AUTOMOX

AUTOMOX ENDPOINT HARDENING: DATA SHEET

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™. If it can be scripted, Automox can automate and enforce it across all endpoints.

AUTOMOX

Agent Requirements

WINDOWS:

Memory utilization	10MB*
Disk space requirements	20MB
CPU requirements	<1%*
Version support	Windows 7+, Windows Server 2008 R2+

macOS:

Memory utilization	10MB*
Disk space requirements	16MB
CPU requirements	<1%*
Version support	macOS 10.13, 10.14, 10.15

LINUX

Memory utilization	10MB*
Disk space requirements	5-10MB**
CPU requirements	<1%*
Version support	RHEL 6 - 7, SUSE 12+, CentOS 6+, Fedora 28+, Debian 9+, Ubuntu 16.04, 18.04, Amazon Linux 2

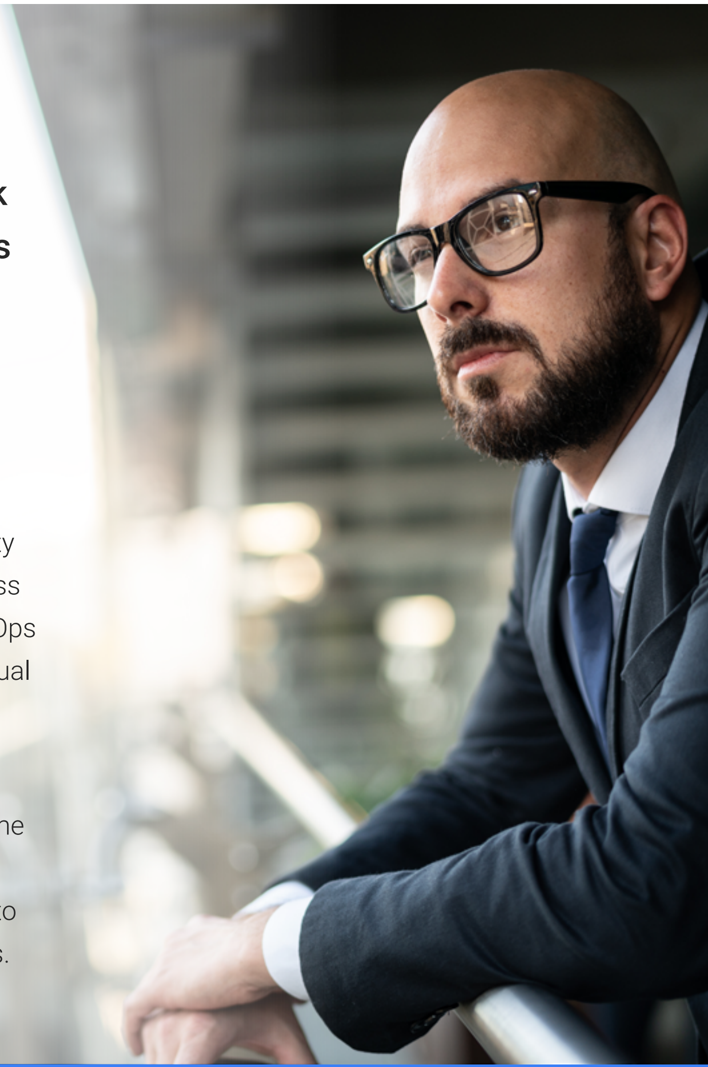
*varies based on agent activity
**varies depending on distro

About Automox

Facing growing threats and a rapidly expanding attack surface, understaffed and alert-fatigued organizations need more efficient ways to eliminate their exposure to vulnerabilities. Automox is a modern cyber hygiene platform that closes aperture of attack by more than 80% with just half the effort of traditional solutions.

Cloud-native and globally available, Automox 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 Automox and start recapturing more than half the time you're currently spending on managing your attack surface. Automox dramatically reduces corporate risk while raising operational efficiency to deliver best-in-class security outcomes, faster and with fewer resources.



Be a smaller target.™

Chat with Automox to set up a demo.
automox.com | info@automox.com | (720) 440-2495