ENDPOINT HARDENING & PATCH MANAGEMENT CHEAT SHEET

Choosing a Vendor

Patch and endpoint management are vital components of a broader IT Operations (ITOps) strategy and evaluating your next patch management solution is a lot easier when you have an inside edge on what is important. At Automox, we understand what makes a market-disrupting endpoint hardening and patch management solution, so we've put together a helpful list of capabilities to review when evaluating vendors. Use this list to quickly understand the important attributes of a comprehensive, cloud-native ITOps platform that provides endpoint hardening and patch management and start the conversation with your vendor to make sure there aren't any unwelcome surprises for your team.

CUSTOMER EXPERIENCE

- Multiple communication channels for your users to reach support (e.g., phone, email, chat, and social media)

- Customer-friendly and easy method to check the status of support requests

- End-user access to self-service content

- Vendor-conducted onboarding of your team with the appropriate structure, training, and resources

- Ongoing support for your team at the level that you need, including a dedicated account manager for your organization

- Regular training and knowledge transfer sessions led by product experts

- Ability to submit ideas and feedback to the vendor to suggest improvements to the product roadmap

COST & VALUE

- An endpoint hardening and patch management platform based on a cloud-native, Software as a Service (SaaS) architecture, free from on-premises infrastructure requirements

- Automated policies to avoid configuration drift and repetitive, manual intervention

- A globally available, cloud-based service

- Reduced administrative labor hours and operations costs

- Extensive capability to reduce data breaches that impact operations

- Expedited vulnerability remediation across an organization when new insights from investigations surface

- Management of multiple Operating System (OS) environments from a single console

- Reduced dependency on costly on-premises tools

- Extensive support to migrate patch management from on-premises tools to a cloud-native solution

- Continuous patch management to help make endpoints less vulnerable to attackers

FUNCTIONALITY

- Instant visibility into vulnerability exposure without relying on manual processes or trouble ticketing between SecOps and ITOps

- Clear identification and communication of vulnerability severity and prioritization of actions and compliance goals

- Native support for Microsoft® Windows®, macOS®, and Linux® devices from a single platform and management console

- Extensive built-in support for third-party patches

- Built-in support for security configuration management

- Built-in support for enterprise software deployment

- Native support for custom scripting at scale

- In-depth and actionable visibility into noncompliant endpoints

- Reduction of patch management complexity

- Complete support for a remote workforce

ADMIN MANAGEMENT

- Easy-to-use administration to add, edit, and monitor devices

- Easy-to-use administration to add, edit, and monitor policies

- View, edit, and/or manage users and organizations with Role-Based Access Controls (RBACs)

- Zero on-premises infrastructure to manage to free up ITOps team for value-added activities

LIGHTWEIGHT AGENT

- Small footprint agent with an imperceptible performance impact on endpoints

- Platform agent with a continuous channel for communication regardless of location to the server

- An agent that requires less than 10MB to run on each endpoint

AUTOMATION

- Comprehensive ability to take any action on endpoints and automatically enforce those actions

- Global, cloud-native, and infrastructure-free solution with no dependence on local distribution servers and complex infrastructure

- Automation features to reduce alert fatigue and improve organizational speed and agility

- Continuous enforcement of patching and configuration policy compliance requirements, regardless of device location

- Rich set of Application Program Interfaces (APIs) for integrating and automating functionality within an organization's existing tools

- Automatic deployment of software and updates at scale

REPORTING

- Out-of-the-box reporting on device activity, device status and history, device compliance, and historical patch activity

- Generate, view, and download reports easily from the console or UI/UX

- An API that provides accessibility for custom workflow processes to business intelligence reporting

IMPROVE YOUR ENDPOINT HARDENING GAME WITH 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, cloud-native platform that closes the aperture of attack by more than 80%, with just half the effort of legacy 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. ITOps and SecOps teams can quickly gain control and share visibility of on-premises, remote, and virtual endpoints without the need to deploy costly infrastructure.

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

Multi-OS support
Support for Windows, macOS, and Linux devices

Endpoint visibility
In-depth visibility to identify noncompliant devices

Lightweight agent
Efficient and lightweight agent — under 10MB

RBAC
Set individual permissions for users and groups

Rich API
Fully featured and documented API for complete integration into your infrastructure

Software deployment
Painlessly deploy, manage, and enforce operating system and third-party applications globally

Straightforward reporting
Real-time, up-to-date reports for meaningful, appropriate, and actionable insight

---

READY TO GET STARTED? TRY AUTOMOX FOR YOURSELF.

Get a free 15-day trial to see why Automox is the only cloud-native, easy-to-use platform for modern IT Operations. **automox.com/signup**

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.