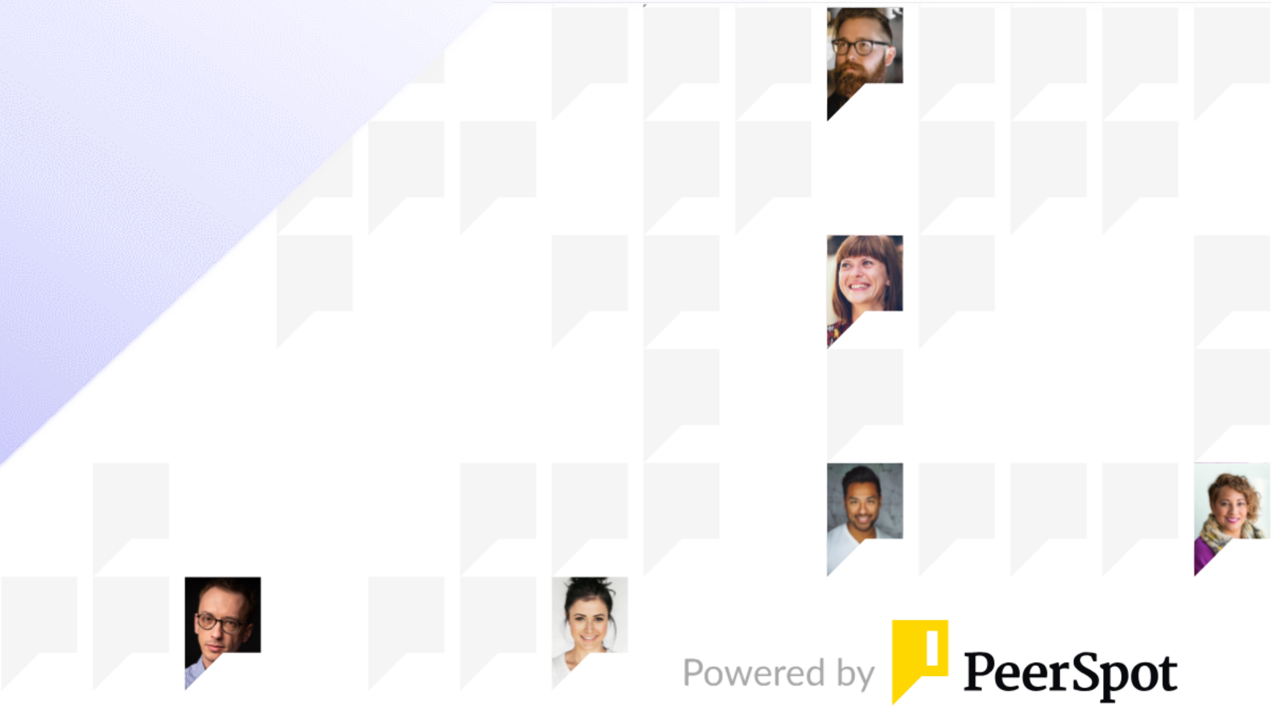
vicarius

Vicarius vRx

Reviews, tips, and advice from real users

March 2025



Powered by PeerSpot

Contents

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “I liked the initial dashboard.”

Verified user

Works at a manufacturing company with 51-200 employees

✓ “Third-party software patching is the most valuable feature.”

Billy-Turner

Vice President , Managed Technology and Security Operations at NovaCopy, Inc.

✓ “Patchless Protection helps protect us from vulnerabilities that may not yet have patches from the manufacturer. I've used it for a piece of software that we don't have a patch for. It monitors that software, analyzes it, and makes sure nothing nefarious is going on when it's vulnerable.”

MichaelCortez

Sr. Director of IT at Charter School Associates

✓ “Agent-based scanning is the most valuable feature.”

Wayne Ajimine

Information Security Professional at Hawaii State FCU

✓ “I like that vRx is cloud-based. It protects the health of applications against zero-day threats.”

Navdeep Saini

Principal Engineer at Blue HERON Technologies

✓ “The most valuable features of vRx would be virtualized patching and severity prioritization.”

Antwune Gray

VP IT Security and Services at netxinc

✓ “We can easily deploy patches for third-party applications. It automatically downloads the patches for you. You do not have to download them, upload them to the solution, and configure your own scripts or anything like that. It is all automatic.”

Verified user

Security Analyst at a manufacturing company with 1,001-5,000 employees

What users had to say about valuable features:

“I like that vRx is cloud-based.

It protects the health of applications against zero-day threats.
We tried patchless protection, but I don't think we've ever tested it.
I don't know if it's ever been triggered, but I believe we'll see a value from it the day it's triggered.”

Navdeep Saini
Principal Engineer at Blue HERON Technologies

Read full review

“I liked the initial dashboard.

I am not even sure if this feature worked, but it has a feature that allows you to put a bubble around systems on which you cannot deploy an agent.
That bubble around the system still gives them a level of protection.
I like this feature and the dashboarding capabilities.”

Verified user
Works at a manufacturing company with 51-200 employees

Read full review

“Agent-based scanning is the most valuable feature.

Previously reliant on network scanning, we faced limitations when devices were offline or remote, such as laptops.
This inconsistency in scan results is resolved through agent-based scanning, which provides more consistent data collection as long as the device has internet access.
Additionally, integrated patching is highly desirable.
While we have other software deployment and patching systems, their reliance on network connections creates similar inconsistencies in reaching all endpoints at scheduled times.
Agent-based patching significantly improves this process.”

Wayne Ajimine
Information Security Professional at Hawaii State FCU

Read full review

“We can easily deploy patches for third-party applications.

It automatically downloads the patches for you.
You do not have to download them, upload them to the solution, and configure your own scripts or anything like that.
It is all automatic.
The vulnerability dashboards are extremely helpful.
It can help us target the highest-priority vulnerabilities.
That is awesome and very helpful.
I have a server engineer who uses this very heavily.
She is used to her legacy solution.
She recommended some improvements to the interface.
They were just minor things related to scheduling and adding some more options to schedule patches that are deployed.
Their support was very open to the suggestions.
They implemented her recommendation.
Their support has been great to work with.”

Verified user
Security Analyst at a manufacturing company with 1,001-5,000 employees

Read full review

“The most valuable features of vRx would be virtualized patching and severity prioritization.

It provides that single pane of glass for vulnerability discovery, prioritization, and remediation, which leads to efficiency gains in most cases.
The user community is very helpful.
There are some incredibly talented good guys willing to help other good guys fight against the cybercriminals out there.
Some users have posted scripts that will be helpful.
Obviously, you would want to vet them, but from what I understand, Vicarius vets any scripts posted into the community.
There's added protection, and you feel confident you can utilize what other administrators or security professionals have posted to leverage the scripting engine, which is incredibly powerful.
The patchless protection component is an incredible technology that learns the behaviors of an application, detects an anomaly, and isolates that particular application if it misbehaves.
It is incredibly powerful because there are many applications out there for which you do not know whether there is a new patch available, or a new binary cannot be deployed because of the environment itself.
One feature customers have praised is the ability to stage packages and schedule tasks.
Having the vulnerability scanner as part of the platform also provides that confidence because it runs the vulnerability scan and shows that patch has been installed, that vulnerability has been mitigated, etc.

Antwune Gray
VP IT Security and Services at netxinc

Read full review

“We did not have any visibility before over the vulnerabilities that were within our network, other than what independent research provided.

We'd have to read news and blogs.
Now we have a simplified dashboard that highlights those vulnerabilities, including zero-days and the risk level of each vulnerability.
The dashboard has been really great.
We can now see trends.
We can see the vulnerabilities that are being detected and mitigated.
It's helped us with challenges in an educational organization.
It's made a big impact.
It's improved the level of flexibility we have to deploy patches.
We do get a lot more granularity and can see what kind of patches we want to deploy, the timeframe, and the groupings and various options we have for deployment.
If we had devices that only need a certain patch due to specific software and other schools don't, we can isolate out groups and deploy patches to specific groups.
The solution consolidates vulnerability discovery, prioritization, and remediation all in one single platform.
It eliminates the need for other services and simplifies management while expediting and streamlining vulnerabilities and patch management.
We've been able to reduce mean time to remediate vulnerabilities.
We're on a good schedule for implementing updates and patches based on the level of severity.
However, we can deploy patches on the fly if the need is severe and critical.
This is the first time we've implemented patch management in this organization, so I can't speak to how much time has been saved.
That said, prior to implementation, all patches were remotely handled by Windows updates.
The reduction in mean time has positively affected operations as it's made it easier on our side.

IT no longer has to manually research and do analysis.
That part is almost non-existent.
In the past, there was a lot of research into updates and trends.
Vicarius does all the hard work for us.
We get real-time, accurate information on the latest cybersecurity trends in order to respond accordingly.
They have a robust library of scripts that we can deploy as opposed to not just knowing there is a vulnerability but having to create a script.
We've been able to reduce the amount of time spent on patching.
We used to do it manually.
If it wasn't possible to do it through a Windows update or if the Intune process did not get the patch applied, we would have to try and get all devices across all organizations to the latest versions and make sure the software was also patched.
It's saved us an incredible amount of time.
We no longer have to touch those systems.
We can just rely on the automated system and the schedules we've set.
It's a huge time saver.
It's saved us hundreds of hours.
Patchless Protection helps protect us from vulnerabilities that may not yet have patches from the manufacturer.
I've used it for a piece of software that we don't have a patch for.
It monitors that software, analyzes it, and makes sure nothing nefarious is going on when it's vulnerable.
The scripting engine enables us to create custom scripts.
I haven't written any scripts; however, I have used it to push out an upgrade, for example.
They have a ton of scripts provided by the community.
Since I started with the solution, the growth of the library has been extensive.
I've been excited with what I've seen and I know I'll be able to use it in the future.

They have a great forum.

I haven't used it and haven't felt like I needed to, although I have used their FAQ and documentation, and that's been really helpful.

It's great for keeping our environment protected.

It does an extremely good job of patching everything we need it to."

MichaelCortez

Sr. Director of IT at Charter School Associates

Read full review

Product Impact

“Vicarius vRx helps consolidate multiple tools for patching and remediation. It's critical that Vicarius combines vulnerability discovery, prioritization, and remediation in a single platform. We selected it for that reason. It protects us well. We use other tools, but we always go back to Vicarius to ensure everything's in line.

It reduces the time needed to detect and remediate threats by about an hour. I would estimate it saves us about 20 hours each month that we can allocate to something else. ”

Navdeep Saini
Principal Engineer at Blue HERON Technologies

Read full review ↗

“The reason we went forward with this software is due to the fact that we needed a solution to patch servers, and it wasn't being done on a regular schedule.

We were using Microsoft Endpoint Manager to configure the update range for our devices across the organization. However, it wasn't getting all of the patches to the software we deployed regularly. We implemented this to supplement the updates alongside patch management. We didn't have a robust patch management solution which made the process of updating and installing cumbersome. Vicarius expedited the process for us.”

MichaelCortez
Sr. Director of IT at Charter School Associates

Read full review ↗

“With its vulnerability reports, vRx has provided confidence that systems are saving their patches. The customer has the assurance that they have mitigated some of those vulnerabilities there. It's also incredibly important to be able to detect missing patches and misconfigurations, missing registry keys, and things of that nature that help close some of the holes in an environment.

It has reduced the mean remediation time for our customers. We've had a few scenarios where customers have migrated from other patch solutions simply because they lacked confidence. There were additional requirements for verifying that the patch was rolled out or implemented successfully. By removing that additional layer of forced verification, vRx has certainly increased efficiency and the ability to implement those patches successfully.

VRx reduces the time customers spend on patching by reducing the overhead on the administrators, allowing them to do additional work. It saves time they would spend addressing the patching process, follow-ups, etc. ”

Antwune Gray
VP IT Security and Services at netxinc

Read full review ↗

“When we deployed it, it seemed like a fairly good tool, but we only scratched the surface. From one to ten, we probably only scratched about one, and we liked what we saw. People got ahead of themselves, not fully testing the tool, and that is the reason why we are in the situation we are in now.

It slowed down one of our main initiatives. It has not done anything. I like the concept of it being able to patch systems, keep them up to date, give a risk score, and things like that, but that is not what it was doing.

There was another team that was evaluating it too. We created scripts, but they did not work the way we thought they would.

vRx did not reduce our mean time to remediate vulnerabilities.

vRx did not reduce the amount of time we spend on patching. It increased our time because it did not work.

It was important for us that vRx consolidates vulnerability discovery, prioritization, and remediation in a single platform.”

Verified user

Works at a manufacturing company with 51-200 employees

Read full review

“Vicarius' ability to consolidate vulnerability discovery, prioritization, and remediation in one platform is extremely important and a fantastic time saver.

We have automated third-party patching on specific software, improving efficiency by 80 percent.

We saw the benefits of Vicarius vRx during our 30-day POC.

Vicarius is a critical layer in our cybersecurity strategy.

The patchless protection feature works well.

Vicarius' scripting engine enables us to create custom scripts to mitigate configuration-based vulnerabilities.

The ability to mitigate custom scripts has allowed for flexibility in some of the automation processes.

Vicarius has helped reduce our mean time to remediate by 80 percent.

Vicarius has reduced our patching time, which has improved our operations.

Vicarius is more robust than other solutions because it offers better third-party remediation.”

Billy-Turner

Vice President , Managed Technology and Security Operations at NovaCopy, Inc.

Read full review

“Vicarius is valuable because it combines vulnerability discovery, prioritization, and remediation into a single platform. Traditionally, these functions are separated and often managed by different teams, such as security teams handling discovery and infrastructure teams responsible for patching. This division requires significant coordination and communication regarding vulnerabilities, necessary patches, and prioritization. Vicarius streamlines this process by directly linking identified vulnerabilities to required patches, enhancing efficiency.

We have automated some of the patching using vRx's ability to perform that function. My infrastructure team handles the patching side, and we have shared access to the platform. I know that at least ten different tasks are automated, but I'm unsure if they've progressed even more. The gathering of patches that have been released, staged, and ready to go has been automated. So, all patches are already available, and we have some pre-done schedules that will automatically launch and start patching at predetermined times without further intervention.

The automation process has saved at least 30 percent of our manual tasks.

It takes two to three months to get a good overall vulnerability picture. The deployment takes a little while and some time to get used to the reporting. However, we saw decent data within two months and started asking questions about reporting and numbers. After three months, the overall dataset was good. Even now, we're still working on reporting, asking questions of Vicarius and trying to tweak some of the different reporting features.

Vicarius has helped us reduce our mean time to remediate vulnerabilities. Because we can examine endpoints, the best use case I can think of as an example for shortening remediation time is when we start spot-checking and looking at the dashboard for endpoints that, for some reason, have a high count of vulnerabilities or a much higher count of more severe vulnerabilities, we can immediately go into patching from that console and start pushing things out. So it helps us to immediately take care of delinquent workstations, for example, those that have not been connected or a person just keeps leaving their workstation off during prescribed patching periods. Overall, I would say remediation time is 25 to 30 percent shorter. The biggest impact is on case-by-case patching. We follow a regular patching cadence. We're a Microsoft shop, so the largest number of patches we have to apply, like most others, is on Patch Tuesdays when Microsoft releases stuff. Since that's on a regular cadence, I wouldn't say that Vicarius has greatly affected that. But there's a great improvement when we perform cleanup work and try to catch all the outliers and delinquent machines."

Wayne Ajimine
Information Security Professional at Hawaii State FCU

Read full review

ROI

Real user quotes about their ROI:

“I do not know if we can quantify that, but I know that we are saving hours of patching time, making our administrators more efficient, and getting our users back into the systems more quickly.

I am sure we are seeing a significant return on investment.”

Verified user
Security Analyst at a manufacturing company with 1,001-5,000 employees

Read full review

“We're an MSP, so we're always looking for new products to sell to our clients at a markup to make a profit.

You can explain the product's benefits in three or four minutes, and we don't need to push the clients very hard.
We already have seven or eight customers who use it, including one of our larger clients.
 We saw the benefits almost immediately because it's bringing us monthly profits, and it's an easy sell.
It's almost like some of them just wanted to sign up on their own without any push from the sales department.”

Jeremy Herman
Security Engineer at NovaCopy, Inc.

Read full review

Top Comparisons

Top Comparisons

Tenable Nessus

Compared 33% of the time

★★★★⯪

Microsoft Configuration Manager

Compared 10% of the time

★★★★⯪

NinjaOne

Compared 16% of the time

★★★★⯪

Microsoft Defender Vulnerability Management

Compared 4% of the time

★★★★☆

Microsoft Windows Server Update Services

Compared 9% of the time

★★★⯪☆

ManageEngine Vulnerability Manager Plus

Compared 4% of the time

★★★★⯪

SanerNow CyberHygiene Platform

Compared 6% of the time

★★★★⯪

Ivanti Security Controls

Compared 5% of the time

★★★★⯪

Vicarius vRx vs.

Tenable Nessus

★★★★½ ⓘ

Compared 33% of the time

Tenable Nessus and Vicarius vRx are prominent competitors in vulnerability management. Tenable Nessus holds an upper hand due to its extensive feature set and cost-effectiveness for larger enterprises.

Features: Tenable Nessus offers automated vulnerability detection, extensive database integrations, and predictive prioritization. Vicarius vRx provides unique patchless protection, automation features, and efficient patch deployment for third-party applications.

Room for Improvement: Tenable Nessus could improve in reporting, user interface, and extend support for scanning beyond basic network devices. Vicarius vRx can enhance network scanning, simplify reporting processes, and improve application management.

Ease of Deployment and Customer Service: Tenable Nessus offers on-premises and hybrid cloud deployments, with generally reliable customer service but some reported delays. Vicarius vRx uses public cloud deployment, which simplifies setup, supported by effective and responsive customer service.

Pricing and ROI: Tenable Nessus is cost-effective with subscription pricing for unlimited IP scanning, providing strong ROI by preventing security breaches. Vicarius vRx utilizes a per-asset pricing model, which is scalable but may appear more expensive.

Tenable Nessus provides an efficient vulnerability management system with swift deployment and comprehensive scanning capabilities, making it an ideal choice for organizations seeking to enhance their security posture through effective threat detection and mitigation strategies.

Renowned for its top-tier vulnerability detection, Tenable Nessus offers a robust platform that integrates effortlessly across systems, enhancing threat management through automation, real-time monitoring, and customizable scanning options. Its broad asset coverage, including network devices and applications, coupled with ease of deployment, positions it as a go-to option for risk assessment and compliance. Organizations value its extensive reporting features and database, although they suggest enhancements in reporting formats and false positive detection. A more intuitive interface, improved cloud support, and competitive pricing models are sought after to cater to evolving enterprise needs.

What are the key features of Tenable Nessus?

- Comprehensive Vulnerability Detection: Identifies security gaps across systems and platforms.
- Remedy Recommendations: Provides actionable insights for vulnerability fixes.
- Predictive Prioritization: Helps in focusing on critical vulnerabilities first.
- Seamless Integration: Compatible with diverse platforms for cohesive threat management.
- Automation Capabilities: Streamlines routine scans and reports.

What benefits and ROI should users look for?

- Fast Setup: Quick deployment that saves time and resources.
- Cost-Effective: Affordable pricing supports budget-conscious cyber strategies.
- Real-Time Monitoring: Offers continuous oversight of system health.
- Extensive Reports: Detailed insights enhance decision-making processes.

In industries such as finance, healthcare, and tech, Tenable Nessus is implemented for scanning internal and external networks, identifying risks, and ensuring data protection compliance. Organizations conduct regular scans to detect security vulnerabilities in servers and databases, leveraging its capabilities to strengthen their security frameworks while managing cloud infrastructures and enterprise networks efficiently.

Learn more about Tenable Nessus

Vicarius vRx vs.

Microsoft Configuration Manager

★★★★⯪ ⓘ

Compared 10% of the time

Microsoft Configuration Manager and Vicarius vRx operate in the IT management and security sector. Microsoft Configuration Manager has the upper hand in extensive device management, while Vicarius vRx shines in advanced security features and vulnerability management.

Features: Microsoft Configuration Manager includes patch management, application deployment, and compliance reporting with a centralized management console. Vicarius vRx offers vulnerability management, patchless protection, and automated threat response for zero-day vulnerabilities.

Room for Improvement: Microsoft Configuration Manager needs enhancements in performance, integration with non-Microsoft products, PowerShell capabilities, network deployment options, and reducing resource consumption. Vicarius vRx should simplify the patchless application process, improve login procedures, enhance network scanning capabilities, and streamline reporting.

Ease of Deployment and Customer Service: Microsoft Configuration Manager's on-premises deployment provides extensive control but complicates setup, with generally good technical support despite some delays. Vicarius vRx's cloud-based deployment offers easy implementation, backed by strong documentation and reliable customer service.

Pricing and ROI: Microsoft Configuration Manager is expensive with licensing complexities but offers cost savings through automation. Vicarius vRx is competitively priced, though smaller organizations might struggle without discounts. Both offer substantial ROI, with Microsoft's high cost contrasting Vicarius's scalable pricing.

Microsoft Configuration Manager helps IT manage PCs and servers, keeping software up-to-date, setting configuration and security policies, and monitoring system status while giving employees access to corporate applications on the devices that they choose. When Configuration Manager is integrated with Microsoft Intune, you can manage corporate-connected PCs and Macs along with cloud-based mobile devices running Windows, iOS, and Android, all from a single management console.

New features of Configuration Manager, such as the support of Windows 10 in-place upgrade, co-management with Microsoft Intune, Windows 10 and Microsoft 365 Apps for enterprise Servicing Dashboard, integration with Windows Update for Business, and more make deploying and managing Windows easier than ever before.

Learn more about Microsoft Configuration Manager

Vicarius vRx vs.

NinjaOne

★★★★⯪

Compared 16% of the time

NinjaOne and Vicarius vRx are competitive in the tech management landscape, each catering to distinct preferences and needs. Based on the comparison, NinjaOne seems to have the upper hand due to more positive feedback regarding deployment and customer service.

Features: NinjaOne excels in remote monitoring and management, provides a comprehensive toolset for IT management, and receives positive user reviews. Vicarius vRx stands out for its advanced vulnerability management features, proactively protecting systems, and robust security capabilities.

Room for Improvement: NinjaOne users often point out the need for better integration with third-party tools, a more intuitive navigation experience, and enhancements in reporting capabilities. Vicarius vRx users mention the need for enhancements in reporting capabilities, the occasional complexity in initial configurations, and improvements in customer service response times.

Ease of Deployment and Customer Service: NinjaOne is appreciated for its straightforward deployment process and accessible customer support, reducing setup time and resolving issues efficiently. Vicarius vRx is user-friendly in deployment but sometimes receives mixed feedback on customer service response times.

Pricing and ROI: NinjaOne is valued for offering a competitive pricing model that aligns with its feature set, often translating to a solid return on investment. Vicarius vRx's pricing might be higher, but its extensive security capabilities justify the expense, leading to satisfactory ROI for those prioritizing cybersecurity.

NinjaOne automates the hardest parts of IT, delivering visibility, security, and control over all endpoints for more than ***20,000 customers.***The NinjaOne automated endpoint management platform is proven to increase productivity, reduce security risk, and lower costs for IT teams and managed service providers. The company seamlessly integrates with a wide range of IT and security technologies. NinjaOne is obsessed with customer success and provides free and unlimited onboarding, training, and support. – Learn more here: https://www.ninjaone.com/

Learn more about NinjaOne

Vicarius vRx vs.

Microsoft Defender Vulnerability Management

★★★★☆ ⓘ

Compared 4% of the time

Microsoft Defender Vulnerability Management and Vicarius vRx are products in the cybersecurity domain, focusing on vulnerability management. While Microsoft Defender is better for integration within the Microsoft ecosystem, Vicarius vRx excels in broad applicability and vulnerability mitigation.

Features: Microsoft Defender features seamless integration with Microsoft tools, a comprehensive threat intelligence dashboard, and real-time alerts. Vicarius vRx offers granular control with predictive analytics, proactive security measures, and broad applicability across infrastructures.

Room for Improvement: Microsoft Defender could enhance cross-platform support, expand predictive analytics, and improve third-party tool integration. Vicarius vRx could improve its integration within specific vendor ecosystems, streamline alert interfaces, and provide deeper insights into Microsoft-specific vulnerabilities.

Ease of Deployment and Customer Service: Vicarius vRx is known for its straightforward deployment and responsive customer service, supporting diverse systems effectively. Microsoft Defender is well-integrated into Windows environments, easing deployment within Microsoft platforms while being less adaptive in multi-platform scenarios.

Pricing and ROI: Microsoft Defender offers competitive pricing for businesses using Microsoft's services, providing ROI through cost-effective security enhancements. Vicarius vRx's pricing aligns with its feature-rich offerings, offering robust ROI by focusing on advanced protection and cross-platform compatibility.

Microsoft Defender Vulnerability Management enables organizations to identify vulnerabilities, manage patches, and fortify threat detection. It offers endpoint assessments, cloud incident management, and dynamic security through Microsoft's Security Scorecard integration.

Organizations leverage Microsoft Defender Vulnerability Management for advanced threat detection and response. It provides robust tools for vulnerability assessment and cloud incident management, integrated with Microsoft's Security Scorecard to enhance dynamic security profiling. Key features include automatic patch deployment, security configuration management, and seamless integration with Microsoft platforms, benefiting both on-prem and cloud environments. Organizations can track vulnerabilities with severity-based reports, helping manage outdated software and minimizing threat exposure.

What are the key features of Microsoft Defender Vulnerability Management?

- Compliance: Ensures adherence to security regulations.
- Recommendations: Provides actionable advice for security enhancements.
- Inventories: Offers detailed inventory tracking for software and hardware.
- Threat Identification: Detects potential threats proactively.
- Vulnerability Assessment: Evaluates system vulnerabilities comprehensively.
- Zero-day Protection: Shields systems from newly discovered exploits.

What benefits should users look for in reviews?

- Integration: Facilitates seamless integration with Microsoft and diverse platforms.
- Risk Mitigation: Assists in mitigating risks through accurate assessments.
- Prioritization: Helps prioritize vulnerabilities for efficient patch management.
- Up-to-date Protection: Ensures systems remain secured and current.

In healthcare, Microsoft Defender Vulnerability Management helps manage compliance with health regulations, while in finance, it aids in securing sensitive data from cyber threats. Manufacturing sectors benefit from its patch management, keeping operational technology systems less vulnerable to disruptions.

Learn more about Microsoft Defender Vulnerability Management

Vicarius vRx vs.

Microsoft Windows Server Update Services

★★★½☆

Compared 9% of the time

Microsoft Windows Server Update Services WSUS and Vicarius vRx are competing products in the field of update and patch management. Vicarius vRx holds a slight edge due to its comprehensive features, while WSUS is favored for its pricing and customer support.

Features: WSUS is praised for its ability to distribute updates effectively, integration with other Microsoft products, and robust update management. Vicarius vRx stands out for its automated vulnerability management, real-time monitoring, and advanced security features, making it suitable for security-centric environments.

Room for Improvement: WSUS users suggest enhancements in reporting capabilities, better support for third-party product updates, and a more intuitive interface. Vicarius vRx users highlight the need for a simpler configuration process, more comprehensive documentation, and improved user manuals.

Ease of Deployment and Customer Service: WSUS is often cited for its straightforward deployment in Windows environments and reliable customer service. Vicarius vRx, while easy to deploy, sometimes requires additional learning resources for optimal usage. However, Vicarius vRx's support team is praised for responsiveness and expertise.

Pricing and ROI: WSUS is seen as cost-effective, particularly for organizations already invested in the Microsoft ecosystem, with a high ROI due to minimal additional costs. Vicarius vRx, while more expensive, delivers substantial ROI through extensive features and enhanced security measures.

Microsoft Windows Server Update Services (WSUS) is a patch management tool that simplifies the administrator’s task of deploying the latest Microsoft updates. Administrators use WSUS to manage the distribution of updates released through Microsoft Update to computers in their network.

WSUS has features you can use to manage and distribute updates from a management console. The WSUS server can also be a source of updates to other servers within the organization, acting as an upstream server.

Microsoft Windows Server Update Services Use Cases

The four main use cases that WSUS adds value to businesses are:

- Centralizes update management.
- Automates update management.
- Performs general patch management to ensure compliance and protect against vulnerabilities.
- Downloads all endpoint updates from data centers to a central location and then distribute them across the organization's network.

Microsoft Windows Server Update Services Features

This built-in server includes the following features:

- Includes Windows PowerShell cmdlets.
- Features client and server separation, which means you can deliver versions of the Windows Update Agent (WUA) separately from WSUS.
- Automatic download of updates.
- Deploy a targeted download of updates to a specific group of computers.
- Multiple language support.
- Advanced reporting capabilities.
- Centralized management of network resources.

Requirements

In order to be able to use WSUS to manage and deploy updates, it is important to use a supported WSUS version, such as:

- WSUS 10.0.14393
- WSUS 10.0.17763
- WSUS 6.2 and 6.3 with installed KB 3095113 and KB 3159706

Microsoft Windows Server Update Services Benefits

- Stable.
- Ensures servers are always patched and prevents vulnerabilities.
- Works great for internal updating.
- Enforces automated updates and patching for applications.
- Because the solution is used in the cloud, clients are always using the latest version.
- Highly scalable and configurable regardless of the organization's layout.

Different Types of WSUS Deployments

- **Simple WSUS deployment**: A server inside the corporate firewall serves clients via a private intranet. The WSUS server downloads updates by connecting to Microsoft Update. Using this model, you can configure multiple WSUS servers with a parent WSUS server.

- **Computer groups**: You can use computer groups to deliver updates to specific computers. There are two basic computer groups: All Computers or Unassigned Computers. When a client first contacts the WSUS server, it is added to both. You can then create a group from the Unassigned Computers group to the new group.

- **WSUS server hierarchies:** The flexibility of WSUS enables the creation of complex hierarchies of servers. To do this, you need only a single WSUS server connected to Microsoft Update. This will serve as an "upstream server," and the connected servers as "downstream servers."

    - You can link WSUS servers in two modes: autonomous or replica. In the autonomous mode, the upstream server shares the updates with the downstream servers but doesn't update status or group information.

    - The upstream server shares updates, status, and group information in replica mode. You cannot administer replica servers apart from the upstream WSUS server.

Learn more about Microsoft Windows Server Update Services

Vicarius vRx vs.

ManageEngine Vulnerability Manager Plus

★★★★½ ⓘ

Compared 4% of the time

Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step vulnerability management in your enterprise with Vulnerability Manager Plus.

Learn more about ManageEngine Vulnerability Manager Plus

SanerNow CyberHygiene Platform

★★★★½ ⓘ

Compared 6% of the time

SanerNow CyberHygiene Platform and Vicarius vRx compete in the cyber hygiene market. While users appreciate SanerNow for its pricing and support, Vicarius vRx is preferred for its superior features.

Features: SanerNow CyberHygiene Platform provides robust vulnerability management tools, automated patching, and comprehensive compliance reporting. Vicarius vRx offers proactive threat mitigation, integrated patch management, and advanced risk assessment features.

Room for Improvement: Users of SanerNow CyberHygiene Platform desire faster scan times and a more intuitive dashboard. Vicarius vRx users suggest better integration capabilities and enhanced reporting tools.

Ease of Deployment and Customer Service: SanerNow CyberHygiene Platform is noted for its straightforward deployment and responsive customer service. Vicarius vRx offers a flexible deployment model but needs improvement in customer support response times.

Pricing and ROI: SanerNow CyberHygiene Platform is seen as cost-effective with a quick return on investment, appealing to budget-conscious buyers. Vicarius vRx, while more expensive, offers significant features that users believe justify the higher cost.

SecPod's SanerNow CVEM prevents cyberattacks. It is a fully integrated, continuous, & automated platform designed to help enterprise IT Security Teams overcome security risks posed by vulnerabilities and misconfigurations. The solution offers seven modules driven by one agent & can be operationalized through an integrated cloud console.

SanerNow Continuous Vulnerability & Exposure Management (CVEM) platform offers an innovative approach to cyber-attack prevention and attack surface management.

SanerNow, with its CVEM capabilities, offers a new outlook on cybersecurity by evaluating enterprise IT infrastructure from a weakness perspective.

By integrating seven modules in one platform, the solution offers a unified approach to tackle IT infrastructure weaknesses - from scanning & detecting vulnerabilities & misconfigurations, asset exposure management, risk prioritization, patch management, endpoint management, and compliance management.

The seven modules are:

SanerNow AE: Discover and monitor usage of hardware and software assets in your IT network, manage licenses and more, daily.

SanerNow CPAM: Continuous assessment of 70+ anomalies on 2000+ data points of infrastructure/posture to detect outliers, trends, and security control deviations.

SanerNow VM: Detect, assess, and prioritize vulnerabilities on devices using industry's fastest scanner & world's largest security intelligence library of 160,000+ checks.

SanerNow CM: Detect and fix misconfigurations to harden systems and comply with regulatory standards or custom policies.

SanerNow RP: Prioritize risk of vulnerabilities, misconfigurations, and other weaknesses, remediate effectively.

SanerNow PM: Integrated patch management to automatically deploy patches for 30+ version of Windows, Linux, Mac OSs and 400+ third-party applications.

SanerNow EM: Get complete visibility into your endpoints and use 100+ security controls for software deployment, system tune-up, application & device control, and more.

The platform offers infrastructure inventory visibility, network anomaly normalization, detection, prioritization, remediation & system hardening of endpoints across every infrastructure layer.

It improves risk visibility beyond software vulnerabilities, expanding the scope of vulnerability management by monitoring more than 100 endpoint health controls, deploying/uninstalling software system health monitoring, eliminating rogue processes and applications, identifying malicious connections and devices, applying system-level security controls, system tuning, fix deviations and anomalies and building queries to get instant visibility to security risks.

Learn more about SanerNow CyberHygiene Platform

Vicarius vRx vs.

Ivanti Security Controls

★★★★½

Compared 5% of the time

Ivanti Security Controls and Vicarius vRx are leading endpoints and vulnerability management solutions. Vicarius vRx seems to have the upper hand for its advanced threat detection features and superior feature set which reflects its worthier investment.

Features: Ivanti Security Controls is valued for its thorough patch management, integration with various systems, and comprehensive patch management. Vicarius vRx is commended for its proactive vulnerability detection, user-friendly experience, and advanced threat management, giving it an edge in user reviews.

Room for Improvement: Users indicate that Ivanti Security Controls could enhance its reporting features, reduce its resource consumption, and improve documentation. Vicarius vRx users suggest better documentation, faster issue resolution, and enhancements in customer support response times.

Ease of Deployment and Customer Service: Ivanti Security Controls is praised for its straightforward deployment but receives mixed reviews regarding customer service responsiveness. Vicarius vRx earns high marks for its smooth setup and proactive support team, making it easier to deploy and better supported.

Pricing and ROI: Ivanti Security Controls is recognized for its competitive setup costs and respectable ROI. Vicarius vRx has a higher initial cost, but users report a greater return on investment due to its robust capabilities, making it the more cost-effective option in the long run.

Ivanti Security Controls simplifies security with unified and automated prevention, detection, and response techniques that target your biggest attack vectors. It provides the security global experts agree creates the highest barriers to modern cyber attacks, including discovery, OS and application patch management, privilege management, and whitelisting.

Learn more about Ivanti Security Controls

Recent Customer Reviews

Billy-Turner

Vice President , Managed Technology and Security Operations at NovaCopy, Inc.

Helps consolidate platforms, enable custom scripts, and improve operations

✓ Pros

“Third-party software patching is the most valuable feature.”

✖ Cons

“The multi-tenant portal has room for improvement.”

What is our primary use case?

“We use Vicarius vRx for vulnerability management.

We implemented Vicarius vRx because we were looking for a vulnerability scanning platform that did more than provide recommendations but assisted with remediation.”

How has it helped my organization?

“Vicarius' ability to consolidate vulnerability discovery, prioritization, and remediation in one platform is extremely important and a fantastic time saver.

We have automated third-party patching on specific software, improving efficiency by 80 percent.
We saw the benefits of Vicarius vRx during our 30-day POC.
Vicarius is a critical layer in our cybersecurity strategy.
The patchless protection feature works well.
Vicarius' scripting engine enables us to create custom scripts to mitigate configuration-based vulnerabilities.
The ability to mitigate custom scripts has allowed for flexibility in some of the automation processes.
Vicarius has helped reduce our mean time to remediate by 80 percent.
Vicarius has reduced our patching time, which has improved our operations.

Vicarius is more robust than other solutions because it offers better third-party remediation.”

What is most valuable?

“Third-party software patching is the most valuable feature.”

What needs improvement?

“The multi-tenant portal has room for improvement, but the changes we would like to see are on the roadmap.

.”

For how long have I used the solution?

“I have been using Vicarius vRx for one year.”

What do I think about the stability of the solution?

“We have not had any stability issues.”

What do I think about the scalability of the solution?

“Vicarius has met all of our scaling requirements.”

How are customer service and support?

“The technical support is excellent.”

Which solution did I use previously and why did I switch?

“We did proof of concepts on other leading vulnerability scanners.

vRX was the clear winner.
.”

How was the initial setup?

“The deployment was straightforward and very intuitive.

After setting up deployment scripts in our RMM, we can be up and running in less than an hour on new clients.
.”

What about the implementation team?

“The implementation was completed in-house with the assistance of Vicarius.”

What's my experience with pricing, setup cost, and licensing?

“The pricing is very fair.

.”

Which other solutions did I evaluate?

“We evaluated ConnectSecure, Nodeware & Rapid Fire Tools.”

What other advice do I have?

“I would rate Vicarius vRx nine out of ten.

After deployment, Vicarius requires minimal maintenance to monitor for any failures.
I recommend that my colleagues using a different patch management tool compare Vicarius with it.

New users should be prepared to find many vulnerabilities in their UC network when implementing Vicarius.”

Which deployment model are you using for this solution?

Public Cloud

Jeremy Herman
Security Engineer at NovaCopy, Inc.

Patchless protection is a feature no other products have, but the login process has unnecessary steps

✓ Pros

“I also like how easy it is to use. We instructed some companies on how to use it, provided them with an account, and gave them the ability to deploy and patch. They could quickly figure it out. We can spend an hour in the office showing someone how everything works, and they're good to go. It's the same with our customers.”

✖ Cons

“Another complaint we've gotten is that the portal doesn't remember your username and password. You tell them your email, and it sends an invitation. You need to click that, and it takes you to a new portal, where you can finally log in. Maybe it's a security precaution, but it seems like a lot of extra steps to log in.”

What is our primary use case?

“We're an MSP managing about 300 companies.

I am responsible for seven of those.
We're primarily using Vicariuse to protect against vulnerabilities and malware.
.”

How has it helped my organization?

“One of Vicarius' biggest benefits is patchless protection, which enables us to address vulnerabilities in applications that do not have a patch yet.

This has reduced our remediation time.
To start with, it's easy to deploy the agents to the endpoints.
Once they're deployed, you can patch whichever application you want with one click.
You can also automate updates and patching with scripts.
We can complete all these tasks in a quarter of the time.
In the past, we spent maybe 25 percent of our time patching because we had to write the automation scripts, push them out after hours, and ensure the patch was applied correctly.
With Vicarius, I've never seen a patch that failed or had to be rolled back.
We're saving quite a bit of time.
Our clients using vRx haven't had any issues, and they've easily established patching for all their endpoints.
If there aren't any problems, I assume it's doing its job and protecting the endpoints.

.”

What is most valuable?

“My favorite feature is patchless protection.

It's the primary reason we decided to use Vicarius.
It can block malware for applications that don't have current patches.
We were less interested in having a solution that could do multiple features simultaneously because we already have existing solutions for vulnerability scanning.
We were looking for something that could patch a wide variety of applications easily.

I also like how easy it is to use.
We instructed some companies on how to use it, provided them with an account, and gave them the ability to deploy and patch.
They could quickly figure it out.
We can spend an hour in the office showing someone how everything works, and they're good to go.
It's the same with our customers.
.”

What needs improvement?

“One difficult thing is all the name changes.

I sometimes get confused about what the product is called.
It's called connect in some places and vRx in others.

When you log into the website, it says it's in beta, which confuses me because it seems like a full-fledged product.
 Another complaint we've gotten is that the portal doesn't remember your username and password.
You tell them your email, and it sends an invitation.
You need to click that, and it takes you to a new portal, where you can finally log in.
Maybe it's a security precaution, but it seems like a lot of extra steps to log in."

For how long have I used the solution?

"I have used Vicarius for seven months."

What do I think about the stability of the solution?

"I rate Vicarius vRx eight out of 10.

We haven't experienced any crashes or lagging.
Initially, I was concerned about how deploying five or six patchless protections to an endpoint would affect resource usage.
However, I tested it with 30, and it didn't seem to degrade the quality or use a ton of resources.
I don't think I've reached the limit."

What do I think about the scalability of the solution?

"I give Vicarius vRx a 10 out of 10 for scalability.

It's infinitely scalable.

When we add a new company, we can deploy to their endpoints without any problems.
Deploying to multiple tenants is effortless.
.”

How are customer service and support?

“I rate Vicarius support eight out of 10.

I've only contacted them once with a question.
They were very responsive.
They got back to me in an hour or two.
I can't remember the issue, but they resolved it quickly.
.”

How was the initial setup?

“Vicarius vRx is very easy to deploy.

We did it all in-house because it's simple.
I deployed it alone.
After playing with it for around an hour, I could start deploying it to endpoints.
You don't need a consultant or anything.
They have it for Linux, too.
If I recall correctly, the Linux deployment was a little trickier.
The Windows-based deployment was much simpler.
After deployment, it doesn't require much maintenance.

.”

What was our ROI?

“We're an MSP, so we're always looking for new products to sell to our clients at a markup to make a profit.

You can explain the product's benefits in three or four minutes, and we don't need to push the clients very hard.
We already have seven or eight customers who use it, including one of our larger clients.
We saw the benefits almost immediately because it's bringing us monthly profits, and it's an easy sell.
It's almost like some of them just wanted to sign up on their own without any push from the sales department.”

What's my experience with pricing, setup cost, and licensing?

“The price of vRx seems fair.

None of our clients complained about the pricing.
They all thought it was reasonable.
Once people understood what it does, it didn't take much to get them to sign up.”

Which other solutions did I evaluate?

“We didn't consider anything else.

We already have multiple layers of security and several patching tools that are giving alerts and updating with malware signatures.

We never compared vRx with a short list of other products.
It had features that we didn't already have, so we signed up for it."

What other advice do I have?

"I rate Vicarius vRx seven out of 10.

It's a relatively new product, so I could increase my rating as they add more features.
If you already have a vulnerability patching tool, I recommend using both to see if you like it more.
I haven't seen another product with patchless protection.
If you are considering vRX, I suggest talking with the Vicarius team.
The vRx team doesn't seem very large, but I think that's normal because the product is pretty new.
Talk with someone there and do a trial or schedule an hour-long meeting.
That should be enough time, so you don't have to click around on your own and figure it out.
Have one of the vRx employees walk you through setting up a deployment and adding a tenant.
It'll save you time in the end."

About this buyer’s guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot’s team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report… Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you’re already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944