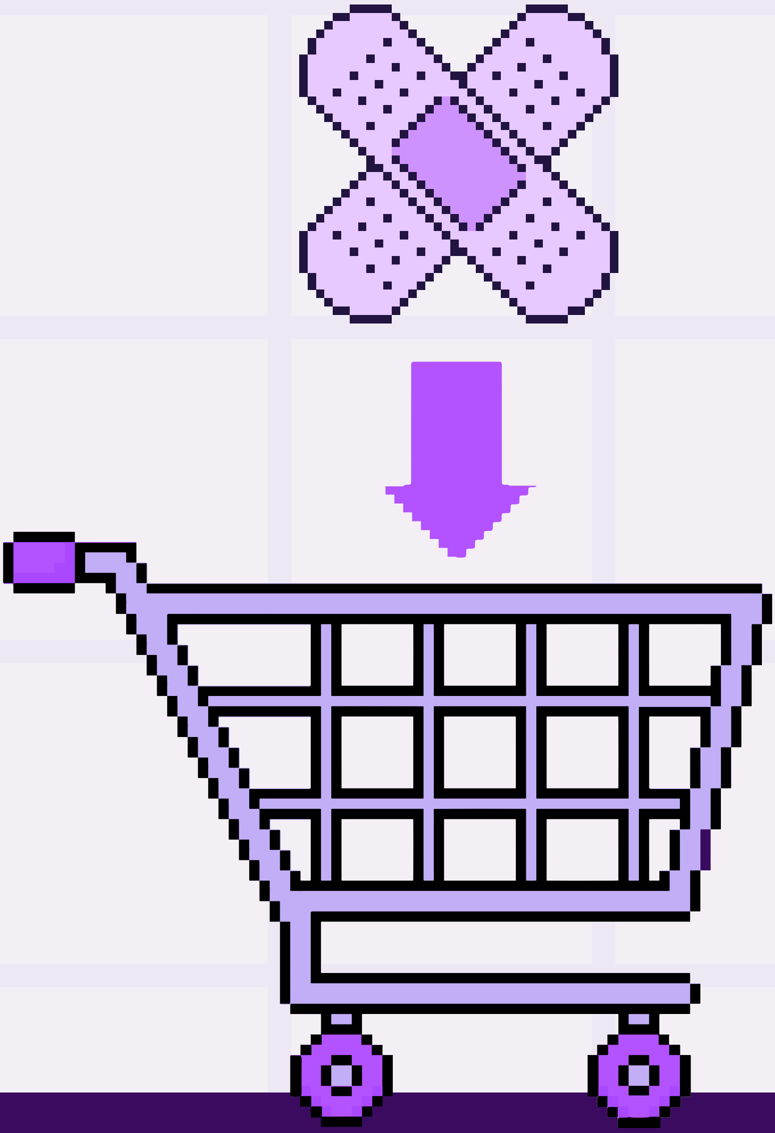
vicarius



Patch management solutions buyer's guide 2024

Recommendations for the best patch management solution is one of the most commonly discussed topics among IT & security communities.

While some tools have long been favorites, newer options are redefining industry standards. Ultimately, the best choice depends on specific use-cases, team skills, infrastructure, organizational culture, and budget.

In this guide, we'll review some of the most popular patch management solutions, examining their strengths, weaknesses, automation capabilities, and pricing to help you find the right fit for your needs.

We've analyzed tons of reddit threads, review sites, and spoken to customers directly to high.

Automox

STRENGTHS

- Cloud-native and agent-based, providing automation across all major OSes.
- Policy-driven automation for precise control over patch deployments.

WEAKNESS

- Many users feel that the reports are too basic and lack full visibility.
- Not cost-effective for very small businesses due to its pricing structure (more under pricing below)
- While Automox integrates with major OSes and has API access, some users need deeper integrations with their IT infrastructure.

Automation

While Automox integrates with major OSes and has API access, some users need deeper integrations with their IT infrastructure.

Pricing

Pricing structure is generally based on a per-endpoint, per-month model. It starts at $2 per month per device. More details here.

Best fit for

Medium to Large enterprises looking for strong automation in a cloud-native olution and those less concerned with in-depth reporting or extensive customization.

Gartner Peer Insights: 4.4/5

Capterra Score: 4.4/5

G2 Score: 4.4/5

PDQ Deploy

STRENGTHS

- Agentless deployment ideal for networks where installing agents is not feasible.
- Strong in environments predominantly running Windows, with batch and manual patch deployment options.
- Supports custom scripts in multiple languages (such as PowerShell, VBScript, and batch scripts), offering flexibility in how deployments are handled.

WEAKNESS

- Limited effectiveness in non-Windows environments.
- While PDQ Deploy is good for deploying software and updates, it does not have a built-in module for patch management.
- Agentless solutions like PDQ Deploy are easy for initial setup but quickly lead to higher operational costs due to their dependence on network configurations and administrative credentials.

Automation

PDQ Deploy primarily focuses on software deployment rather than comprehensive automated patch management. Its primary strength lies in manual control over scheduling and automating software deployments

Pricing

Free basic version; advanced features available in paid versions. The pricing for PDQ Deploy's paid versions is typically on an annual subscription basis per administrator. Starting at $1500 per admin per year. Details here.

Best fit for

Small to medium-sized businesses using Windows and preferring agentless patch management. It is well-suited for SMBs, educational institutions, and Managed Service Providers who need efficient software update solutions and do not require comprehensive lifecycle patch management.

Gartner Peer Insights: 4.4/5

Capterra Score: 4.8/5

G2 Score: 4.9/5

Microsoft Intune

STRENGTHS

- Agent-based solution that integrates deeply with the Microsoft ecosystem (like Azure Active Directory, Office 365, Microsoft Teams, etc).
- Supports both Windows and macOS, suitable for managing diverse device environments.
- Offers strong security policies and configurations to protect corporate data on mobile devices.

WEAKNESS

- Complexity in deployment, particularly in diverse environments that aren't heavily Microsoft-centric.
- Intune can be relatively expensive for smaller organizations or those that do not fully utilize the broad suite of features offered.
- Occasional delays and performance issues, particularly when managing a large number of devices or pushing updates

Automation

Intune supports automated patching, particularly within the Windows environment. It allows for the automation of update policies and the management of security patches across diverse devices.

Pricing

Microsoft Intune is priced on a per-user basis and included in Microsoft 365 subscriptions. The cost typically starts at $8.80 per user per month for the standalone version.

Best fit for

Larger organizations deeply embedded in the Microsoft ecosystem and needing comprehensive device management alongside patching.

Gartner Peer Insights: 4.6/5

Capterra Score: 4.6/5

G2 Score: 4.5/5

Action1

STRENGTHS

- Being entirely cloud-based, Action1 allows IT teams to manage and secure endpoints from anywhere, without the need for complex on-premises infrastructure.
- Easy to set up and effortlessly distribute the client software to remote endpoints.
- Offers strong security policies and configurations to protect corporate data on mobile devices.

WEAKNESS

- Action1 offers limited application coverage - some users complain about failure to support updates for some widely-used and crucial apps like Microsoft Office.
- Does not offer Mobile Device Management (MDM) capabilities.
- Outdated and non-intuitive UI.

Automation

Automates the detection, deployment, and installation of updates across Windows devices.

Pricing

Free for up to 100 endpoints; scalable for larger deployments. Request a price quote here.

Best fit for

Might be better suited for small businesses with distributed teams that primarily use Windows environments and have a straightforward software stack that does not include a broad range of third-party applications needing frequent updates.

Gartner Peer Insights: 4.8/5

Capterra Score: 4.9/5

G2 Score: 4.9/5

Tanium

STRENGTHS

- Agent-based with strong scalability and control, capable of managing tens of thousands of endpoints.
- Offers comprehensive visibility and control over complex networks, suitable for real-time and batch patching.
- Highly customizable, allowing organizations to tailor workflows and integrations to their specific needs.

WEAKNESS

- The complexity of the platform may require a significant investment in training and setup.
- Steep learning curve and may require significant time to become proficient in using the platform effectively.
- Generally considered expensive, particularly for smaller businesses.

Automation

Tanium automates endpoint discovery, patch management, compliance checks, and incident response.

Pricing

Custom pricing; detailed quote available upon request.

Best fit for

Very large enterprises or environments with extreme complexity and scalability needs. Orgs must have the capability to manage a complex, highly customizable platform. For small-mid sized organizations, the platform can be overwhelming and unnecessarily complex, leading to underutilization and inefficient use of resources.

Gartner Peer Insights: 4.8/5

Capterra Score: 4.3/5

G2 Score: 4.5/5

Vicarius vRx

STRENGTHS

- Consolidated solution for vulnerability scanning, prioritizing, and remediation.
- Focuses on proactive vulnerability remediation using an agent-based approach, offering Patchless Protection™ to secure systems before patches are available.
- Integrates well with various OSes and 3rd party apps.
- Easy to use interface and great customer support.

Automation

vRx uses automation to continuously discover vulnerabilities, prioritize them based on risk, and automate remediation actions. Its Patchless Protection™ applies compensating measures to high-risk apps until patches are available.

Pricing

Free trial is available. Paid plans start at $5 per month per asset.

Learn more about vRx Patch Management.

WEAKNESS

- As a newer product, limited integration capabilities with broader IT management ecosystems.

Best fit for

Organizations of any size looking for an innovative vulnerability management solution. vRx is a good fit for teams that want to take a proactive remediation-focused approach. It is not a good fit for organizations that are more focused on only running scans.

Gartner Peer Insights: 4.8/5

Capterra Score: 4.9/5

G2 Score: 5/5

ManageEngine Patch Manager Plus

STRENGTHS

- ManageEngine offers flexible deployment options for both on-premises and cloud-based.
- Extensive multi-OS support, including third-party applications, with capabilities for batch and automated patching.
- Offers strong security policies and configurations to protect corporate data on mobile devices.

WEAKNESS

- User interface and user experience is complex to navigate.
- Relies on scheduled scans to detect vulnerabilities, which can be time-consuming and leaves systems exposed to new threats between scans.
- Tiered pricing can force organizations to upgrade for essential features, leading to unexpected costs and complicating budget management.

Automation

ManageEngine Patch Manager Plus offers automated patch management across the lifecycle. It supports auto-approval of critical updates, scheduled deployments during off-hours, and features a test-and-deploy mechanism that ensures stability before widespread rollout.

Pricing

Depends on deployment type and number of devices. Free Edition of Patch Manager Plus supports up to 25 computers and 25 mobile devices. Typically begins at approximately $245 for 50 computers annually when deployed on-premises. Detailed pricing here.

Best fit for

Medium to large enterprises with complex IT needs that require both on-premises and cloud deployment options. It's better suited for technically skilled teams that can navigate its complexities effectively.

Gartner Peer Insights: 4.6/5

Capterra Score: 4.6/5

G2 Score: 4.4/5

I hope this guide helps you make the right choice for your business needs.

In addition to review sites like G2 and Capterra, I highly recommend searching reddit threads for more detailed feedback on your shortlisted tools. These forums helped my research and gave me more granular level insights. Some of these threads are in the source links below.

Good luck patchin'!