SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

TECHNICAL BRIEF

# The Automox Platform

**Automox enables IT Operations (ITOps) to dramatically reduce the time, complexity, and effort required to effectively manage their IT estate. The Automox platform delivers cloud-native agility, global visibility, and workflow automation to assess, analyze, and act on all critical information across on-premises and remote endpoints; all from an intuitive, web-based console.**

## SECURE-BY-DESIGN ENDPOINT AGENT

At under 10MB in size, the Automox® agent is low impact, lightweight, and can be deployed across Microsoft® Windows®, macOS®, or Linux® endpoints. The Automox agent is responsible for software and patch deployment, monitoring, and executing process operations on the endpoint. The Automox agent uses privileged access to the endpoint, and because of this, it has multiple security features built in to safeguard the endpoint from eavesdropping and unwanted access attempts. All communications are encrypted with transport layer security (TLS) 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.

## CLOUD-NATIVE, MULTI-TENANT ARCHITECTURE

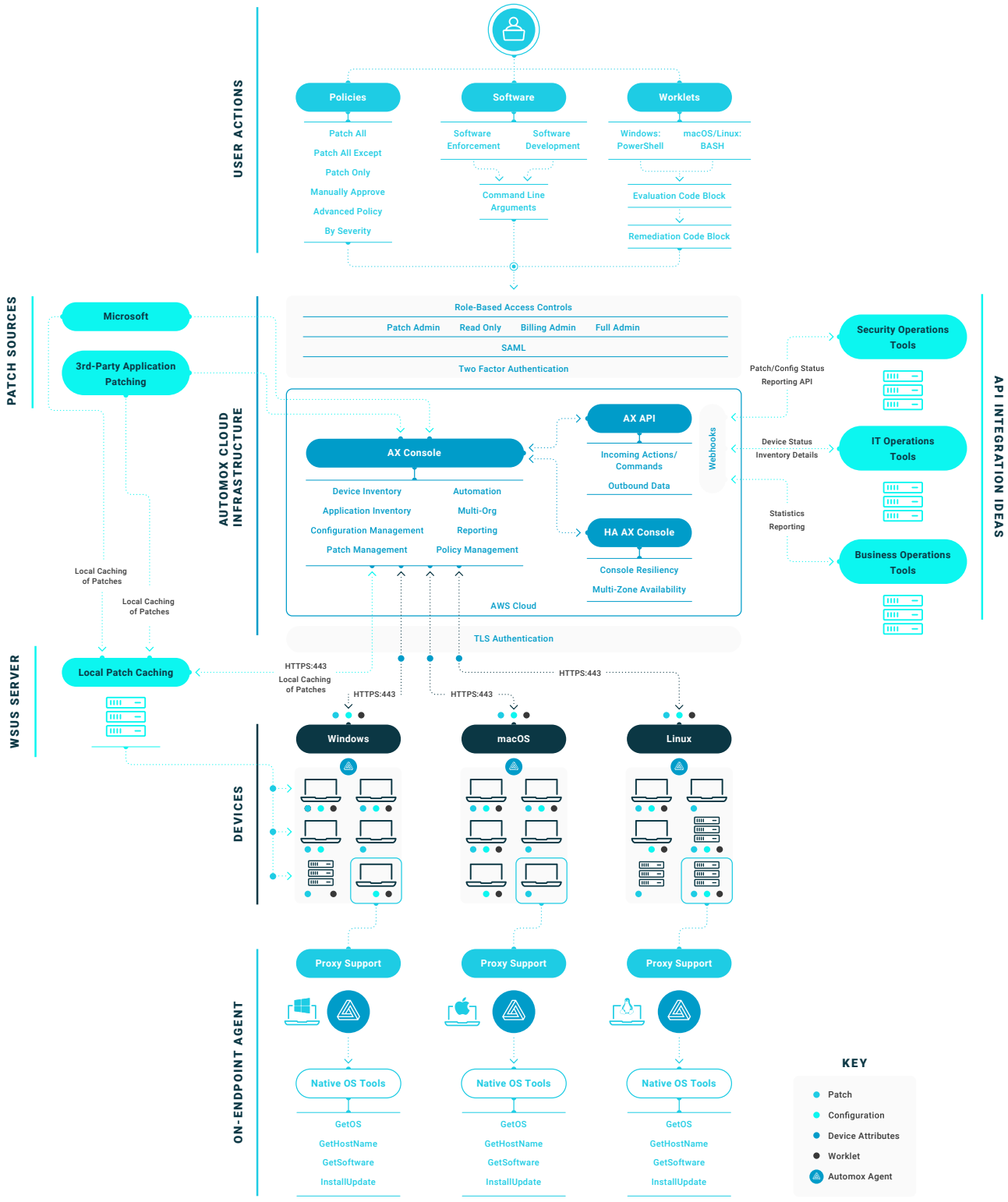
Automox's cloud-native architecture requires absolutely no on-premises infrastructure for complete functionality, meaning zero maintenance and zero VPNs needed to manage your on-premises, cloud, and remote endpoints. The Automox platform utilizes AWS® and native services such as Identity and Access Management (IAM), CloudTrail®, and CloudWatch to enable segmenting, auditing, and monitoring of activity and access to production systems, which provides faster anomaly detection.

## 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 ensure services and data are safe, secure, and continuously available. Automox follows frequently tested backup and restore procedures to ensure the highest level of reliability and security.

## AUTOMOX FUNCTIONAL DIAGRAM

The diagram below illustrates basic operational workflows and identifies various components of the platform.



SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

## 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 rigorous automated and manual testing in a staging environment to catch and eliminate operational and security issues.

### Industry certifications

SOC 2 Type II certification

## ENFORCED ACCESS POLICIES AND LOGGING

Automox implements IAM policies and partitioned access to systems for staff, in adoption of 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, monitored using OSSEC and other tools 24x7.

### Multi-OS support

Automox offers support for Windows, macOS, and Linux, 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, no matter their location.

### 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 ITOps 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.

### Software deployment

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

### Role-Based Access Control (RBAC)

Automox offers the ability to define individual access by full administrator, read only, billing admin, or patching admin to ensure users are granted the necessary privileges based on their required tasks.

### Fully featured API

The Automox API is a powerful interface that integrates Automox platform data into other applications to control your devices, policies, and configurations. Automox can be integrated with other security operations, ITOps, or business intelligence solutions.

### Pre-built reports

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

For additional information please contact
**sales@srccybersolutions.com**

+91 120 232 0960 / 1

www.srccybersolutions.com