SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

GUIDE

6 REASONS YOU SHOULD SWITCH TO CLOUD-BASED PATCH MANAGEMENT

In the ever-evolving digital landscape, there are many reasons why organizations may consider cloud-based patch management as an alternative to on-premise solutions. Traditional, on-premise patch management platforms were designed for a different era; cyber threats have grown and changed significantly in recent years. Taking a more sophisticated approach to patch management is essential to securing systems adequately. Cloud-native patching and endpoint hardening tools are designed for the modern workplace and offer users a bevy of new features and options and eliminate much of the cost burden associated with on-premise solutions.

With cloud-based tools, organizations can ensure every piece of their infrastructure is getting critical security updates within an adequate time frame. The manually driven workflows of traditional on-premise solutions make the job of patch management a slow and arduous process. Meanwhile, attackers can weaponize a known vulnerability in seven days or less. Exorbitantly long time-to-patch windows and overly complex patching processes make legacy, on-premise patching solutions extremely inefficient in the modern workplace. With a modern patching solution, organizations can reduce their time-to-patch window and get their patching and endpoint hardening up to the speed they need.

HERE ARE 6 REASONS WHY YOU SHOULD SWITCH TO A CLOUD-BASED PATCHING AND ENDPOINT HARDENING SOLUTION.

01

Cost Burden to Manage Other Solutions

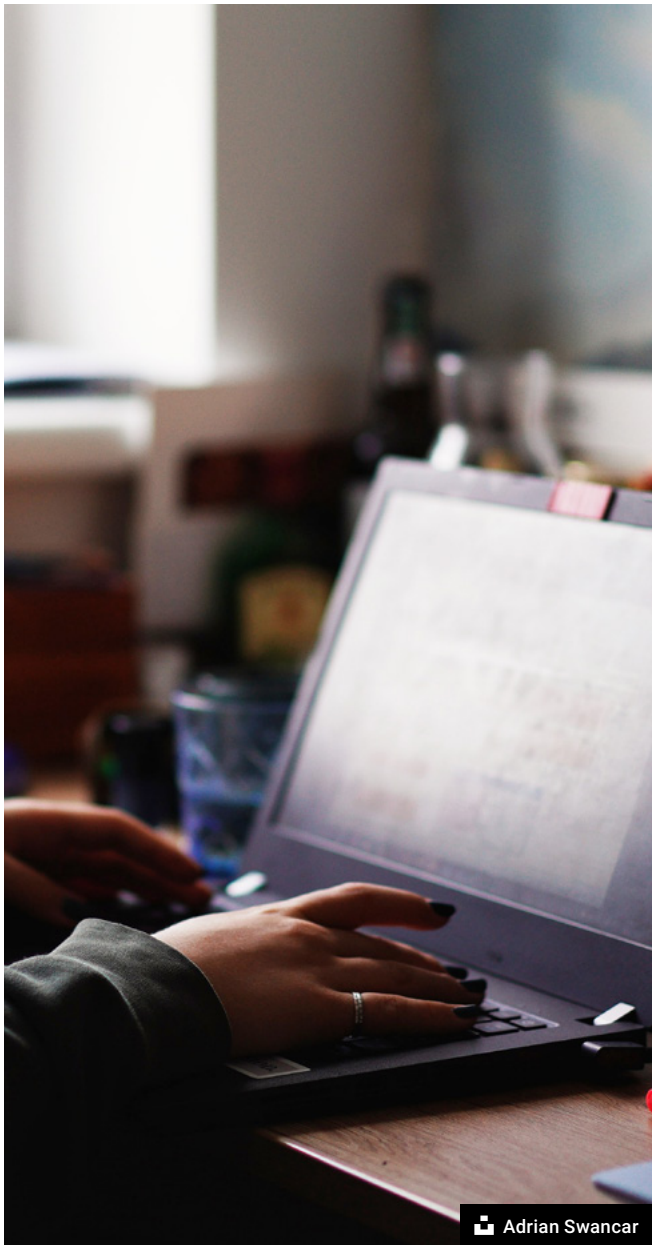
Cloud-based patching alternatives can help organizations conserve limited IT resources and reduce overall costs associated with patch management. Legacy, on-premise patching tools often come with an array of hidden expenses, from additional tool purchases to time spent on maintenance.

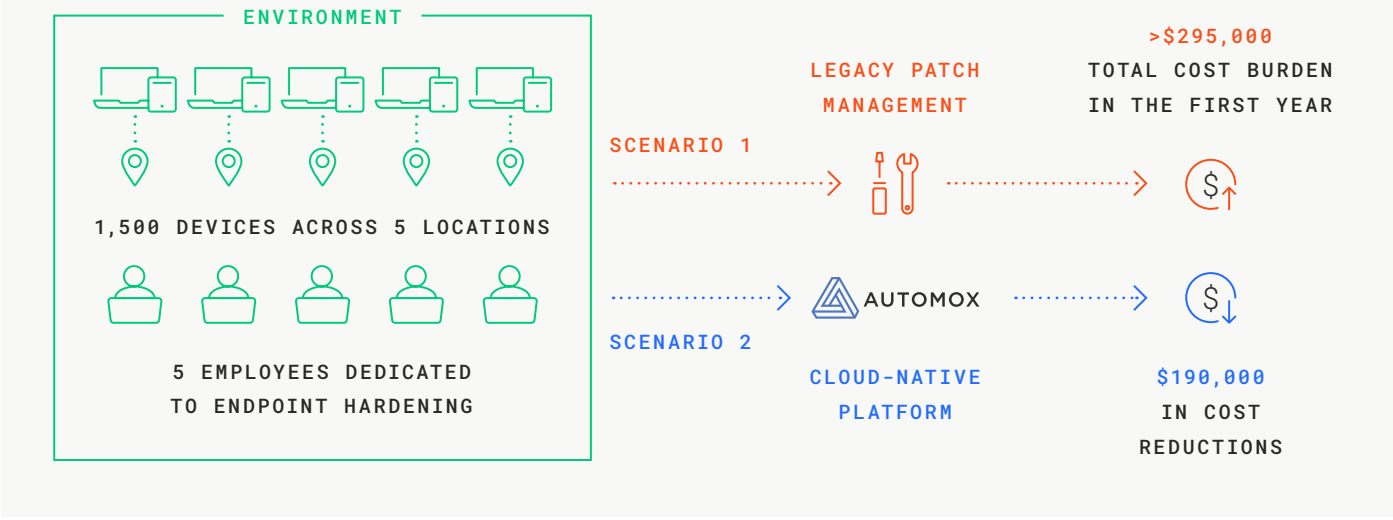
The limitations of on-premise patching solutions, such as WSUS or SCCM, may not seem like a big deal initially, but these restrictions on user capabilities can actually end up costing organizations quite a bit, in terms of both finances and resources.

MOST ON-PREMISE PATCHING SOLUTIONS ARE SINGLE-USE TOOLS

For example, WSUS is good for patching Windows, but not much else. Organizations that rely on multiple operating systems and third-party applications may find that they need several tools to meet the needs of their patching workloads.

Time spent on maintenance, configuration, and employee education for multiple tools can really add up. Some products may require upwards of 40 hours of training per employee. Survey data suggests that most IT staff are spending around 38 hours a week just on the process of deploying patches with legacy tools.





Despite IT staff dedicating countless hours to maintaining, configuring, and troubleshooting these tools, around 80% of CISOs and CIOs admit they've experienced the shock of discovering a patch they thought deployed successfully had actually failed. Legacy tools offer little to no insight on patch status and are especially weak when it comes to endpoint visibility. Insufficient reporting impedes the process of patch management and can undermine an organization's cyber hygiene efforts.

More, organizations with multiple geographic locations may find that many of these tasks may need to be repeated in each region. In an environment of 1500 devices across 5 geo locations, with five employees dedicated to endpoint hardening, the total cost burden of legacy patch management can exceed $295,000 in just the first year.

Even with such a massive investment in timeand resources, 74% of organizations say they can't patch fast enough because they don't have enough employees. Another 64% say they are looking to hire more dedicated resources for patching within the next year. Legacy patch management protocols were revolutionary when they were released 20 years ago, but they are not sufficient when it comes to handling the needs of the modern digital landscape. The cost of legacy patch management is too high and the return value is far too low.

Comparatively, a cloud-based solution reduces complexity and increases patching efficiency. In the 1500-device scenario above, cloud-native platforms like Automox can yield $190,000 in cost reductions.

02

Improved Operational Efficiency

The cost of on-premise patch management solutions can also be measured by the overall effect on your cybersecurity strategy. Reliance on outdated technologies can lead to a number of unnecessary complexities in your patch management strategy.

Legacy, on-premise patch management solutions are severely limited in their ability to patch across diverse infrastructure. These options are often designed as single-purpose tools, which can lead to a lot of frustration. Configuring pathways for patching alternative operating systems or third-party applications can be difficult and time-consuming, if it's even possible at all. In many cases, IT staff will need multiple tools and agents to complete patching tasks. A number of these on-premise solutions require on-site servers and ongoing maintenance — including manual patching of the servers themselves.

In addition to the burden of dedicating time and effort to the maintenance and configuration of multiple on-premise patching solutions, the use of multiple consoles can also make the process of reporting and tracking patch status overly complex. Under the legacy patching paradigm, users are often responsible for manually tracking, prioritizing and testing new patches. These processes need to be repeated multiple times for different product vendors — and staff will also need to ensure these patches are actually deployed successfully across the entire network.

OVERALL, THERE ARE TOO MANY TOOLS WITH INSUFFICIENT FUNCTIONALITY FOR THE MODERN WORKPLACE.

Today's digital landscape boasts a wide variety of operating systems, third-party applications, and endpoints. Desktops, laptops, and tablets are all examples of devices on your network that need to be secured against threats, and legacy patch management platforms simply do not give users the ability to patch their networks efficiently or with confidence. Across the board, IT staff are spending too much time on redundant and needlessly complex tasks that can be streamlined with modern technology.

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

Current estimates suggest that for most organizations, the average time to patch sits at 102 days. In some cases, organizations report that it can take up to 6 months for them to deploy a single patch. With cloud-based platforms, users can eliminate much of the manual labor associated with patch management. Advances in automation and cloud computing reduce manual and error-prone tasks while increasing the speed, efficiency, and accuracy of your patching and endpoint hardening strategy. Instead of having to patch each and every operating system, third-party application, and geographic location separately, a cloud-based SaaS strategy allows users to configure and patch every device from a single console. Every piece of equipment on your network gets treated exactly the same, no matter where it is located. With just a few clicks, users can deploy patches, monitor patch status, and generate reports.

Modern, cloud-native technology provides users with the agility they need to implement patch management best practices and meet new security standards across their entire infrastructure, regardless of OS or location.

BY IMPROVING THE OPERATIONAL EFFICIENCY OF PATCH MANAGEMENT ROUTINES, ORGANIZATIONS CAN ENSURE THEIR ENDPOINT HARDENING STRATEGY IS FUNCTIONING AT ITS BEST AND THAT PATCHES ARE GETTING DEPLOYED AS QUICKLY AS POSSIBLE.

> "Automox has been a huge time saver. We had a full-time IT Manager working 30 hours per week to keep our systems patched and now it takes him an hour per week. The time savings has been massive."
>
> Jared Haggerty / CEO, Databerry

03

Complete Visibility of Your Distributed Workforce

Endpoint visibility is a top concern for organizations today. Many enterprises have seen the number of endpoints on their systems expand exponentially as the modern workplace changes face. In the digital landscape today, a single employee can represent multiple endpoints and each endpoint is a device that needs to be secured against threats.

Statistics show that 68% of organizations say they were victims of an endpoint attack. Of those, 80% of respondents indicated they were attacked through a zero-day vulnerability — or that the attacker had used a new malware variant that their security solutions couldn't recognize.

A 24-hour patching threshold for zero-day vulnerabilities is the new standard organizations should be reaching for; deploying patches quickly is a key element of endpoint hardening best practices, as well as your overall patch management strategy. Endpoints are vulnerable, and your remote endpoints are in an especially prone position, as they are without the extra security of a corporate firewall.

ENDPOINT VISIBILITY IS CRUCIAL TO ENDPOINT SECURITY FOR A FEW KEY REASONS.

Dark endpoints, or endpoints that cannot be seen, pose a significant challenge for many organizations. Being able to verify what devices are on your network and create an inventory of your systems is key to virtually every area of cybersecurity best practices.

For endpoint hardening and patch management, organizations need to first know what needs to be patched. If you can't see a device, you can't verify if it's been patched.

Cloud-native platforms like Automox can be easily installed on any device and gives users the visibility they need to harden endpoints effectively. Because our tool is cloud-native, you can access your locally and globally distributed endpoints through their connection to the internet, with no reliance on virtual private networks (VPN). With accurate endpoint visibility, IT staff can detect and remediate potential threats in real-time.

04

Endpoint Security for Remote Teams

In recent times, many organizations have had to make a rapid shift to remote work. This can come with a unique set of challenges, especially in terms of endpoint security. Remote endpoints can be particularly vulnerable to threats for a number of reasons. These endpoints are outside the organization's perimeter and aren't covered by the protections the corporate infrastructure may have and are further put at risk by limitations in endpoint visibility.

In addition to the fact that remote devices are not going to be using a protected corporate connection, many organizations rely on VPN for hardening remote endpoints and deploying security updates.

LEGACY, ON-PREMISE PATCHING SOFTWARE TYPICALLY CANNOT BE USED FOR PATCHING REMOTE ENDPOINTS WITHOUT A VPN — WHICH REPRESENTS ANOTHER POTENTIALLY INEFFICIENT CORPORATE EXPENDITURE.

VPNs allow remote users to connect to the corporate network securely — however, these virtual networks are limited by bandwidth and can be costly to use. If a VPN exceeds its capacity, users may find themselves extremely frustrated with slow connections, if they can even connect at all. Ultimately, remote employees have to be able to connect their devices to the corporate network if they are to receive critical patches. This can be a huge stumbling block for everyone involved; slow connection speeds may impede an employee's ability to receive updates or they may refuse to connect to the VPN out of frustration. This means their devices may not receive updates in a timely manner, leaving those endpoints open and vulnerable to attack.

With SaaS adoption and cloud-based patching platforms, organizations can ensure every device is receiving critical security updates as soon as they're deployed, no matter their location. As long as your remote workers are using the internet, their devices can be updated seamlessly, and IT staff can use the same cloud-native platform to verify the patch status of remote endpoints.

Cloud-native solutions like Automox make it possible for IT staff to maintain an accurate inventory for remote teams and their devices, deploy patches quickly, and keep tabs on the overall status of their remote endpoints.

> "Cost savings come from reducing vulnerability and our security footprint as well. Automox has definitely helped us minimize our attack surface. Reports are coming in cleaner, with fewer critical things, and less panic. It has reduced our worry around patching and increased our ability to do patch management successfully."
>
> Adam Todd / Director of IT Operations, Cooke, Inc.

05

Cross-Platform Endpoint Management for Patching and Software Deployment

Legacy, on-premise platform solutions have a tendency to lock users into a specific "roadmap" for their products, however, modern SaaS-based solutions give users the freedom they need to customize their product experience. Automox is a cloud-based tool that can be used to patch across multiple operating systems and third-party applications but can also be used for software deployment and much more.

With cloud-native software solutions, versatility and agility is the name of the game. SaaS adoption strategies for patch management open many doors, allowing users to get more from a single tool. While legacy patching options are unable to adapt to new operating systems and applications, new programs can be added regularly to a cloud-based tool's functionality.

BEING ABLE TO PATCH ACROSS MULTIPLE OPERATING SYSTEMS AND THIRD-PARTY APPLICATIONS FROM A SINGLE PANE OF GLASS REDUCES MUCH OF THE WORK ASSOCIATED WITH PATCHING, AND THE SAME PLATFORM CAN ALSO BE USED TO AUTOMATE SOFTWARE DEPLOYMENT.

As a tool designed for the modern workplace, the Automox platform does more than just patching; it can also be used to manage software deployment across your systems as well.

With software deployment functionality, organizations can deploy software remotely to individual devices or across entire systems with confidence — and without interruption. Software deployment management tools allow organizations to effectively manage their endpoints and ensure each device is in compliance with corporate standards. This means users can see which version of the software is installed on each endpoint and can create a full software inventory for their organization — critical for ensuring proper endpoint protections are in place.

Automated software deployment can help organizations reduce the labor and costs associated with manual software deployment and minimize the burden of performing software updates.

06

More Scalability and Agility With Cloud-Based Tools

For organizations that want to look ahead and prepare for the future, scalability and agility are crucial features to look for in a cloud-based tool. With everything going on today, organizations need to know their tools can handle new tasks and adapt to changes in the workplace. Many companies have had to make a dramatic shift to remote work in recent times, and a majority of these organizations say that shift is here to stay. However, the recent influx of remote endpoints has really put on-premise patch management tools to the test, and many enterprises are finding that their legacy patching protocols are not up to snuff.

Cloud-based platforms like Automox offer the scalability organizations need to meet the demands of their workforce as it grows and changes shape. The SaaS-based solution can be deployed on virtually any device and is compatible with an array of other cloud-native security tools.

While on-premise patch management tools are known for being difficult to implement, configure, and maintain, cloud-based tools make integration easy for users. There is no required maintenance on the user-end; cloud-native tools update and maintain themselves.

CLOUD-BASED TOOLS CAN GROW AND CHANGE WITH YOUR ORGANIZATION.

A cloud-native platform can be installed on every endpoint, updated to include new applications on your systems, and used to meet a variety of cybersecurity needs.

This combination of scalability, agility, and versatility helps organizations move faster than potential adversaries, giving users the ability to see more and do more from a single pane of glass.

> "Automox gives us a tremendous amount of agility. Agents that took an hour per laptop when we were pushing them manually now take five minutes."
>
> Corey Dolan/ Network & Systems Admin, Tekside.iO

Being able to patch quickly and efficiently is a crucial element of cyber hygiene best practices and security management. Reliance on outdated technology is, at best, a hindrance to overall cybersecurity posture. The modern digital landscape requires a more robust patching protocol that can do more at a much faster pace.

By streamlining patching protocols, reducing redundancy in patching workloads, and offering an array of other desirable features, SaaS-based solutions can help organizations realize a patch management strategy that provides pre-incursion value, cuts costs, and meets new standards for cybersecurity. Minimizing your attack surface and staying ahead of threats necessitates a smaller time-to-patch window, and that can be accomplished with cloud-native cyber hygiene platforms like Automox.

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.