vicarius

SOLUTION BRIEF vRx 2.0 PLATFORM

Asset and inventory management

Full visibility across every managed and unmanaged asset, so your team can find it, group it, and fix it from one platform

The challenge

The problem: you cannot protect what you cannot see

Most security teams are working from an incomplete map. Managed endpoints give one layer of visibility. But routers, IP cameras, OT controllers, and cloud hosts without agents sit entirely outside that coverage. Meanwhile, tags go stale, inventories drift, and manual triage cannot keep pace.

- Blind spots: unmanaged devices grow attack surface in the dark.
- Asset sprawl: no single source of truth makes scoping remediation guesswork.
- Remediation gaps: a known vulnerability cannot be acted on without a proper inventory entry.
- Compliance exposure: inventory gaps become audit failures.

How vRx builds your asset inventory

vRx combines agent-based and agentless discovery into one continuously updated inventory. Every asset, managed or not, feeds the same scoring engine and the same remediation workflow.

Managed assets

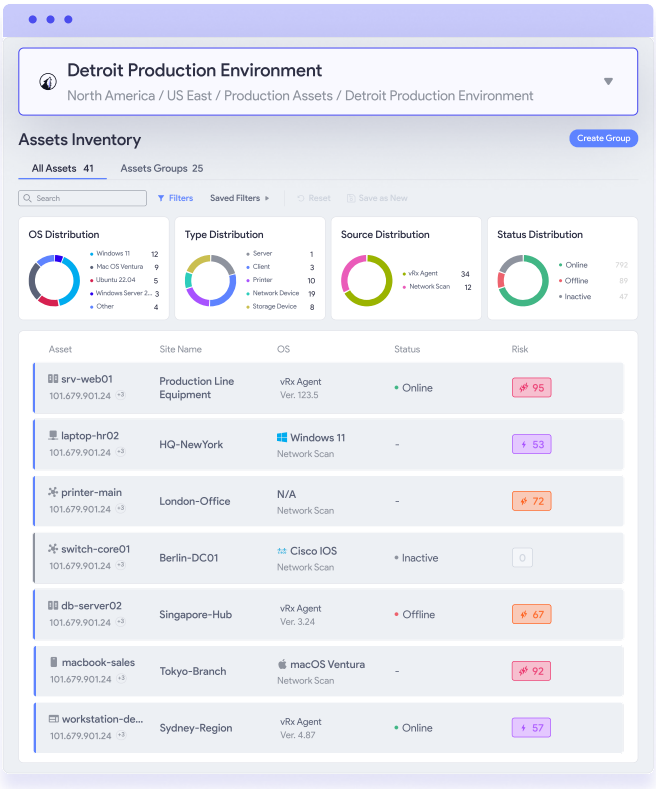
The vRx agent on Windows, Linux, and macOS delivers real-time software inventory, OS patch state, CVE correlation, SBOM generation, and direct remediation via vPatch, vScript, and vShield.

Unmanaged assets via vRadar

vRadar discovers and fingerprints every device an agent cannot reach: routers, cameras, printers, OT sensors. Every finding lands in the same unified inventory. Assets that cannot run an agent stay fully in scope for scanning and remediation.

Grouping: AI, vQL, and static

Dynamic groups in natural language or vQL are built and maintained by the system automatically. Policies attached to dynamic groups update their targets in real time. Static groups give your team direct control over membership.



Capability, grouping and benefit reference

Capability	How vRx delivers it	Benefit
Detection, coverage and policies		
Managed asset detection	Lightweight vRx agent on Windows, Linux, and macOS collects full software inventory, OS telemetry, CVE findings, and SBOM per endpoint in real time.	SecOps: complete endpoint coverage, no scanner blind spots. IT: always-current patching status per device, patched and pending in one view.
Unmanaged asset detection	vRadar agentless scanning discovers every network-attached device where an agent cannot be deployed: OT, IoT, printers, routers. If an agent can be installed, deploy it from the asset view. If not, the asset stays in scope for vulnerability scanning, compliance scanning, and remediation via vRadar.	SecOps: shadow IT and rogue devices surface automatically. IT: no device falls out of inventory or coverage simply because it cannot run an agent.

Capability	How vRx delivers it	Benefit
Detection, coverage and policies		
Software inventory and SBOM	Agent-side collection of every installed application, version, and vendor. SBOM generated per endpoint on every supported OS.	SecOps: full software attack surface visible. IT: per-device software record ready for audit, licensing review, and risk assessment.
Event-driven policies	Configure policies that trigger on conditions you define: a new asset discovered, a device joining a group, a scan returning a specific finding. The policy acts immediately, no scheduled scan required.	SecOps: security posture responds to estate changes in real time. IT: new devices are automatically scanned and onboarded the moment they appear.
Asset-to-remediation loop	Every discovered asset feeds vScore prioritization and triggers remediation: patching via vPatch, scripted fixes via vScript, or patchless protection via vShield for assets that cannot be patched.	SecOps and IT: inventory is not a dead-end report. Every asset has a clear action path from day one, including assets where patching is not possible.
Asset and software grouping		
AI dynamic grouping	Describe a group in plain natural language. The AI builds it and keeps it current: matching assets are added automatically, assets that no longer fit are removed. Any attached policy updates its targets in real time.	Policies always act on the right assets. No stale targets, no missed coverage as the estate changes.
vQL dynamic grouping	Write a structured vQL query to define group membership. Evaluated continuously with the same automatic policy-target updates as AI grouping.	Exact attribute-level control with no manual upkeep. Groups and policy targets stay current automatically.
Static grouping	Manually select specific assets and add them to a group. Membership only changes when a user explicitly adds or removes an asset.	Right for fixed scopes: critical server sets, compliance boundaries, or any group where membership must be human-controlled.

Get started

vRx deploys in hours. The agent installs silently through your existing software distribution tooling. vRadar requires only a network-accessible scan node. It supports both unauthenticated and authenticated scans depending on the depth of visibility required.

Other vendors show you what is vulnerable. vRx shows you what is vulnerable and then closes it, across every managed and unmanaged asset in your environment.
Talk to your Vicarius account team or visit vicarius.io to schedule a walkthrough.