CONNECTWISE

The Essential Patch Management Checklist

Unpatched software is one of the most preventable causes of cybersecurity breaches, yet it remains a persistent threat across IT environments of all sizes. The risks of neglecting timely patching are significant.

The best patch management programs are consistent, repeatable, and proactive. Use this checklist to benchmark your current process, identify gaps, and drive continuous improvement across your patch management strategy.

☐ Create and maintain an IT asset inventory

Patch management begins with understanding the scope of what you're protecting. Take inventory of your IT environment, including all endpoints, operating systems, and applications.

☐ Establish a clear patch management policy

A patch management policy establishes a structured approach for identifying, evaluating, testing, and deploying software patches. When implemented effectively, it reduces security risks, resolves issues, enables new features, and maintains operational stability.

☐ Build a consistent patch schedule

Regular patch schedules help teams plan ahead and reduce disruption. Coordinate your schedule with vendor patch releases and schedule deployments around off-peak hours or maintenance windows.

☐ Automate patch management where possible

Manual patching is time-consuming and prone to human error. Automated patch management software allows you to:

- Schedule and deploy patches across multiple endpoints
- Enforce policies consistently
- Receive alerts on failures or delays
- Reduce the time between patch release and implementation

☐ Test patches before deployment in a test environment

Before deploying patches in production, test them in a sandbox environment that closely reflects real-world conditions. Testing reduces the risk of introducing bugs, compatibility issues, or performance degradation.

Patches that seem safe in theory can still conflict with custom configurations, legacy systems, or critical business apps.

☐ Prioritize patches based on risk

Not every patch has equal importance. Use a risk-based approach to decide which patches to address first. Smart prioritization keeps business-critical systems secure while managing time and resources efficiently.

Prioritization criteria might include:

- Severity of the vulnerability (CVSS scores, known exploits)
- Ideal downtime of affected systems
- Exposure level (e.g., internet-facing vs. internal-only)

Ensure timely patch deployment

Delaying patch deployment increases your exposure to exploits, especially for known vulnerabilities. Develop internal SLAs for:

- Testing turnaround times
- Deployment timeframes based on patch severity
- Emergency patch response targets

Timely patching also supports compliance with cybersecurity frameworks like NIST, ISO 27001, and HIPAA.

Monitor and audit the patch management process

Visibility is essential for ongoing improvement and regulatory compliance. Set up real-time monitoring and periodic audits to track:

- Which assets are fully patched
- Patch success and failure rates
- Coverage gaps and missed updates
- System performance and stability post-deployment
- Hardware or software that is outdated, unsupported, or non-compliant

Have a rollback and disaster recovery plan

Make a backup plan for when patching doesn't go as expected. Before applying patches, backup systems or create a system snapshot. This allows for a fast rollback to a stable state if a patch causes unexpected issues and will minimize downtime while preserving data integrity.

Perform post-patch analysis

The patching process doesn't end at deployment. Perform post-patch assessments to confirm success and identify areas for improvement.

Track key metrics such as:

- Patch success rates
- Time to remediation
- Outstanding vulnerabilities
- System stability post-update

This data helps refine future cycles and supports compliance reporting, audits, and SLA reviews.

Whether you manage dozens of clients or a single complex enterprise network, ConnectWise RMM™ provides the flexibility and reliability to stay ahead of vulnerabilities and maintain business continuity.

Ready to take the hassle out of patch management?

Check out our Patch Management Best Practices Guide or start a free trial of ConnectWise RMM today and discover how you can protect more, work smarter, and respond faster.