

Automated Patch Management

Continuous patching of OS and third-party applications

Automox Worklets™

Create custom tasks using scripts across any managed Windows, macOS, or Linux device

Cloud-Native Platform

Harden endpoints without complex infrastructure or VPN requirements

Configuration Management

Serverless configuration management for all managed devices with zero drift

Continuous Policy Enforcement

Automatically enforce patching, configuration, deployment, and Automox Worklet tasks

Cross-OS Support

Support for Windows, macOS, and Linux devices

Endpoint Visibility

In-depth visibility to identify non-compliant devices

Lightweight Agent

Efficient and lightweight agent under 20MB

Role-Based Access Control

Set individual permissions for users and groups with RBAC

Rich API

Fully featured and documented API for complete integration into your infrastructure

Software Deployment

Painlessly deploy, manage, and enforce OS and third-party applications globally

Straightforward Reporting

Real-time, up-to-date reports

Automox® is a cloud-native endpoint hardening platform that supports Windows, macOS, and Linux from a single console. It enables continuous connectivity for local, cloud-hosted, and remote endpoints with no need for on-premises infrastructure or tunneling back to the corporate network.



Cloud service and a lightweight agent save the day

The Automox lightweight agent continuously monitors each device and inventories its hardware, software, patches, and configurations — while staying in constant communication with the Automox cloud service.



Automation that you control

With built-in cross-platform patching for OS and third-party applications along with security configurations and software deployments, Automox ensures the right software is deployed and compliance is maintained. It works on user-defined schedules and provides notifications and reporting according to organizational requirements.



Automate and enforce custom tasks

Automox can accomplish any process that can be scripted with Automox Worklets $^{\text{\tiny{M}}}$. If it can be scripted, Automox can automate and enforce it across all endpoints.





10MB*

<1%*

Agent Requirements

2008 R2+

WINDOWS: macOS: LINUX

Memory utilization 10MB* Memory utilization 10MB* Memory utilization Disk space requirements 20MB Disk space requirements 16MB Disk space requirements 5-10MB** **CPU** requirements <1%* **CPU** requirements **CPU** requirements macOS 10.13, Version support Version support Windows 7+, Version support

Windows Server 10.14, 10.15

CentOS 6+, Fedora 28+, Debian 9+, Ubuntu 16.04, 18.04, Amazon Linux 2

RHEL 6 - 7, SUSE 12+,

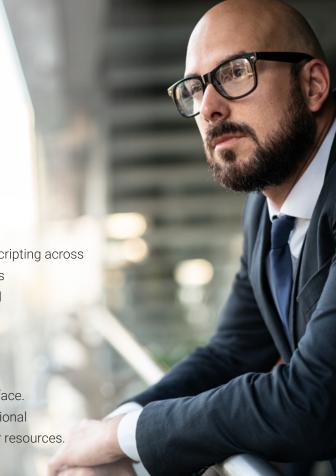
ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide NexGen, Highly Automated and User-Friendly solutions in partnership with IRONSCALES with the POWER OF NOW for Comprehensive NexGen Email Security, THREATX for NexGenWAAP (WAFF++) with an Attack-Centric approach and Cyber Security Training with Project Ares by CIRCADENCE CORPORATION for Online Simulation based Cyber Security Training.

Cloud-native and globally available, SRC Cyber Solutions LLP enforces OS and third-party patch management, security configurations, and custom scripting across Windows, macOS, and Linux from a single intuitive console. IT and SecOps can quickly gain control and share visibility of on-prem, remote, and virtual endpoints without the need to deploy costly infrastructure.

Experience modern, cloud-native patch management today with a 15-day free trial of SRC Cyber Solutions LLP and start recapturing more than half the time you're currently spending on managing your attack surface. SRC Cyber Solutions LLP dramatically reduces corporate risk while operational efficiency to deliver best-in-class security outcomes, faster and with fewer resources.





^{*}varies based on agent activity **varies depending on distro