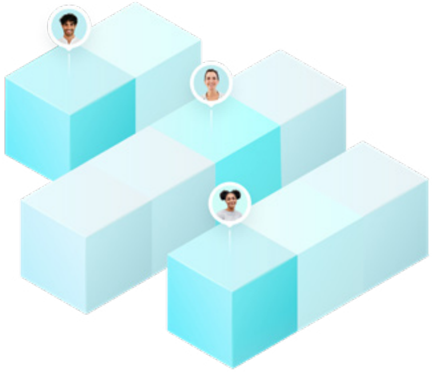
AUTOMOX

TECHNICAL BRIEF

The Automox Platform



Automox is the IT operations platform for modern organizations. It makes it easy to keep cross-platform endpoints patched, configured, controlled, and secured. Automox is an IT and security-focused organization; by prioritizing safety, our customers achieve a higher level of security. For the latest information on Automox's Security program, visit the Trust Center.

Empower your ITOps to take their time back with Automox Worklet™ automation scripts.. Eliminate manual tasks across all your endpoints (regardless of OS or location) and improve your endpoint security posture and compliance. With Automox, there's no need to spend hours combing through audit spreadsheets or applying fixes manually.

Single, Secure-by-Design Endpoint Agent

The Automox® agent is lightweight and deployable across Microsoft Windows®, macOS®, or Linux endpoints. With just an internet connection, the agent connects to Automox to automatically patch, control, configure, and secure your endpoints. The 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. Automation is deployed through scripts via the agent (called Automox Worklets ™) and is signed to improve your security posture and reduce risk. 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

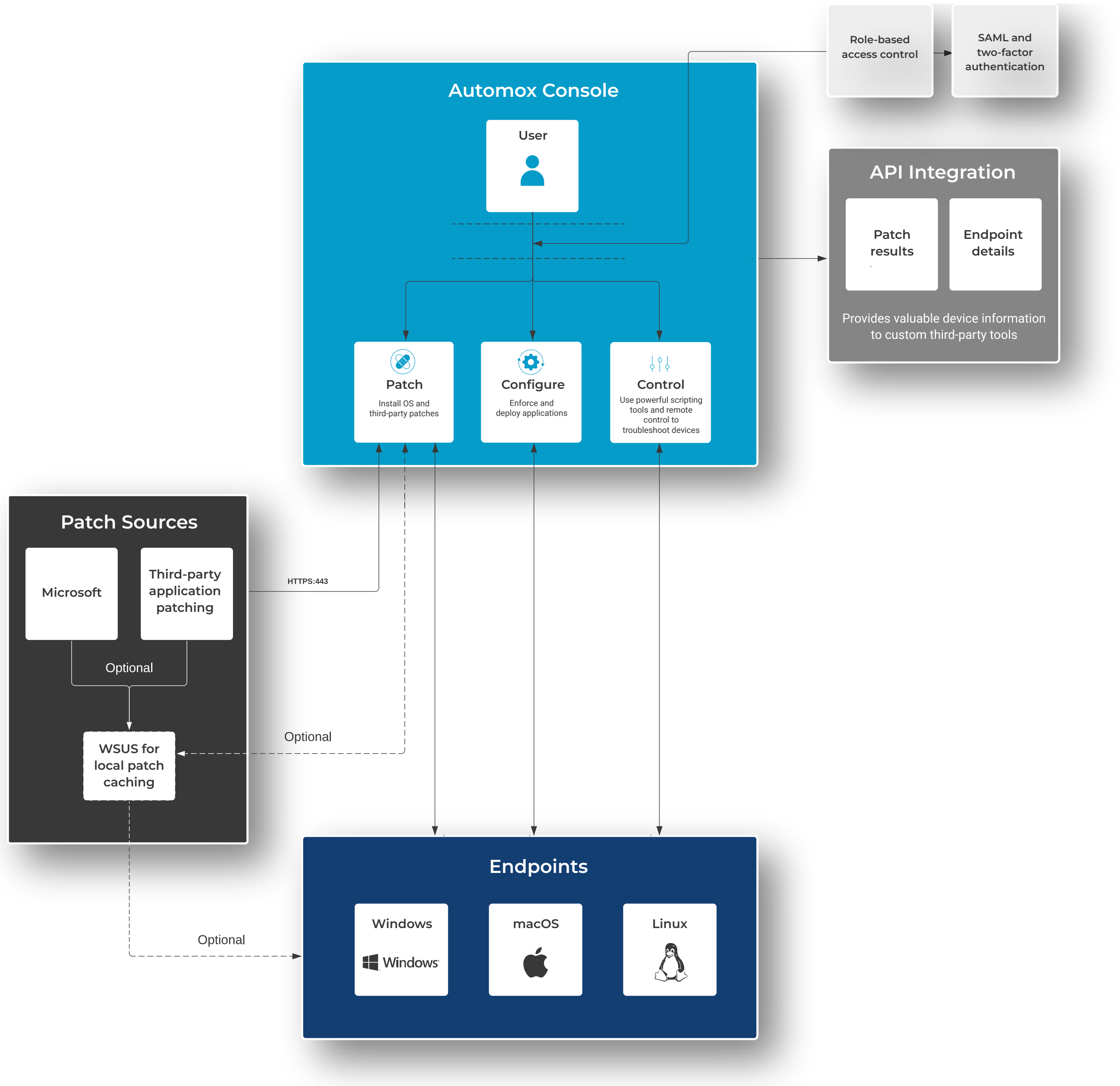
With Automox, you eradicate the need for legacy hardware like servers, clunky VPN connections, or multiple tools for different operating systems. Automox will patch, deploy, and configure devices automatically, from anywhere on Earth.

Modern, Scalable, and Secure Foundation

The Automox platform architecture uses a clustered design to ensure high availability, reliability, and flexibility to instantly adapt to your organization's needs without worrying about performance. Automox leverages the Amazon Web Services 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.

How Automox Works

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


Role-based access control
SAML and two-factor authentication
Automox Console
User
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
Optional
Endpoints
Windows
Windows
macOS
Linux

AUTOMOX

SECURITY-FOCUSED DEVELOPMENT

Automox's Security and Product Development teams operate with a security-driven culture threaded throughout our product and development processes. We follow 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 rigorous automated and manual testing in a staging environment to catch and eliminate operational and security issues. You can see the result of this product and security philosophy by reviewing the "Secure for All, Always" page.

CSA STAR EU-US DPF GDPR PCI Security Standards Council AICPA SOC TX-RAMP CERTIFIED

Third-Party Patching

Manage, configure, and track third-party inventory and natively patch it all from one place. We automatically collect, scan, store, and distribute over 500 third-party applications. Automox offers, FREE, the Patch Safe feature, which utilizes industry-leading malware detection on all third-party packages processed by the platform. If any package is flagged as potentially dangerous, it will not be distributed by the tool. Automox is a proactive partner in your organization in preventing and patching vulnerabilities.

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. Automox can integrate with your ITSM tools to enrich your CMDB and automate IT workflows.

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.

OS 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

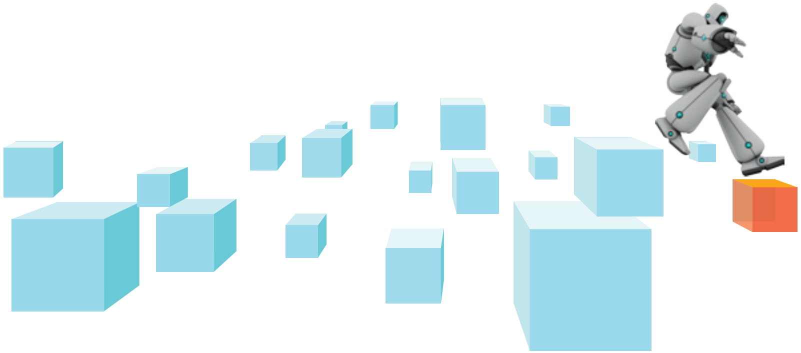
The Automox platform is based on an extensible and scalable architecture that enables IT administrators to create any custom task using Automox Worklet Automation Scripts. Powered by PowerShell® and bash scripting, the platform can execute and automate Worklets across any managed device.

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.



Get a free 15-day trial to see why Automox is the leading VPN-free IT automation solution for modern organizations. Sign up today! automox.com/signup