vicarius

Vicarius vRx Support Lifecycle Management



Introduction

Vicarius is committed to providing robust, enterprise-grade support throughout the entire lifecycle of the vRx vulnerability remediation platform. Vicarius vRx is a cloud-based (SaaS) solution with an intuitive dashboard console and supporting on-premises components (lightweight agents on endpoints and an optional proxy server).
This document outlines how Vicarius supports customers from initial onboarding through ongoing operations, including maintenance of the SaaS console, update management for agents and proxy, and comprehensive technical support. It details the support structure, service level commitments, release and update policies, and proactive practices in place to ensure vRx operates reliably and effectively for the long term.
The information below is structured to meet the expectations of IT procurement, InfoSec, and operations professionals evaluating Vicarius for mission-critical deployments, with clear sections addressing each aspect of the support lifecycle.

This document is intended to provide helpful information about current product support timelines and policies. While we aim to keep this information accurate and up to date, it is subject to change over time as our offerings evolve.
Please note that this document does not create any legal rights or obligations. For specific terms related to your use of our services, including support commitments, please refer to your applicable customer agreement or subscription terms.

Onboarding and Deployment Assistance

Structured Onboarding Process

Upon purchase, Vicarius initiates a guided onboarding program to ensure a smooth deployment and configuration of vRx. A dedicated Customer Success Manager (CSM) (or certified partner, if applicable) reaches out to the customer immediately after licensing to coordinate next steps . Vicarius confirms the customer's cloud tenant is provisioned or upgraded from trial to the full production license (with any licensing start dates honored). The CSM and support team provide an overview of the onboarding phases, which typically include planning, deployment, configuration, training, and post-deployment review.

Deployment Planning and Prerequisites

Vicarius works with the customer's team to prepare the environment before deploying vRx agents. This includes reviewing system requirements and network prerequisites (e.g. confirming which ports and addresses need to be allowed for the vRx service to communicate, and any antivirus exclusions for agent processes) . The support team provides guidance on best practices for organizing assets (such as setting up Asset Groups and tags) to align with the organization's structure and patching cycles . If the customer's endpoints do not have direct internet access, Vicarius advises on deploying the vRx on-premises proxy to enable secure connectivity for agent updates.

Agent and Proxy Deployment Support

During deployment, Vicarius assists with installing vRx agents on Windows, Linux, and macOS via manual or automated methods (e.g., Group Policy, Intune). For environments needing local caching, Vicarius supports setting up the vRx Proxy (Ubuntu-based) and configuring it in Forced, Failover, or Fallback mode. Engineers help troubleshoot installation or connectivity issues to ensure agents register with the console and the proxy operates as intended.

Initial Configuration and Training

After deployment, Vicarius assists with configuring vRx to align with the customer's environment. This includes setting up asset hierarchies, RBAC, vulnerability scan schedules, SAML SSO, and SIEM integrations. Training sessions cover dashboard use, remediation workflows, and reporting. Onboarding concludes once core use cases like running scans and deploying patches are validated. Vicarius documents configurations and remains available for follow-up as the customer moves into steady-state operations.

Technical Support Channels and Escalation

Multiple Support Channels

Vicarius offers multiple integrated support channels to ensure customers receive timely and effective assistance based on their preferred method of communication and the nature of their request.
These channels are fully integrated into Vicarius's support operations, ensuring continuity, accountability, and consistent service regardless of how the request is initiated.

Support	Knowledge Consultation
Manned chat support	Assistance using Remote Desktop and a VPN where available
Monitored email support - support@vicarius.io	Planned or Emergency assistance (Extra costs apply)
Ticketing system - https://customer-portal.vicarius.io/portal	Knowledge Base: https://customer-portal.vicarius.io/

Support Availability:

Support Channel	Days	Hours (UTC+3)	Notes
Chat Support	Sunday	11:00 AM – 8:00 PM	Chats outside office hours forwarded to mobile; best effort response. Backup voicemail service in place
	Monday - Friday	24 hours	
Email Support	Sunday	11:00 AM – 8:00 PM	Emails sent outside of core hours will be collected. Action may not occur until the next working day.
	Monday - Friday	24 hours	

Support Tiering and Expertise

This tiered model ensures that routine matters are resolved quickly at the first line, while more complex problems receive attention from the appropriate experts without delay.

Support Tier	Role	Responsibilities
Tier 1	Front-Line Support Engineers	Initial triage of issues - Handle usage questions and common troubleshooting, assist with configuration and known issues
Tier 2	Senior Technical Support / Product Specialists	Analyze complex issues - Access advanced diagnostics, resolve problems beyond Tier 1 scope
Tier 3	Development and Engineering Team	Address critical defects - Provide code-level fixes or product-level interventions
Escalation	Support Manager / Customer Success Manager (CSM)	Monitor unresolved or high-impact issues - coordinate internal escalation, ensure timely resolution and accountability
Customer Path	Escalation Request (upon customer need)	Customers may request managerial escalation for unresolved concerns or dissatisfaction with issue handling

Vicarius ensures seamless tier escalation and keeps customers informed throughout. For high-impact or delayed issues, support leadership monitors progress and can allocate extra resources. Customers also have a clear escalation path to request managerial oversight, ensuring accountability and timely resolution.

Communication and Remote Assistance

Throughout the support process, Vicarius emphasizes clear and timely communication. Upon receiving a support request, an acknowledgment is sent and a support engineer is assigned. This engineer will communicate updates, findings, or requests for additional information to the customer on an ongoing basis.

Knowledge Base and Self-Service

Vicarius offers a rich knowledge base and documentation portal for self-service help . This online repository contains user guides, how-to articles, troubleshooting tips, and FAQs covering all aspects of vRx from deployment and integrations to remediation techniques and common error resolutions. The knowledge base is continuously updated with new content as the product evolves and as new support cases yield insights. Customers are encouraged to use this resource to quickly find answers or to learn best practices.

Service Levels and Response Commitments

Incident Severity Levels

Vicarius aligns its service request handling with industry-standard ITIL practices, categorizing support tickets by severity/impact to ensure appropriate prioritization. The Service Level Agreement (SLA) for vRx defines clear severity levels and target response times for each

Severity	Description	SLA
Critical	Issue is causing downtime/malfunction in production environment e.g., service is completely unavailable	Max 1 hour to respond
High	Issue is affecting the service of production environment e.g., significant number of agents don't communicate with the tenant	Max 4 hour to respond
Medium	Issue is affecting the service of Dev environment e.g., a specific app does not have patches available	Max 24 hour to respond
Low	Any other question/issue e.g., Typo in the UI	Max 3 days to respond

These response SLAs refer to the maximum time for the **initial response** by a support engineer. In practice, Vicarius often responds faster (especially via live chat, where initial responses are typically within minutes during support hours). The response entails acknowledging the issue and beginning troubleshooting. Resolution times will vary by issue complexity, but Vicarius endeavors to resolve problems or provide mitigation as quickly as possible, keeping the customer informed of status at regular intervals.

Service Request Handling and Resolution

Stage	Action / Description	Data Collected / Output
Ticket Creation	Customer submits a service request via chat, email, or portal.	Ticket is created in the system with problem description, customer details, and scope of impact.
Issue Identification	Support engineer reviews the issue, confirms context, and performs initial triage.	Logs, screenshots, error messages, asset details, and environment information gathered from the customer.
Initial Response	Engineer attempts to resolve using known solutions or adjusts configuration.	Reference to KB articles, config changes, or first-response resolution actions documented in the ticket.
Escalation (if needed)	If not resolved, the issue is escalated per support tiers (Tier 2 or Tier 3) for deeper investigation or code-level fixes.	Escalation logs, assigned specialist notes, and diagnostic findings added to the ticket.
Investigation & Resolution	Support works through diagnostics and applies solution or mitigation (e.g., config fix, patch, hotfix, firewall guidance).	Resolution notes, actions taken, test results if applied in staging/limited rollout.
RCA (if applicable)	For critical incidents, a Root Cause Analysis is conducted and shared with the customer upon request.	RCA document detailing root cause, timeline, resolution steps, and future prevention actions.
Customer Confirmation	Support communicates resolution to customer, validates resolution in production, and ensures the customer confirms successful outcome.	Customer acknowledgment, issue confirmation, or request for further clarification captured in the system.
Ticket Closure	Upon customer agreement, ticket is formally closed and marked resolved in tracking system.	Final status, resolution summary, and closure timestamp recorded. SLA compliance metrics are logged.

Feature Requests and Feedback

Vicarius welcomes feature requests via support channels or account reps. Requests are logged, reviewed regularly by product management, and used to guide the roadmap. While not covered by SLAs, viable requests may be prioritized, and timelines shared when appropriate. Customers are updated on progress, and notified when features are released, closing the loop and reinforcing Vicarius's commitment to customer-driven innovation and continuous improvement.

Maintenance of the vRx SaaS Dashboard

Managed Cloud Service

The vRx console is a fully managed SaaS platform, with Vicarius handling all hosting, maintenance, and updates. It runs on resilient, secure cloud infrastructure with built-in redundancy and regular backups. The service targets 99.9% uptime and is monitored 24/7 for anomalies. Customers benefit from high availability, proactive issue response, and automatic improvements, without needing to manage any infrastructure themselves.

Planned Maintenance Notifications

Vicarius provides advance notice for scheduled vRx SaaS maintenance, typically during off-peak hours to reduce impact. Notices include timing, duration, and expected effects. Unexpected service issues are also communicated promptly via in-console announcement or direct alerts, with ongoing updates until resolved. This ensures transparency, minimizes disruption, and reinforces Vicarius's commitment to reliable, predictable service for all customers.

Regular Platform Updates (Upgrades and Backward Compatibility)

Vicarius regularly updates the vRx platform with new features, fixes, and security patches through zero-downtime, rolling deployments. All updates are tested for stability and backward compatibility, ensuring existing agents and proxies continue to function without requiring immediate upgrades. Release notes are published in the customer portal. This approach ensures customers always run a secure, up-to-date platform without service disruption or added maintenance burden.

SaaS Security and Compliance

Vicarius ensures vRx meets strict security and compliance standards, including SOC 2 Type II, GDPR, and CCPA. The platform is continuously patched at the infrastructure and application levels, with critical vulnerabilities remediated immediately. Regular audits, data encryption, logical tenant isolation, and daily backups protect customer assets. Security incidents, though rare, are communicated promptly. These practices ensure vRx remains secure, resilient, and enterprise-ready at all times. Vicarius's official security & compliance page

Agent and Proxy Software Release Management

vRx Agent Updates

The vRx agent enables scanning, patching, and patchless protection on each endpoint. Vicarius regularly updates the agent to add features, support new OS versions, and fix issues. Releases align with the platform's development cycle and include detailed release notes. Updates are managed via the vRx console or existing deployment tools, allowing organizations to roll out new versions gradually and with control, minimizing disruption while staying current and secure.

vRx Proxy Maintenance

The optional vRx proxy enables local caching for environments where agents lack direct internet access. Vicarius maintains the proxy software, aligns updates with agent releases, and provides easy upgrade paths (e.g., via Ubuntu package or Docker). If unavailable, agents can fall back to cloud connectivity. Vicarius support helps configure this failover, ensuring resilience. Customers are notified of new versions, with older proxy builds supported for a limited time to allow controlled upgrades.

Continuous Vulnerability Updates

vRx is continuously updated with the latest vulnerability intelligence and patches across thousands of apps and OSs. New CVEs, vendor fixes, and risk insights are evaluated and added within hours or days. Agents detect applicable updates automatically, requiring no manual input. This real-time content delivery ensures customers always have up-to-date remediation options, maintaining strong security posture without added effort.

Automated Patch Deployment and Scheduling

Vicarius notifies customers through the vRx console when new patches are available and enables the admin to perform automated deployment through customizable schedules. vRx supports staggered patch cycles, maintenance windows, and controlled reboots to minimize disruption. Patches can be queued and applied based on operational policies, with support available to fine-tune settings. This proactive, automated approach reduces time to patch and ensures timely, low-risk remediation across diverse environments.

Patchless Protection and Interim Mitigations

vRx offers Patchless Protection to defend against vulnerabilities when patches are unavailable or delayed. Using in-memory exploit prevention, the agent blocks techniques like code injection and memory scraping. This virtual shielding is vital for zero-days and unsupported systems. Vicarius continually expands Patchless Protection capabilities to enhance coverage across more threats. Customers are notified when protections are available.

Lifecycle Management, Backward Compatibility, and Security Assurance

Vicarius manages the full lifecycle of vRx agents and proxies with a focus on enterprise-grade stability, security, and transparency. Older versions remain supported across multiple releases, enabling customers to upgrade on their own timeline without disruption. The company follows a long-term support (LTS) model, typically backing major agent or proxy versions for 1–2 years, with critical fixes provided throughout the support period.

Backward compatibility is a design priority. New vRx components are built to work with existing infrastructure, so customers can run mixed-version environments during gradual upgrades. If breaking changes are needed, Vicarius introduces compatibility shims or parallel support to avoid forced "big bang" transitions. This allows enterprises to roll out upgrades in phases, aligned with internal change management policies.

Security is treated with urgency. If a critical vulnerability is found in the agent or proxy, Vicarius issues out-of-band hotfixes, provides mitigation steps, and supports temporary workarounds, ensuring risk is minimized while maintaining stability.

End-of-life (EOL) events are handled with transparency and support. Customers receive formal EOL notifications 6–12 months in advance, along with upgrade guidance, tools, and direct support for migration. Vicarius helps plan and execute transitions, treating them as managed efforts to ensure continuity.

This balanced approach, frequent innovation backed by long-term support, gives enterprises confidence that vRx will remain secure, compatible, and manageable as their environment evolves.

Support for Legacy Systems

Vicarius vRx helps secure legacy systems even after vendor end-of-life. The platform continues detecting vulnerabilities and applying virtual patches on outdated OSs like CentOS or Windows 2008. Rather than ending support immediately, Vicarius evaluates customer usage and maintains agent functionality as long as feasible. In rare cases, a "frozen" agent may be provided for limited protection. This pragmatic approach protects critical legacy infrastructure and reflects Vicarius's commitment to real-world enterprise needs.

Monitoring, Logging, and Proactive Support

System Health Monitoring

Vicarius proactively monitors the vRx cloud service for performance and availability, addressing issues like degraded regional performance often before customers notice. While on-prem components aren't monitored directly, the vRx dashboard shows agent connectivity and proxy health. Customers can configure alerts for offline agents or failed patch jobs, with Vicarius support available to assist. These built-in monitoring tools help ensure uptime, rapid response, and overall platform stability across both cloud and on-prem environments.

Log Collection and Analysis

Vicarius vRx agents, proxy, and console generate detailed logs of all activity, supporting fast issue resolution and compliance. Customers can access logs directly and share them with Vicarius support for troubleshooting. Logs help pinpoint root causes like installer errors, misconfigurations, or permission issues. Vicarius provides guidance on locating logs and increasing verbosity if needed. Logs also support audits by recording all actions. Support can assist with secure log sharing or real-time review in sensitive environments.

Proactive Support and Health Checks

Vicarius's support includes proactive success checks for enterprise accounts. Customer Success Managers conduct periodic reviews of deployment health, covering agent coverage, remediation times, and proxy status. They flag outdated agents, missed check-ins, or underused features and help resolve issues. Vicarius also alerts customers to maintenance needs and offers brief sessions to introduce major new features. These proactive touchpoints ensure the platform remains optimized and customers fully benefit from evolving capabilities.

Threat Advisories and Guidance

During major threats like zero-days or ransomware outbreaks, Vicarius issues timely threat advisories via email or the vRx dashboard. These include detection steps, mitigation guidance, and ready-made scripts. For example, during Log4Shell, Vicarius released a scanning script and patchless protection guidance. The team may also proactively contact affected customers and mobilize emergency assistance when needed. This proactive approach ensures vicarius support goes beyond break-fix, serving as a preventative, responsive partner in security operations.

Capacity Planning and Scaling

As customers scale vRx usage across more assets or sites, Vicarius ensures performance and capacity remain optimal. The SaaS backend scales transparently, while support may recommend adding proxies (if used), segmenting asset groups, or tuning scan schedules. Vicarius reviews system architecture, offers performance adjustments, and uses monitoring data to guide decisions. This proactive scalability support ensures vRx remains efficient and reliable as organizations grow, reinforcing it as a future-proof solution backed by expert guidance.

Continuous Excellence Customer Success

Dedicated Customer Success Management

Vicarius assigns a dedicated Customer Success Manager (CSM) to each enterprise account to maximize vRx value. The CSM conducts regular check-ins, aligns support with customer priorities, and coordinates extra help during audits or major projects. They also assist with training, integrations, and migrations. This high-touch engagement ensures a strong partnership, helping customers succeed with both day-to-day operations and long-term security goals.

Training, Enablement, and Community Support

Vicarius provides live onboarding, on-demand tutorials, and feature-specific webinars to keep customers informed and skilled on vRx. Certification workshops are also available for partners and advanced users. New features are launched with clear documentation and support team readiness. A monitored community forum enables peer learning and direct support engagement. This ongoing education and collaboration help customers mature their vulnerability management practices beyond technical troubleshooting.

Customer-Driven Innovation and Feedback Loop

Vicarius actively incorporates customer feedback into product and support improvements. Feedback is collected via support ratings, QBRs, and feature requests. Many vRx enhancements like expanded integrations, stem directly from user input. The product team prioritizes these insights, and customers are often updated when their suggestions are implemented. This ongoing dialogue extends to support processes, ensuring the platform evolves in ways that reflect real-world needs and fosters a true customer-vendor partnership.

Operational Excellence and SLA-Driven Support

Vicarius delivers enterprise-grade support by closely monitoring SLA metrics like response times, resolution rates, and customer satisfaction. Trends drive updates to the knowledge base and tooling, while the SLA itself is reviewed annually to reflect evolving needs. Support quality is benchmarked against top industry players, with many customers praising Vicarius's responsiveness. Enhanced support tiers are available, but even the standard package reflects the company's commitment to proactive, professional, and high-performing support.