

# Steps to Implement Patch Management

## 1. Deploy Asset Management Tools

To make patch management work, first identify all devices and software requiring protection using asset management tools. Set up discovery software across your network, schedule daily scans during off-hours, and tag items based on their importance to prioritize patching.



## 2. Create Your Patch Policy

A strong patch policy eliminates guesswork and keeps your systems secure. This written document defines exactly how your organization handles updates—from emergency security fixes to routine feature upgrades.

## 3. Set Up Automated Scanning

Continuous monitoring forms the backbone of effective patch management. Manual checking doesn't scale and leaves you vulnerable to missed updates. Automated scanning tools detect missing patches and alert you to vulnerabilities, ensuring you're always up to date.



## 4. Establish Testing Protocols

Every patch needs testing before it touches your production systems. A dedicated test environment lets you catch problematic updates before they affect your business operations. Set up a small-scale replica of your network with samples of each system type you manage.

## 5. Implement Deployment Workflows

Your patching success depends on having a solid, repeatable process for every update. One missed step or badly timed deployment can bring your business to a halt. Build a workflow that handles both routine maintenance and emergency patches.



## 6. Monitor and Measure Results

Numbers tell the real story of your patch management success. Track your key metrics consistently. Watch your trends over time. Maybe you notice that critical patches take too long to roll out, or certain systems regularly miss updates. Use these insights to fine-tune your process.

