SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

Hybrid Work is the New Normal

Does your IT operations team have full visibility into your dispersed environment?

> Many organizations have been supporting the remote or hybrid model for years. But, as things continue to shift, how confident are you that you are efficiently managing all of your remote endpoints?

Here are **five key considerations** for securing remote endpoints with the latest software, patches, and configurations.

1 Can you secure your workers' endpoints without a VPN?

MAKE SURE YOUR VPN ISN'T A CRITICAL POINT FOR SECURING YOUR ENDPOINTS.

Legacy patching platforms can only update systems and software on remote endpoints that are connected to the corporate network via virtual private network (VPN). Users often avoid connecting via VPN to circumvent the tedious, frustrating, and time-consuming process of making updates over slow connections.

Automox **seamlessly updates and patches any corporate endpoint** that's connected to the internet, which means users are always current with patches and configurations.

2 Will you be able to outmaneuver attackers when new vulnerabilities are announced?

ATTACKERS ARE WEAPONIZING VULNERABILITIES FASTER AND MORE FREQUENTLY THAN EVER.

In fact, the moment new critical vulnerabilities are reported sets off a race to see if you can patch vulnerabilities faster than adversaries can exploit them. To be safe, you need to remediate critical vulnerabilities within 72 hours of their announcement. Traditional, VPN-based patching solutions will likely not allow you to remediate in time.

Automox customers, on the other hand, meet this speed threshold thanks to **automated, cloud-native remediation**.

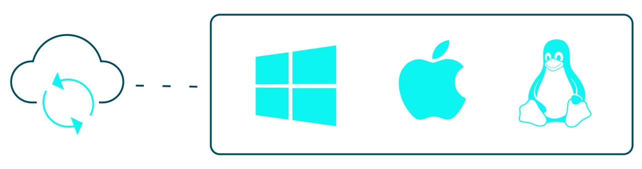
3 Can you automate your endpoint and patch management on devices not connected to your network?

PATCHING CAN BE A THANKLESS, TIME-CONSUMING TASK THAT'S EASY TO FALL BEHIND ON.

What's worse, IT administrators often can't see which software titles on which systems are out of date and susceptible to attack. Unpatched and misconfigured laptops are a huge concern for maintaining cyber hygiene. And an increase in remote laptops not connected to the corporate network for extended periods will only compound this problem.

Automox gives you visibility into the status of remote endpoints so you can **customize and automate both operating system (OS) and third-party application updates or patches**.

4 Are you able to patch and update across operating systems and third-party software?



58% OF DATA BREACHES ARE ATTRIBUTED TO POOR PATCH MANAGEMENT.*

Yet managing and maintaining the latest software versions and configurations across multiple operating systems and myriad remote laptops is a huge hurdle for legacy patch platforms.

Automox keeps IT teams ahead of attackers across **Windows®, macOS®, and Linux® platforms, along with a growing library of third-party patching support** — to secure remote laptops through a single cloud-native console.

5 Do you have visibility and control of all your remote endpoints?

IT'S DIFFICULT TO AUTOMATE POLICIES FOR REMOTE ENDPOINTS YOU CAN'T SEE.

As a cloud-native solution, Automox provides a complete inventory of all hardware, software, patches, and configuration details for your remote endpoints. You'll have a unified view of your remote laptops to identify misconfigured systems, discover missing patches, remediate patch vulnerabilities, deploy required software, and fix misconfigured systems across Windows, macOS, and Linux — without the need for multiple tools.

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.

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com |

* AimPoint Group (2020) Cyber Hygiene Report.