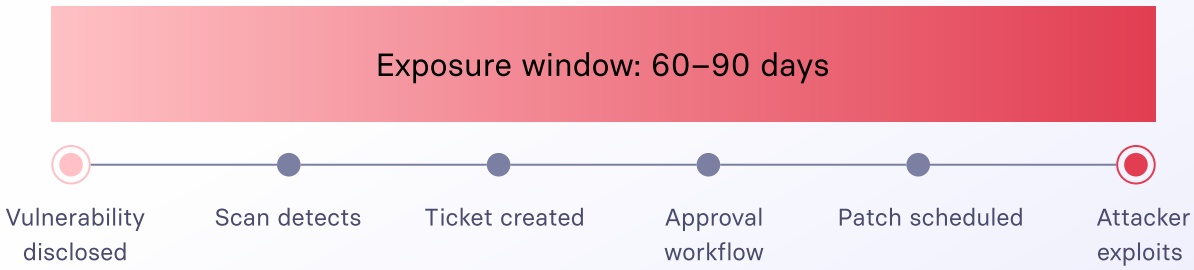
vicarius

SOLUTION BRIEF

vRx v2 PLATFORM

True remediation

Closing the loop between detection and resolution , once and for all



Legacy models separate detection from remediation: leaving organizations exposed for months.

The challenge: scanning is not fixing

For two decades, enterprise security programs have been built around a fundamental flaw: the tools designed to find vulnerabilities were never built to fix them. Scanners generate findings. Dashboards display risk scores. Tickets get created. And somewhere in the handoff between security and IT operations, vulnerabilities sit unresolved : for 60, 90, sometimes 120 days.
The numbers tell the story. The National Vulnerability Database now tracks over 40,000 new CVEs annually. Meanwhile, exploit timelines have compressed from months to days. The gap between disclosure and active weaponization has never been narrower : yet the average enterprise remediation cycle has barely moved.

> *What stood out was that the platform wasn't just a scanner or a patch manager : it was an entire remediation platform that discovers vulnerabilities, prioritizes based on real risk, and remediates automatically.*

Legacy vendors responded to this crisis by adding dashboards and integrations : more ways to see the problem, never a way to solve it. The word "remediation" became a marketing term stripped of its operational meaning. True remediation means one thing: the vulnerability no longer exists.

The solution, vRx - A remediation-first platform

Vicarius built vRx from a premise that sounds simple but represents a fundamental departure from the market: a vulnerability scanner that cannot fix vulnerabilities is not a complete solution. vRx unifies detection, prioritization, and remediation within a single operational platform : eliminating the tool sprawl and workflow friction that allows risk to accumulate.

1 **Discover**
Asset & vulnerability discovery

2 **Prioritize**
Risk-based scoring & analytics

3 **Remediate**
Automated patch deployment

4 **Validate**
Continuous validation after remediation completion

Remediate with precision

- Automated patch deployment across OS and third-party applications : no separate tooling required
- Scripting engine for custom remediation actions and complex environment configurations
- Scheduled, policy-driven patch cycles that compress weeks of work into hours

Protect when patching isn't possible

- Patchless Protection shields vulnerable assets in real time when a vendor patch is unavailable
- Virtual patching via memory-level controls neutralizes exploitability without touching the application
- Continuous exposure validation confirms whether risk has actually been eliminated

Discover and analyze risk

- Continuous asset discovery across endpoints, servers, cloud workloads, and containerized environments
- vAnalyzer correlates CVE data with real-world exploitability context : not just CVSS scores
- xTags enable intelligent asset segmentation for targeted, policy-based remediation

Measure and report

- Built-in compliance engine maps remediation posture to major frameworks (SOC 2, ISO 27001, NIST)
- Role-based dashboards give CISOs executive-level visibility and practitioners actionable queues
- Full audit trails demonstrate closed-loop remediation to auditors and cyber insurers

Proven outcomes, what organizations achieve

60–70%
Reduction in mean time to remediate

40,000+
CVEs tracked annually – covered

1 day
Patch cycles reduced from weeks to hours

100%
Closed-loop remediation verified

These are not theoretical benchmarks. Organizations adopting vRx report mean time to remediate reductions of 60 to 70 percent. Security teams that previously dedicated full workweeks to manual patch coordination now complete patch cycles in a single day. A major airline reduced patch scheduling from a full-time operational burden to a one-day event. The measurable impact extends from operational efficiency through to insurance and compliance outcomes.

Why does it matter now? the market inflection point

Three forces have converged to make the remediation gap untenable. First, vulnerability volume has scaled beyond any team's capacity to manage through manual processes alone. Second, attackers have accelerated : time-to-exploit now routinely falls within the window that legacy patching workflows require just to open a ticket. Third, regulators and cyber insurers are no longer asking whether organizations scan for vulnerabilities. They are asking how quickly organizations fix them, and demanding documented proof.

The CISO who can demonstrate measurable remediation velocity : not just detection breadth : is the one positioned to navigate this environment. That requires a platform built around completion, not observation.

Business value at a glance

Outcome	What vRx enables
Reduced attack surface	Automated remediation closes vulnerabilities before attackers can exploit them, shrinking dwell time and blast radius.
Faster compliance posture	Built-in compliance mapping and audit trails satisfy regulatory and cyber-insurance requirements with documented evidence.
Operational efficiency	Unified workflows eliminate tool sprawl and inter-team handoffs, freeing security and IT teams for higher-value work.
Risk-informed prioritization	Context-aware scoring ensures the highest-risk exposures are addressed first : not the easiest or the loudest.
Resilience without downtime	Patchless Protection shields assets during patch testing and maintenance windows, eliminating the exposure gap.

> *The question is no longer whether your vulnerability scanner can find your exposures. The question is whether your remediation platform can eliminate them before attackers exploit them. vRx answers that question*

See true remediation in action

Request a live demonstration of vRx at vicarius.io and discover how leading security teams have transformed vulnerability exposure into a closed-loop, measurable, and auditable program.