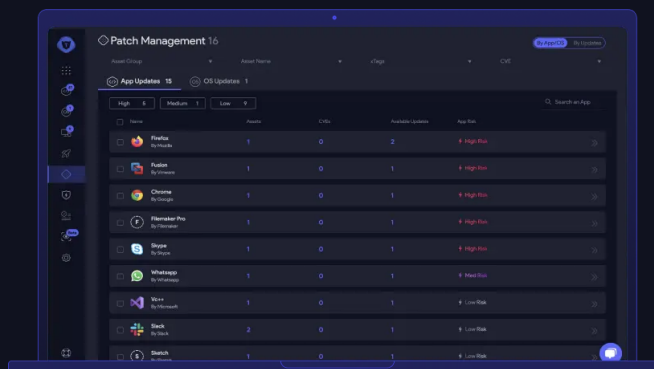


# Auto Actions

## Streamline your organization's vulnerability management workflow and decrease operation costs

vRx's Auto Actions capabilities enable your IT and cybersecurity teams to automate repetitive, tedious, and time-consuming tasks like patch implementation so they can refocus their expertise where it's needed most. Harden your cybersecurity posture by decreasing the chance of human error and setting up automated responses to specified triggers.



## Secured

Reduce human error and intervention with powerful, dynamic, and scalable patching capabilities. Empower IT teams to protect and defend from known and unknown vulnerabilities with advanced asset targeting.

## Maintained

Schedule patch deployments, set up triggers to manage workload, and update all of your organization's operating systems ahead of time. Regain lost time spent manually rebooting assets with flexible scheduling features.

## Streamlined

Send reports to key stakeholders, lock specific assets against unwanted actions, and run customized scripts all in one dashboard. Recuperate lost hours spent chasing false positives

# Auto Action Use Cases

## Never Miss a Critical

With complex IT infrastructures and the never-ending river of new vulnerabilities, it's possible that critical issues might slip under any IT team's radar. vRx's Auto Actions give you the power to plug those gaps.

## Common Task Automation

Security teams are inundated with managing and monitoring vulnerabilities. vRx removes the time-consuming labor so your team can utilize their skills and resources efficiently.

## Stay up to Date

Automate vulnerability management and mitigation along with other routine tasks to ensure software is up to date across your entire digital landscape. This allows your IT teams to stay ahead of the curve and anticipate the next cybersecurity threat.

## Optimize Mitigation

vRx's Auto Actions empower your organization to start the mitigation process before human intervention begins. Get a head start on cybersecurity issues by automating the remediation cycle.

## Act Anytime

vRx's Auto Actions allow you to react at any moment, 24/7. Malicious agents capitalize on lowered response times during weekends and holidays. Automate incident responses and ensure your team stays notified with triggers and notifications.

## Actions on scale

Trigger responses can be scaled up or down according to requirements. Ensure that the highest-risk assets are automatically protected with Patchless Protection if a critical vulnerability is detected, or automatically schedule low risk vulnerabilities to be patched during the following weekend.

## Generate auto-reports & notifications

Set up daily, weekly, and monthly reports that only contain the information you need. Streamline information sharing between departments and keep everyone on your team in the loop with auto-reports and notifications.

## Incident Response

With vRx's Auto Actions, you can specify triggers that cause an immediate and tailored response to a variety of incidents. If a critical vulnerability on a high-risk asset is detected, vRx can instantly quarantine the affected asset.

## Auto Actions Steps

Threats don't take time off. Auto Actions empower you to respond and mitigate threats automatically.

Deploy cybersecurity policies and incident response measures in three simple steps.

# 01

### Define Triggers

Specify time and frequency or select advanced triggers like new patch or CVE.

# 02

### Identify Targets

Select the servers and workstations to apply the specified triggers.

# 03

### Take Action

Activate defense mechanisms such as patch deployment, patchless protection, or script execution.

# Auto Actions List

React faster and work smarter with cost-effective actions. Improve your security ROI and relieve headaches with a secured and streamlined bundle of features.

**Patch**

Action

Dynamic and scalable patch management keeps third-party software and operating systems secured and up-to-date.

**OS Update**

Action

Ensure asset versions are secured, unified, and up-to-date across Windows, Linux and Mac.

**Run script**

Action

Create a customized or built-in script as an independent action or insert in a sequence.

**Patchless Protection**

Action

Protect or monitor assets with no available patch with triggers, rules, and batch actions.

**Report**

Action

Export frequent auto reports for stakeholders and the IT/Security management team.

**Reboot / Shutdown**

Action

Set and schedule a reboot or shutdown to selected assets and groups.