# Top Patch Management Software For Network Security

**TechRounder PDF Edition**

Live article: https://www.techrounder.com/software/top-patch-management-software-for-network-security/

By Vipin PG | Published June 17, 2021 | Updated January 4, 2026 | Format: Article | 5 min read

## In brief

Patch management is the process of applying patches to a computer system, such as a software patch or an update to the system BIOS, to fix or improve some aspect of the operation.

Patch management is the process of applying patches to a computer system, such as a software patch or an update to the system BIOS, to fix or improve some aspect of the operation.

Patch management can be seen as a way to reduce vulnerability risks by keeping computers up-to-date with current patches. It has been estimated that patching reduces risk exposure by 50%.

Patch management requires the user to install patches on their systems according to schedules specified by vendors. The installation of security updates and service packs is also included in this category.

Companies look for the tools to reduce the network admin's responsibility to update their existing software and applications to make sure known vulnerabilities are resolved.

## Patch Management Software For Network Security

To help you out we have covered top patch management software that you can consider while selecting the best patch management tool for your business.

## 1. Motadata ServiceOps Patch Manager

Beneficial: Small to large businesses

Motadata's patch manager helps organizations in maintaining desired visibility over the newly released Windows security updates and also helps in reducing bandwidth utilization. It makes sure that all the Microsoft Operating System and applications are up-to-date and has all the performance-related updates to improve overall security position. The platform handles all phases of Patch & Deployment Management spontaneously and proficiently.

### Features

- Auto Discovery of Endpoints from a Single Dashboard
- Manage Security Compliance
- Automated Package Deployment
- Automated Registry Deployment
- Automatically scan for missing & available patches for Windows
- Status monitoring of deployment
- Relay server for multi-location deployment
- Deployment policies for patches and packages
- Automatic patch testing, approval & deployment

- Patches & packages un-installation
- Remote deployment of both silent and non-silent packages
- Push Windows registry changes
- Batch deployment for internal bandwidth optimization
- Comprehensive reporting

Price: Get custom quotes as per request. It provides a 30-days free trial.

## 2. SolarWinds Patch Manager

Beneficial: Small to large enterprises

SolarWinds Patch Manager is the tool that does patching of Microsoft Servers, networked PCs, and 3rd-Party apps automatically. This tool simplifies patch management on servers and all desktop computers. It provides automated patching and reporting elements that help save a lot of time.

### Features

- Decreases the security risks and narrows the service interruptions.
- Ensures the applications of patches and controls what is going to get patched and when.
- Keep all the devices patched and secured
- Provides summary reports through patch status dashboard
- Offers pre-built/pre-tested packages
- Capable of handling vulnerability management

Price: You will get a completely operative free trial for 30 days. The platform price starts at $6440. Various licenses are available from $ 6440 to $ 150000.

Expert’s Tip: When you select the Patch Management Software make sure the Software is an automated solution and it should be able to identify the need for the latest patch updates.

## 3. ManageEngine Patch Manager Plus

Beneficial: Small to large businesses.

ManageEngine Patch Manager Plus is one of the best patching solutions. It offers automated patch deployment for Windows, Mac, and Linux. It also provides patching support for almost 650 third-party updates over 350 apps. You can deploy on-premise or in the cloud.

### Features

- Manage and deploy patches to more than 350 third-party applications.
- Provides the features for flexible deployment policies and insightful reports.
- Functionalities to test & approve patches, decline patches, and third-party applications patching.
- Makes patch compliance easy with advanced analytics and audits.
- Ability to track patching through patch management reports.
- Customizable deployment policies.

Price: Free trial is available. It offers Professional and Enterprise with On-premises and cloud options. The Paid plan starts at $34.5 per month for 50 PCs.

## 4. Syxsense Patch Management

Beneficial: Medium to large enterprises

Syxsense offers two types of service bundles for patch management - Syxsense Manage and Syxsense Secure.

### Features

This platform has a centralized remote endpoint management package that allows system administrators to access a cloud-based console to manage and monitor each added device. It also cures manual actions and automated processes. There are patching agents available for Windows, Mac, and Linux operating systems.

Price: It offers subscription-based plans and each account includes cloud storage. A 14-day trial is available for both Syxsense Manage and Syxsense Secure.

## 5. NinjaRMM

Beneficial: Small to Large Enterprises

NinjaRMM is a remote monitoring and management (RMM) platform that can be used in IT services. This platform has a collection of software that is particularly managed service providers (MSPs) use but it could also be used by IT departments that manage several remote sites.

The package of services in NinjaRMM includes a patch manager that watches Windows and MacOs plus other hardware drivers.

### Features

- Notes the versions of each OS and software package that indicates their patch statuses
- Watch out for the available patches from suppliers.
- Copies and stores the installation packs whenever the patch is available.
- Schedules patches for out-of-hours installation.
- Able to apply patches individually on demand.
- Automatically implement a system reboot whenever it is required.
- No need to install or maintain software as it is a cloud-based system.

Price: Custom pricing offered based on the need with a free trial option.

### Key Takeaways

Most commonly, companies use patch management for fixing issues with different versions of software. Patch management solutions can analyze the existing software and notify the absence of security features.

Whenever you are choosing any patch management software, you must check:

- Does it capable of maintaining a database of software, middleware, and hardware updates?
- Does it offer alerts of new updates or patch software automatically?
- Does it inform the administrator of endpoints and users about out-of-date software?

It is important to have the right platform to minimize the possibility of crashing the systems due to inactive software. The right patch management solution will help organizations in improving their software’s security and help them implement the right update at right time.

Patches will not only fix the bug but they can help organizations in having new functionality that can help them identify the software that has stopped bug fixing so that organizations can switch to new software.

Hopefully, the above-given list will guide you to choose the best patch management solution for your organization, and you will be able to get the most out of it.

## References


1. forbes.com - sites / forbestechcouncil - https://www.forbes.com/sites/forbestechcouncil/2021/05/24/why-live-patching-is-a-critical-part-of-vulnerability-management/
2. motadata.com - free-trial-patch-manager - https://www.motadata.com/free-trial-patch-manager/
3. solarwinds.com - patch-manager - https://www.solarwinds.com/patch-manager
4. manageengine.com - patch-management - https://www.manageengine.com/patch-management/
5. syxsense.com - https://www.syxsense.com/
6. ninjarmm.com - https://www.ninjarmm.com/