AUTOMOX

TECHNICAL SOLUTIONS BRIEF

AUTOMOX PATCHING AND ENDPOINT HARDENING PLATFORM

Automox enables IT teams to dramatically reduce the time, complexity, and effort required to effectively secure and manage endpoints. Automox's cloud-native platform delivers workflow automation that enforces OS and third-party patch management, security configurations, and custom scripting across on-premise and remote endpoints; all from an intuitive, web-based console.

SECURE-BY-DESIGN ENDPOINT AGENT

At under 16 MB, the Automox agent is low impact and lightweight, and can be deployed across Windows, macOS, or Linux endpoints. The Automox endpoint agent is responsible for monitoring and controlling the endpoint patch and management process. To facilitate this, the agent requires privileged access to the system to access secured locations. Because of this privilege, we architected the agent with multiple security features to protect the endpoint. All communications are encrypted with TLS and authenticated with public-key cryptography. Automated tests ensure agent integrity and that it is not vulnerable to replay or MITM attacks.

MULTI-TENANT, CLOUD-HOSTED INFRASTRUCTURE

Our cloud-native solution requires no on-premises infrastructure to manage corporate devices, meaning zero maintenance and zero VPN licenses required to connect to the patching and endpoint hardening platform.

We host everything on AWS and utilize many of their security services, including but not limited to IAM, CloudTrail, and CloudWatch. These services allow us to segment, audit, and monitor activity and access to our production systems, which enables us to identify anomalies quickly.

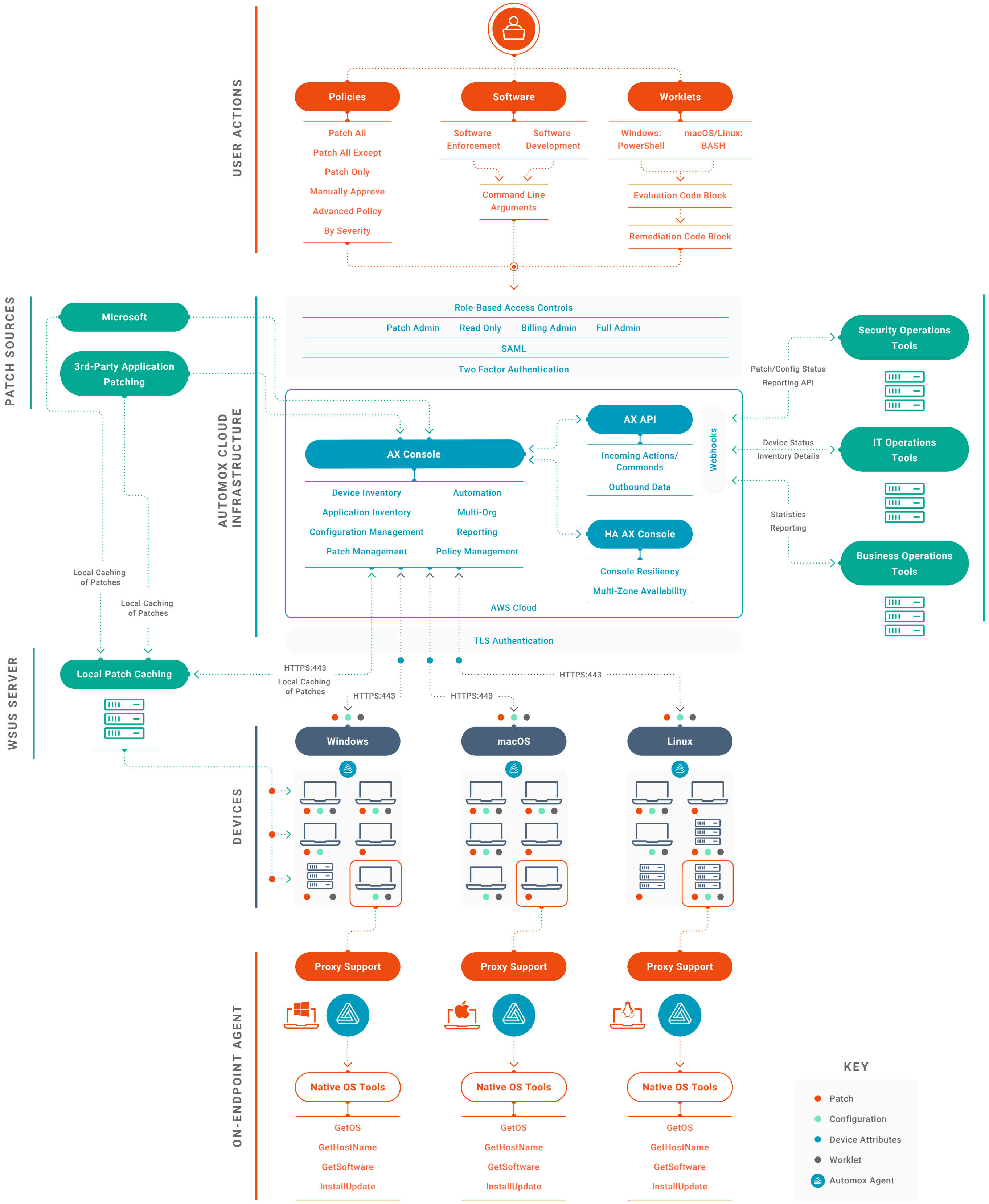
SCALABLE, RELIABILITY-FOCUSED SOLUTION

The Automox architecture uses a clustered design to ensure high availability, reliability, and ability to scale up or down on demand quickly.

We leverage the AWS concepts of regions and availability zones to ensure our services and your data are safe, secure, and 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.



SECURITY-FIRST DEVELOPMENT PROCESS

The Automox development process is focused on quality and security. We develop software using a modern, quality-driven process and mindset to ensure high reliability. All product changes undergo rigorous automated and manual testing in a staging environment to detect and eliminate operational and security issues before deployment to production.

Industry certifications

We received our SOC II Type I certification in 2019 and expect to receive SOC II Type II in 2020.

NEED-BASED ACCESS POLICIES AND MANDATORY LOGGING

At Automox, we implement IAM policies and partition access to our systems to give our team members the least amount of access to perform their development and maintenance tasks. Need-based access is granted on a per-employee basis and regularly reviewed. We also use monitoring software to track all console logins and privileged command execution, alerting on any anomalous activity. All log files are written to centralized log hosts which are hardened and monitored using OSSEC and other tools.

KEY FEATURES AND BENEFITS

Cross-OS support

Automox offers support for Windows, macOS, and Linux devices, plus a growing library of third-party applications. Automox offers a single platform to patch and harden all your endpoints, no matter the domain.

Straightforward reporting

Automox offers real-time, up-to-date reports. The tool includes access to view all activity, device status and history, non-compliant devices, and patching impact prior to patching corporate devices.

Automated patch management

Perform continuous patching of OS and third-party applications. Patches can be pulled down directly to the Automox Agent using our cloud-native infrastructure, or from a locally maintained WSUS server that is a trusted source of patches within the organization’s perimeter.

Automox Worklets™

The Automox platform is based on an open extensible automation architecture that allows IT operations to create any custom task using Automox Worklets. Powered by PowerShell and Bash scripting, Automox consumes and automates worklets across any managed device.

Fully featured and documented API

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

Continuous telemetry

Automox is in constant contact with your corporate endpoints and pulls the full breadth of hardware, software, patches, and configuration details of the connected devices. The platform offers in-depth visibility to identify non-compliant and compliant devices.

Software deployment

From automated installations based on policies to one-off installations using an Automox Worklet, Automox lets you deploy and verify software installation to any or all corporate devices.

Automated policy enforcement

The Automox Platform offers full control of your response to system or software updates, preventing configuration drift within the organization. Policy features include: patch all, patch only, include/exclude, manually approve, patch by severity, or set up advanced rules for which OS and software is patched.

Role-based access control

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