AUTOMOX

The Automox Platform

Technical Brief

Automox is the IT operations platform for modern organizations. It makes it easy to keep cross-platform endpoints patched, configured, controlled and secured – without servers to manage or VPNs. Using thoughtful automation, IT admins can fix critical vulnerabilities faster, slash cost and complexity, and win back hours in their day.

SINGLE, SECURE-BY-DESIGN ENDPOINT AGENT

Automox® agent is lightweight and deployable across Microsoft Windows®, macOS®, or Linux endpoints. The Automox agent is responsible for software and patch deployment, monitoring, and process operations on the endpoint. The Automox agent uses privileged access to the endpoint and has multiple security features built to safeguard the endpoint from eavesdropping and unwanted access attempts. Communications are encrypted with transport layer security and authenticated with public-key cryptography.

Automated, manual, and third-party testing is conducted on the agent to reduce the risk of potential replay or man-in-the-middle (MITM) attacks.

VPN-FREE MANAGEMENT

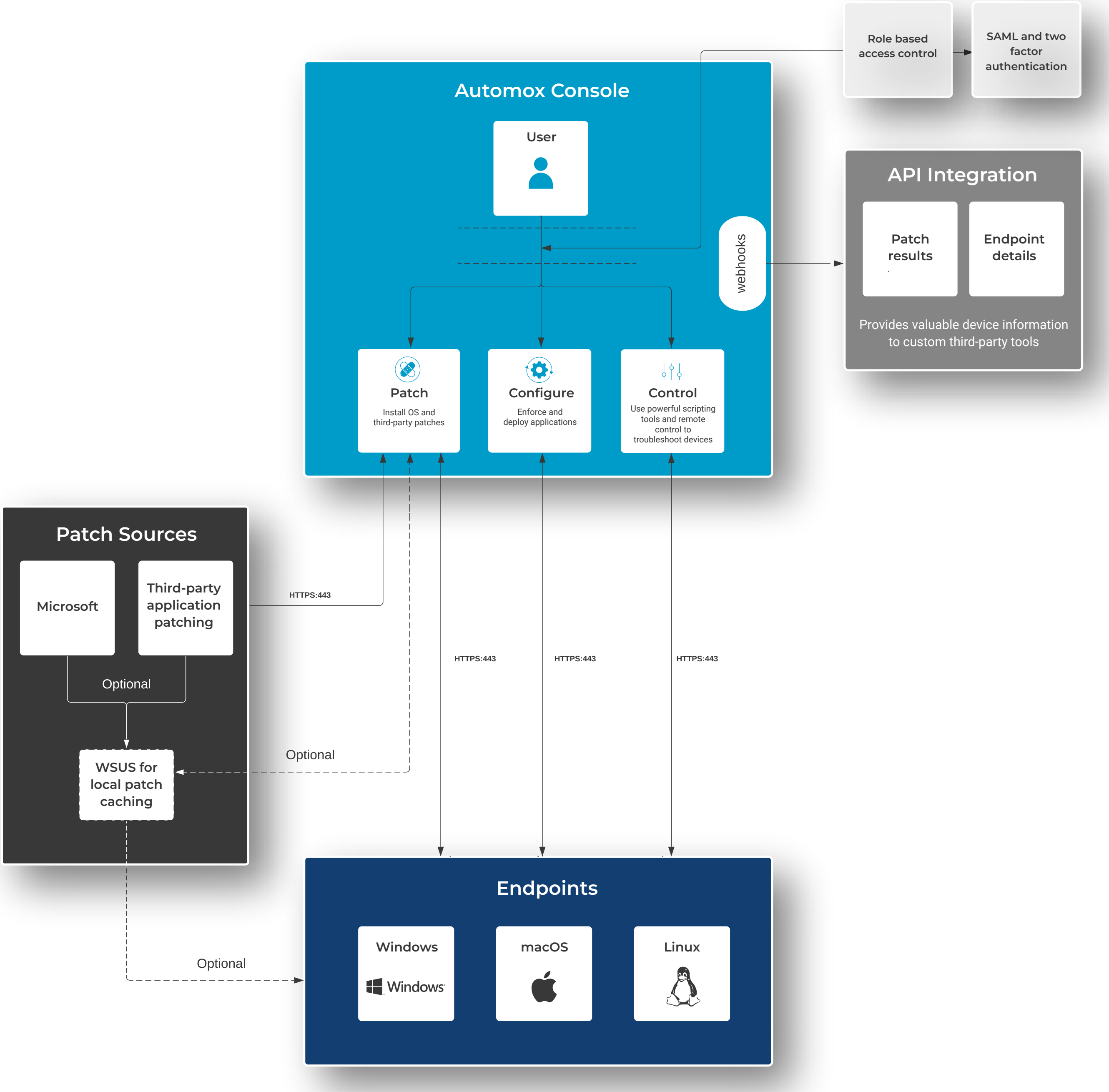
Automox is a simple, light, versatile endpoint management that can patch, configure, and control any endpoint anytime, anywhere. With Automox, you eradicate the need for legacy tools such as patch servers (or any hardware), clunky VPN connections, or multiple solutions for different OS platforms. Instead, patch, deploy, configure, and remediate vulnerabilities from one VPN-free platform. With Automox's zero-maintenance solution, managing your devices is simple. As a result, you significantly lower your endpoint management costs while delivering high strategic value to your organization without the hassle.

SCALABLE FOUNDATION

The Automox platform architecture uses a clustered design to ensure high availability, reliability, and flexibility to scale up or down quickly on demand. Automox leverages the AWS concepts of Regions and Availability Zones to provide services and data that are safe, secure, and continuously available. In addition, Automox follows frequently tested backup and restore procedures to ensure the highest reliability and security. However, even with spikes caused by outside factors, Automox ensured lower risk levels were brought into remediation within a short time frame.

AUTOMOX FUNCTIONAL DIAGRAM

The diagram below illustrates basic operational workflows and identifies primary platform components.


Role based access control
SAML and two factor authentication
Automox Console
User
webhooks
Patch
Install OS and third-party patches
Configure
Enforce and deploy applications
Control
Use powerful scripting tools and remote control to troubleshoot devices
API Integration
Patch results
Endpoint details
Provides valuable device information to custom third-party tools
Patch Sources
Microsoft
Third-party application patching
Optional
WSUS for local patch caching
HTTPS:443
Optional
HTTPS:443
HTTPS:443
HTTPS:443
Optional
Endpoints
Windows
Windows
macOS
Linux

SECURITY-FOCUSED DEVELOPMENT

Automox follows a modern software development process that focuses on quality and security, employing the latest technologies for the highest level of reliability. Before deployment to production, all product releases undergo rigorously automated and manual testing in a staging environment to catch and eliminate operational and security issues.

ENFORCED ACCESS POLICIES AND LOGGING

Automox implements Identity and Access Management policies and partitioned access to systems for staff in adopting best practices and alignment to the principle of least privilege. Need-based access is granted on a per-employee basis and regularly reviewed. Monitoring software is used to track all server logins and privileged command execution, alerting on any anomalous activity. All activity logs are written to centrally located and hardened servers and monitored using OSSEC and other tools 24x7.

Multi-OS support
Automox offers Windows, macOS, and Linux support, providing the same seamless experience for all operating system (OS) types.

Complete endpoint visibility
Automox provides a complete inventory of your endpoints, with comprehensive, in-depth visibility to identify noncompliant and compliant devices. The agent will discover the full breadth of hardware, software, and configuration details of all the connected endpoints, regardless of location.

Software deployment
From automated group and one-off deployments to removing unauthorized software, Automox enables you to deploy, verify, and enforce software installation and configuration on all endpoints.

Role-Based Access Control (RBAC)
Automox can define individual access by the full administrator, read-only, billing admin, or patching admin to ensure users have the necessary privileges based on their required tasks.

Fully featured API
The Automox API is a powerful interface integrating Automox platform data into other applications to control your devices, policies, and configurations.

Pre-built reports
Automox delivers out-of-the-box reports covering device activity, status and history, compliance, pre-patch, and historical patch activity. Reports can be easily generated, viewed, and downloaded from the console.

Patch management
Perform continuous patching of OS and third-party applications. Patches can be pulled down directly by the Automox agent or from a locally maintained WSUS server that is a trusted source of patches reachable by the agent.

Task and workflow automation
The Automox platform is based on an extensible and scalable architecture that enables IT administrators to create any custom task using Automox Worklets™. Powered by PowerShell® and Bash scripting, the platform can execute and automate Worklets across any managed device.

Remote Control
Automox elevates your IT and Help Desk troubleshooting operations by removing the need for another tool or process. With Automox Remote Control, you can access, investigate, and fix issues on Windows devices from the same VPN-free console and agent you use for endpoint management, shortening the time to resolve tickets.

Automated Vulnerability Remediation (AVR)
Even with the best vulnerability detection solutions, remediation can be very manual. You can minimize exposure windows and discover unmanaged endpoints with Automated Vulnerability Remediation (AVR). Delaying critical vulnerability remediation means leaving your organization defenseless against cyberattacks. With AVR, you get full-cycle remediation to close your exposure window in minutes.

Third-Party Patching
Manage, configure, and track third-party inventory and natively patch it all from one place. The fatigue and frustration of managing third-party software can be a distant memory with Automox. We take care of third-party patching, maintenance, and deployments with minimal uplift for IT. With a growing list of supported third-party vendors, effortless patching starts here.

AUTOMOX

INFO@AUTOMOX.COM
WWW.AUTOMOX.COM