WORKING REMOTELY IS THE NEW NORMAL

Can your IT make the shift while seamlessly keeping your corporate endpoints secure?

SHIFTING TO A REMOTE WORKFORCE IS NOT NEW NEWS

Many organizations have been supporting the model for years. But, if your organization is embracing remote work for the first time you have a lot to consider — specifically, how to manage all your newly roaming devices and, most importantly, how to keep these remote endpoints secure.

Here are the five key considerations to ensure a seamless strategy for securing remote laptops 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 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?

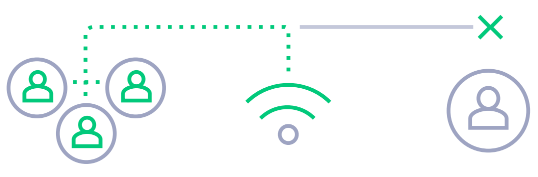
Attackers are weaponizing vulnerabilities faster and more frequently than ever.

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?



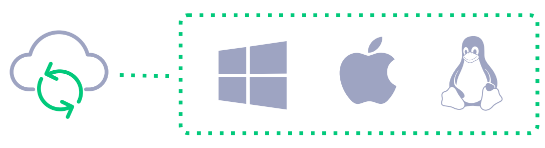
Patching can be a thankless, time-consuming task that's easy to fall behind on.

What's worse, IT administrators often can't see which software titles on which systems are out of date and susceptible to attack.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 OS and third-party application updates or patches.**

4

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



57% of data breaches are attributed to poor patch management.*

Additionally, third party applications are responsible for over 75% of all endpoint vulnerabilities. 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 laptops you can't see.

As a cloud-native solution, Automox is uniquely able to provide **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.

Automox has solutions no matter which path you choose. **Contact us now for a demo** of how we can deliver fast, simple cyber hygiene solutions for your remote workforce.

* Ponemon Institute recently found that 57% of data breaches are attributed to poor patch management.

About 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 cyber hygiene platform that closes the aperture of attack by more than 80% with just half the effort of traditional 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. IT and SecOps can quickly gain control and share visibility of on-prem, remote and virtual endpoints without the need to deploy costly infrastructure.

Start your free trial