

vRx 2.0

The remediation-first platform for exposure management



How vRx builds your asset inventory

Scanners tell you what's broken. vRx 2.0 fixes it. It's the only platform that unifies discovery, prioritization, and remediation in one workflow, then verifies every fix closed the exposure. No handoffs, no spreadsheets, no waiting on a ticket queue to move.

The foundation



Unified discovery

vRx combines agent-based and agentless scanning (vRadar) across endpoints, servers, cloud workloads, network devices, and containers. SBOM-based detection catches vulnerabilities in dependencies and libraries that signature-based scanners miss entirely.



Risk-based prioritization

vScore fuses CVSS, EPSS, and KEV data with your own environment context, asset criticality, exploitability, business impact, so your team fixes what attackers will actually use, not just what scores highest on paper.



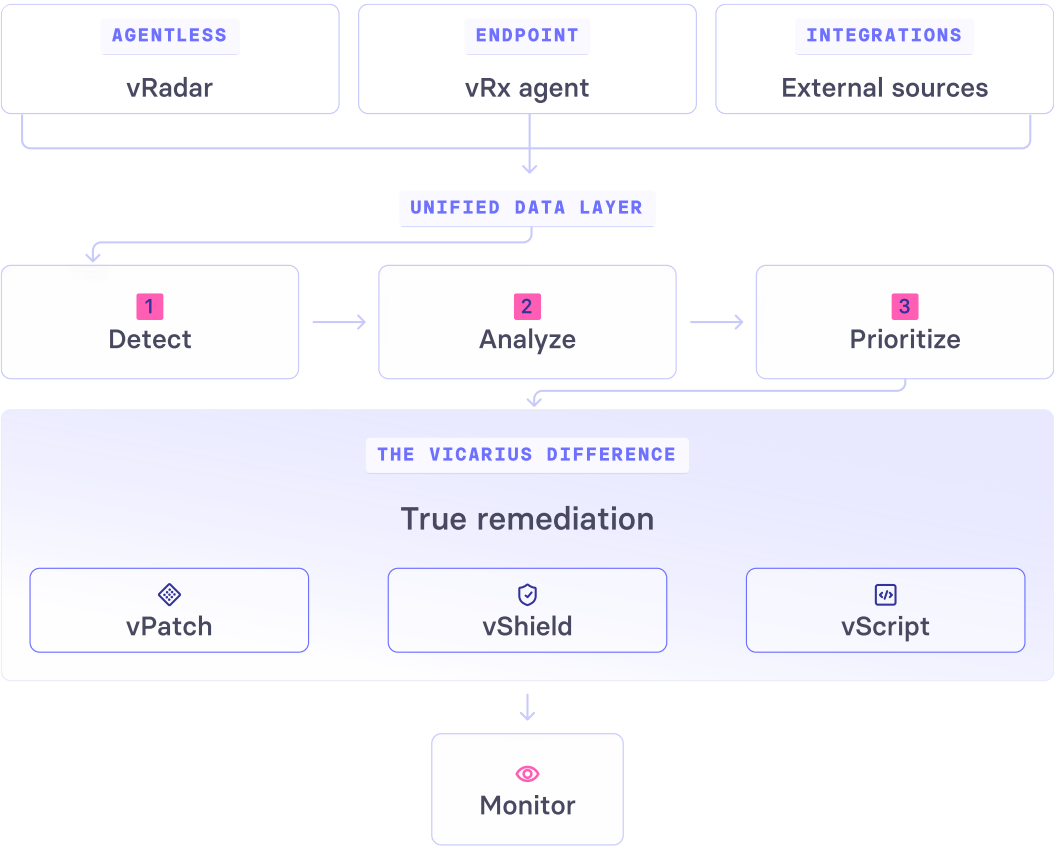
Automated remediation

Three built-in paths close the loop: vPatch deploys patches across Windows, macOS, and Linux covering 20,000+ third-party apps, vScript handles custom fixes and misconfigurations, and vShield shields unpatchable vulnerabilities at the memory level.



Compliance mapping

Every remediation action maps automatically to HIPAA, PCI DSS, Cyber Essentials, and 100+ CIS Benchmarks. Audit-ready reporting without the manual spreadsheet work.



The only platform that fixes what others only detect.

What's new in 2.0

Higher-end capabilities built for teams managing scale and complexity

Advanced patching policies

Move beyond one-size-fits-all deployment. Configure rule-based patching that triggers on vScore thresholds, schedule maintenance windows by asset group, or push patches on demand, all without forcing unplanned reboots. vRx brings every patch type, application patches, Windows KBs, macOS updates, Linux packages, into one console with consistent search and filtering.

Policy Name

Emergency Patch Deployment

1 Trigger

Time-Based

2 Action

Patch Selection

6

3 Target

Asset Selection

3

4 Settings

Deployment Settings

Which assets should receive these patches?

Define the target systems that will receive the selected patches

Scope Selection

Asset Groups

Select from existing asset groups

Asset Inventory

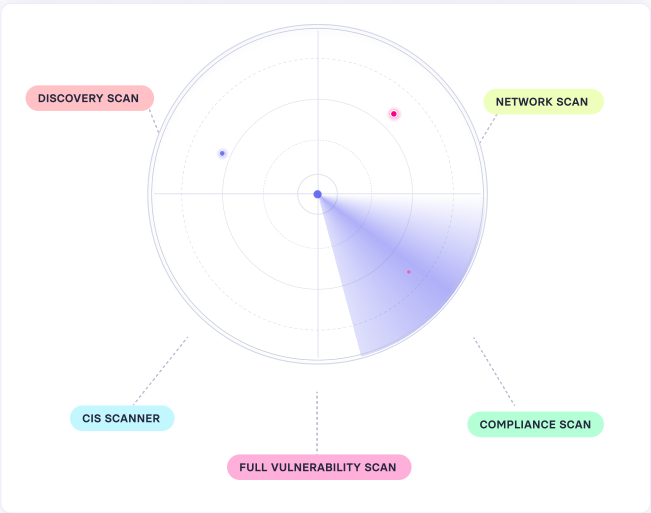
Select from asset inventory

Asset Group Selection

Add Group

Group Name	Assets	Created By	Created at
☒ US-East Datacenter	134	Hange Zoe	26.04.25 10:54
☒ Production	115	Armin Arlert	26.04.25 10:54
☒ Windows Servers	76	Annie Leonhart	26.04.25 10:54
☐ Engineering Team	219	Reiner Braun	26.04.25 10:54
☐ US-West Datacenter	156	Armin Arlert	26.04.25 10:54

Show More

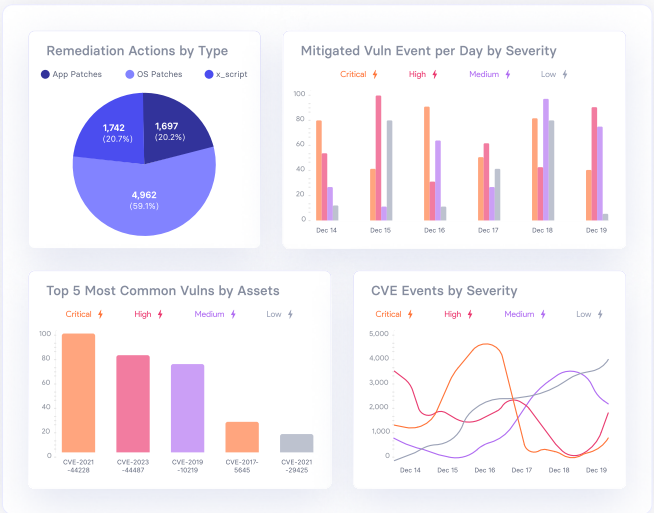


vRadar: agentless scanning at scale

vRadar continuously scans on-premises and cloud environments without deploying an agent, building an always-current asset and vulnerability inventory. Paired with agent-based coverage, it closes the visibility gaps that remote endpoints, IoT devices, and unmanaged assets typically create.

Enriched vulnerability intelligence

vRx goes past CVSS scores alone. It layers in EPSS exploitation probability, CISA KEV data, and real-world weaponization signals, then adds your own asset and business context, so every finding reflects actual risk instead of theoretical severity.



Script Type

x_remediation

CVE-2024-9810

```
1 if (-NOT ([Security.Principal.WindowsPrincipal]
2 [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal
3 WindowsBuiltinRole]::Administrator))
4 {
5
6 Write-Output "[*] Run as admin"
7 Exit
8 }
9
10
11
12 Write-Output "[*] Disabling randomization of IPv6"
13 netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent
14 Write-Output "[*] Disabled Successfully"
15
16
17 Write-Output "[*] Creating inbound rule in firewall to block router
18 advertisement"
19 New-NetFirewallRule -DisplayName "Block ICMPv6 Router Advertisement" -
20 Direction Inbound -Protocol ICMPv6 -IcmpType 134 -Action Block
21 Write-Output "[*] Cre
22
23 Write-Output "[*] Cre
24 solicitation"
25 New-NetFirewallRule
26 Direction Outbound
27 Write-Output "[*] Cre
28
29
30
```

Remediation Center

01 No Patch Available

Install Patch

02 Run vScript

CVE-2024-9810: Mitigate CraftCMS RCEs

Run vScript

03 Add Rule

Acknowledge the CVE

Add Rule

04 Run vShield

Enable patchless protection on Windows ver:1903

Run vShield

vScript and vShield

The vScript engine automates custom fixes and misconfiguration changes across Mac, Windows, and Linux, using publicly available scripts or your own. For anything that can't be patched, vShield's Patchless Protection secures vulnerable applications at the memory level, closing the exposure window between disclosure and patch availability, without a reboot.

AI-powered reporting and asset grouping

Ask vRx a question in plain English, no filters or query builder and get the answer from live platform data. Generate reports on vulnerabilities, remediation progress, assets and compliance on demand or on a schedule, with CSV, PDF and XLSX exports scoped by site, group, framework or time range. You can also describe the dynamic asset or software group you need and vRx builds it, then keeps membership current as your environment changes.

Create Group

Group Scope

Dynamic

Static

AI

vQL

windows 11

+

hasOSFamily(asset, 'windows')

↶ ↷ ? 🔍

Group Preview

Asset Name	Operating System	vRx Version	Status	Risk Level
osboxes	Windows 11	7802.90	Offline	High Risk
LAPTOP-M2LO...	Windows 11	5.2.1	Online	High Risk
hammerstein.loc...	Windows 11	7.2.211	Online	High Risk
WIN-7470	Windows 11	5.2.1	Offline	Medium Risk
EC2AMAZ-I7DM...	Windows 11	6.2.4	Online	Low Risk

