SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

GUIDE

MANAGING THE MODERN WORKFORCE:
YOUR GUIDE TO CHOOSING THE BEST WSUS ALTERNATIVE

For most, Windows Server Update Services (WSUS) is the first solution organizations will look at when exploring their options for automated patch management. As a legacy patch management platform, WSUS has been around for a long time and is still one of the most commonly used patch management platforms. However, being the most common choice doesn't make it the best choice.

While WSUS certainly has advantages over manual patching, there are plenty of alternative patching platforms on the market today — many of which are specially designed to meet the needs of the modern workplace. WSUS is good at what it does; however, it was built for a different era and struggles to keep up with the needs of more current infrastructure.

The digital landscape has transformed over the last 10 years, and today it is common for organizations to rely on multiple operating systems and third-party applications to meet their needs. Remote work is on the rise, and that means that IT staff are wrangling more remote endpoints than ever before. These are all problem areas for WSUS, but there are other options out there. Contemporary patching solutions solve many of the issues seen in legacy patch management platforms, whether it's cross-platform patch deployment or increased endpoint visibility.

Choosing a modern WSUS alternative can help organizations meet all of their patch management needs from a single interface, without the hassle of legacy technology. Modern patching solutions can even integrate with legacy options like WSUS, allowing users to keep features they like, such as local caching, without having to miss out on the versatility and improved user experience of a more current platform.

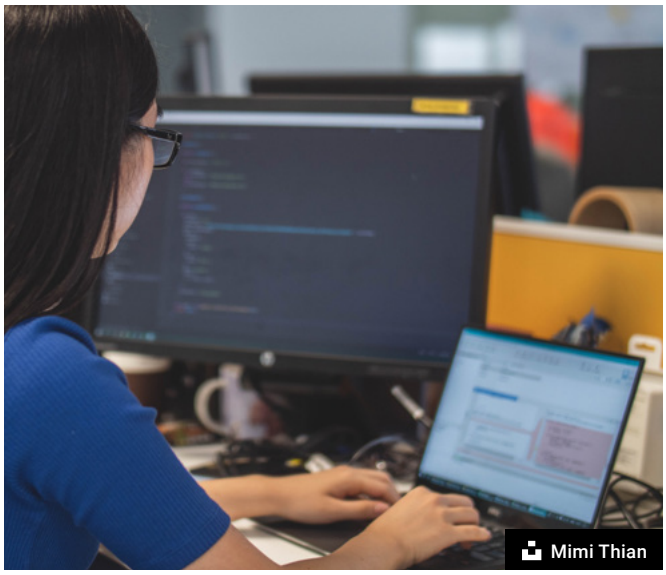
Here's your guide to help you choose the best alternative based on your corporate patching and endpoint hardening needs:

Why Use WSUS: Then vs Now?

When WSUS was first released in 2003 it revolutionized the process of patching Windows and Microsoft products. WSUS was the beginning of automated patching and gave IT staff the ability to start managing their patching.

WSUS is a Windows patching platform that is offered as a free tool from Microsoft that is installed on Windows servers as a role. The lack of upfront costs makes it an easily accessible option for organizations of any size, and if it is configured properly, WSUS handles the job of patching Windows OS and Microsoft products quite well. And at that time, most systems were Windows-based and alternative operating systems were unusual.

Unsurprisingly, it was a **popular first choice for organizations looking to begin automating their patch management**. However, the digital landscape has evolved over the last several years and WSUS has not kept pace.



For example, it is far more common for organizations today to utilize diverse infrastructure to meet their needs. WSUS lacks any sort of integration for Mac and Linux, and while it does offer some pathways for patching third-party applications, these options can be difficult to use and configure. When WSUS made its debut all those years ago, Windows systems were the norm and at that time, there were far fewer endpoints for IT to manage. Though Microsoft still holds the lion's share of the global desktop market, alternative OS are becoming far more common. Third-party applications also make up a significant portion of the cyber vulnerabilities found on systems today. And in today's world, it's not uncommon for a single employee to represent multiple endpoints on an organization's network. Desktops, laptops, and tablets are all examples of endpoints that need security updates; even smaller organizations may find they have hundreds of endpoints to look after. WSUS offers some rudimentary endpoint management but it is notoriously inefficient when it comes to handling the demands of more modern infrastructure.

Organizations may find they need multiple tools in order to patch alternative OS and third-party applications. Limited reporting and poor endpoint visibility can also create more work for IT staff as they may need to perform time-consuming tasks manually, such as checking the patch status of endpoints.

When selecting an alternative to WSUS, one of the first considerations is System Center Configuration Manager (SCCM). However, SCCM is not all that different. While SCCM does offer a bit more to users, it still doesn't offer users the full complement of features seen in more modern patch Mimi Thian management platforms.

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

What is the Difference Between SCCM and WSUS?

Both SCCM and WSUS are patch management tools offered by Microsoft. These platforms are on-premise solutions that are primarily designed for use with Windows OS and Microsoft products. While the two have many similarities, there are also some significant differences..

HOW DOES WSUS WORK?

WSUS is good at patching Windows and Microsoft products, but it lacks the versatility necessary for patching alternative operating systems like macOS or Linux and has limited capabilities when patching third-party apps. For organizations that run solely on Microsoft, WSUS can help patch systems semi-automatically and reduce the manual labor associated with patching. However, limitations in network visibility and reporting may still be of concern.

While the lack of upfront costs makes it an attractive option, WSUS is known for hidden expenses regarding maintenance and troubleshooting. Organizations may also have to acquire and maintain additional patching tools for alternative operating systems and third-party applications.

HOW DOES SCCM WORK?

SCCM is a paid patch management tool offered by Microsoft. SCCM uses the WSUS platform to check for and apply patches, but has some additional features and gives users more control over patch deployment. Larger organizations may see SCCM as a more desirable option compared to WSUS, but may find there are some difficulties with relying solely on SCCM for patch management.

With SCCM, users can find basic tools for generating reports and managing endpoints — options that are not seen in WSUS. As a Microsoft product, SCCM integrates best with Windows-based systems, though it does offer pathways for patching alternative OS as end-clients. However, these pathways can be difficult to configure and still require a Windows server to run. SCCM has limitations in its functionality for non-Windows OS and is also limited in its ability to patch third-party applications. In fact, difficulties with patching thirdparty apps is one of the top complaints from IT managers.

Overall, patching hybrid infrastructure with SCCM can quickly become a complicated process and will still require some work to be done manually.

MANAGING HIDDEN COSTS

While there are some strong points, the costs associated with SCCM can be prohibitive, especially given its limitations. SCCM is known for being expensive and is usually part of a larger suite of tools. Endpoints and servers are usually priced separately, and SCCM also requires a SQL server to run — which can further inflate costs and also requires a fair amount of maintenance. Given its limitations, the cost of SCCM can be hard to justify.


Hardware


Software


OPEX

WSUS and SCCM are both on-premise patch management tools, and while there are some differences, both tools are lacking the necessary agility for the modern digital landscape. Neither tool is well-equipped to handle the demands of diverse infrastructure.

Automate WSUS Patching with Alternative Patch Management

While WSUS has many drawbacks, there are some features that organizations may find desirable — such as the ability to locally cache updates within their environment. Local caching allows administrators to ensure that updates are only downloaded once, saving bandwidth on internet connections. Preserving local caching is important for many organizations, however, the limitations (and frustrations) of WSUS can still be addressed without losing those capabilities.

Automox is a cloud-native, cross-platform patching solution that can be used directly with WSUS. As a modern patch management platform, **Automox provides an array of desirable features** not seen in legacy patching solutions. With Automox, users can automate tedious tasks, such as creating patch status reports, and have confidence in reporting accuracy.

With proper configuration, Automox and WSUS can work together to create a better overall user experience without sacrificing local caching abilities. While Automox will work with WSUS configurations natively right off the bat, organizations will likely need to **configure their WSUS environment to properly integrate with Automox**. Many of these settings will be dependent upon a company's individual environment, however, the end-goal is to set WSUS up to locally cache updates, while the Automox console will administer these updates.

Once the integration is complete, organizations can have the best of both worlds: A modern, cross-platform patch management solution that's easy to use — and local caching capabilities. Updates can then be managed directly from the Automox platform.

Managing Windows Updates

As a WSUS alternative, Automox is fully capable of meeting patch management needs for organizations of all sizes — with or without WSUS. Compatibility with WSUS is a desirable feature, but Automox can also be used independently. Managing Windows updates without WSUS may seem like foreign territory, however, modern patch management solutions can **revolutionize the process of deploying and managing patches** — providing organizations the patch coverage they need and a more user-friendly platform.

As a cross-platform patching solution, Automox allows users to patch for Windows OS, as well as alternative operating systems such as macOS or Linux from a single interface. With Automox, users can also patch for third-party applications with ease.

Modern patch management platforms can also offer users an array of desirable, new features that can help organizations follow cyber hygiene best practices. Endpoint visibility, for instance, is crucial to ensuring every device within a system is properly patched. Legacy patch management solutions may offer some rudimentary endpoint visibility, but these options are often lacking in accuracy and are severely limited. Conversely, a patch management solution like Automox offers full endpoint visibility and gives users the ability to remediate threats in real-time.

Cybersecurity has become one of the top concerns for organizations today and ensuring that systems are patched appropriately is a crucial step in safeguarding against potential cyber threats. Estimates suggest that one out of every three data breaches links back to an unpatched vulnerability. It is not uncommon for patches to get delayed, or for a patch failure to go unnoticed; legacy patching solutions may be a step-up from manual patching, but they can still be overly complex and tedious to use. Limitations in endpoint visibility and reporting can also make it difficult for IT staff to determine what devices have or haven't been patched successfully. Modern solutions like Automox help resolve these headaches and streamline the patching process from start to finish. In addition to reducing patch fatigue, Automox can help users deploy patches faster.

Time-to-patch is a critical element of patch management best practices. Currently, the average time to patch is estimated to be between 60 and 105 days. It's also estimated that attackers can weaponize a known vulnerability in seven days on average. Once a patch is released, the clock starts ticking. **Equifax suffered a data breach** linked to a known vulnerability some two months after the patch was released. That breach affected the personal data of roughly 148 million Americans, and has cost Equifax **over $1.7 billion.**

In the past, WSUS was a sufficient option for organizations looking to take a step-up from manual patching. However, today's digital landscape demands a patching solution that does more.

WSUS Patching Without Servers

One of the defining features of WSUS is that it's a free tool installed on Windows servers, which makes it fairly easy to obtain. However, tools like WSUS can be difficult to configure and maintain.On-premise patching options struggle to keep pace with the needs of the modern workplace in many ways and being tied to a server is one of them.

On-premise patching solutions require a connection to an organization's network from inside the firewall or a VPN connection for patching endpoints. When WSUS was first created, remote endpoints were scarce, but today, employees are using multiple devices to get work done at the office as well as from home. Because remote work is far more common, there are more remote endpoints to manage and secure. On-premise patch management solutions are not ideal for patching remote devices due to their reliance on VPNs, or virtual private networks.

VPNs are costly, and they may struggle to handle increases in network traffic. Slow VPN connections can make it difficult for remote workers to connect and receive critical security updates — if they even bother trying. Frustrations with VPNs can build, and employees may even put off connecting entirely.

In addition to difficulties with patching remote devices, organizations may find that maintaining on-premise patching solutions is a real pain point. IT staff must dedicate time and resources to the maintenance and configuration of an on-premise system, and there are many tasks which still may need to be done manually or with separate tools. For example, IT staff may need to configure and maintain WSUS as well as multiple other tools for patching alternative operating systems and thirdparty applications. Configuration and maintenance alone can become arduous and overly burdensome if there are too many tools needed to complete the same task.

Patching without the headache of servers and VPNs is possible with cloud-native patch management platforms. Cloud-based patching platforms do away with cumbersome servers and do not require routine maintenance. Updates in functionality can be implemented automatically without any user-end frustration and the cloud-native approach makes platforms like Automox easy to set-up and maintain. Automox can be installed on virtually any device, giving users the ability to ensure patches are deployed seamlessly across every endpoint on their network, no matter where those devices might be located.

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

Get More From Your WSUS Alternative

There are many important features found in newer patch management technologies that can help organizations achieve best practices. When looking at a WSUS alternative, organizations should consider the elements of patch management best practices. Patch management is a tenet of basic cyber hygiene, which means it's a critical part of overall cybersecurity. When considering a patch management platform, choosing a solution that is focused on patch management best practices is going to be your best bet.

Some elements of patch management best practices include: Inventorying all systems, endpoint visibility, automating patching, and generating routine reports.

With a modern patch management platform like Automox, users can create a living inventory of all systems and see what's happening in real-time. Along with full endpoint visibility, users can create their own policies and set their own automated patching schedules, as well as generate reports. As a cross-platform solution, Automox makes it easy for users to patch multiple operating systems and third-party applications, all from the same dashboard.

Modern patching platforms can help organizations increase their patching confidence, speed, and coverage. A patch management solution like Automox can help organizations minimize their attack surface, reduce their risk, and increase patching efficiency.

AUTOMOX		WSUS
Designed for diverse infrastructure		Designed for Windows
Patches Windows, macOS, and Linux without complication		Doesn't patch alternative OS
Generates reports		Requires configuration and maintenance
Updates third-party applications easily		Doesn't patch most third-party applications
Provides full endpoint visibility		No endpoint visibility
Patches remote devices seamlessly		Requires VPN for remote device patching

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

Choosing a WSUS Alternative for the Modern Workforce

When you're looking for tools to extend your WSUS patching, or wanting to evolve past WSUS entirely, be sure to choose a solution that checks all the boxes. Here's a high-level listing of what to consider when choosing a patching and endpoint hardening solution that meets the needs of your evolving workforce — today and in the future.

Remote workforce support without VPN

Today, more workers operate from remote locations than ever. WSUS can only ensure all those remote endpoints get patched when they connect to the corporate network via VPN.

Automox, on the other hand, patches automatically every time a device is connected to the Internet.

Cloud-native console

Leverage a SaaS solution to reduce your reliance on on-premises hardware and software, increasing your agility to manage patching from any device, anywhere.

Automox uses a single cloud console that offers full functionality to manage all your endpoints.

Native cross-platform support for the latest Windows, macOS, Linux, and popular third-party applications

Vulnerabilities also exist in non-Microsoft products. Yet WSUS does not provide simple, straightforward options for updating anything but Windows software.

Automox does, providing out-of-the-box support for other OS and third-party applications. Now, you can feel secure in your other business-critical products like Java, Adobe, Chrome, and more.

Multi-location support across geos from a single interface

Have full visibility of all your corporate endpoints from a single interface that manages multiple locations and remote workforces — with no additional requirements.

Automox's cloud-based solution reduces the complexity and cost to keep distributed workforces patched and protected.

Infrastructure-free architecture

Choose a cloud-based solution that doesn't require investing in expensive hardware or planning hours on routine server maintenance.

With Automox, no additional hardware is required. Commands are sent directly from the cloud to the supported endpoints with no need for an on-premise server.

Granular, cloud-based control

While providing the ability to create groups of devices to target for patching, the WSUS functionality can be quite limited.

An alternative solution should provide the ability to create more granular and controlled patch schedules, and assigning device groups to them should be intuitive.

Reliable, real-time reporting

With one glance at your Automox console, you can be certain your endpoints are up-to-date, and your inventories are accurate.

You can't say the same about your WSUS reporting, which is notorious for showing results that a manual scan will contradict.

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.

Contact SRC Cyber Solutions LLP
www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com