

SOLUTION BRIEF

Automated Vulnerability Remediation: Find and Fix Vulnerabilities [Now]

RESOLVING VULNERABILITIES DOESN'T HAVE TO BE A FIRE DRILL OR FINGER-POINTING EXERCISE ANYMORE.

Dramatically reduce the time between detection and remediation to harmonize your cross-team remediation efforts with Automated Vulnerability Remediation (AVR) from Automox + Rapid7 InsightVM.

KEY BENEFITS



Lightning fast detection and remediation

Dramatically reduce MTTR and overall risk with a predictable, continuous process.



Full-spectrum vulnerability coverage

Deploy patches, configuration changes, and other remediation actions from a single console.



Smooth, efficient coordination between teams

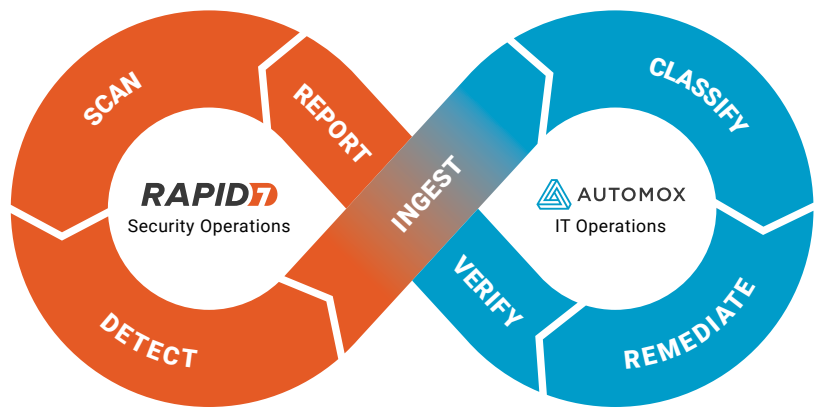
Enable ITOps and SecOps to work as one risk-reducing team with fewer crossed wires.



"Better together" remediation with your existing solution

Maximize your existing investments for faster remediation and reduced overall risk.

Now you can minimize exposure windows and discover unmanaged endpoints with AVR. This powerful integration delivers full-cycle detection and remediation of vulnerabilities, enabling security and IT teams to easily coordinate endpoint protection on a regular, predictable cadence.



FULL-CYCLE DETECTION AND REMEDIATION IN ACTION

AVR gives IT and security teams the exact same vulnerability information, allowing coordination from the moment a vulnerability is discovered until it's remediated – all without confusion or mixed messages. Your IT team can also quickly see endpoints that are known to Rapid7, but not under Automox management. You can then deploy agents to those devices, ensuring 100% automated patch and remediation coverage. With no installation or downloading required for this cloud-to-cloud integration, IT teams just need to configure, ingest vulnerability information, and start remediating.

SOLUTION BRIEF

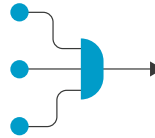
JUST 4 EASY STEPS

Take advantage of AVR with just four simple steps in the Automox console.



1. DETECT

Rapid7 scans and identifies existing vulnerabilities.



2. INGEST

Vulnerability data is automatically pulled into the Automox console at regular intervals using filters based on Rapid7 vulnerability categories and device tags.



3. ASSESS

Vulnerabilities are classified and automatically sorted into **three remediation types**.

Patchable Vulnerabilities: Identified vulnerabilities that are immediately patchable by Automox.

Rapid7 Solutions: Vulnerability that require configuration or non-patch actions. Rapid7 provides remediation instruction with the vulnerability information that can be used in Automox Worklets.

Unknown Devices: Devices known by Rapid7 that need the Automox agent installed for remediation.



4. REMEDIATE

Patching or Automox Worklets are deployed and verified across any and all specified devices in minutes.

GET THE FASTEST PATH TO FULL-CYCLE VULNERABILITY MANAGEMENT

Delaying critical vulnerability remediation means leaving your organization defenseless against cyberattacks. With AVR, you get full-cycle remediation in minutes to quickly close your exposure window.

All your endpoints. Always configured. Always secured.

Cloud-native IT operations for modern organizations.

Get a free 15-day trial to see why Automox is the leading cloud-native IT operations solution for modern organizations.

Demo Automox today to see AVR in action

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.