch management easy. OS and 3rd party app patches are automatically aggregated in vRx for you and are able to be installed on endpoints through one time patches as well as through automations.	Ranger does not offer any patch management. This means you will need additional tools to address this stage of the vulnerability lifecycle with Ranger - this increases risk, effort, and costs.
OS/App Inventory	vRx fully supports all major OS's (Windows, Linux, and MacOS) as well as over 2700 apps across all OS's. This includes identifying	Ranger does not have any App or OS inventory making it incredibly difficult to properly understand the different risks in

	which patches are needed in your environment and installing them from the vendor repositories. Not only does vRx support all these OS/Apps it dynamically tracks and displays which ones exist in your environment, what version, and where - the first step in an effective vulnerability management program.	your environment.
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.	Ranger is based on periodic, point-in-time scans leaving potential for blindspots or gaps between scans.
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, Ticketing systems is possible as well as downloading executive and granular technical reports.	Ranger offers a dashboard to display scan analytics and several offline reports
Great overall value	All of vRx's 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.	With the lack of remediation, continuous assessment, and prioritization, Ranger does not offer the same value as vRx