

Patch Management Process

1 INVENTORY

Make a list of the hardware and software assets (like servers, storage, operating systems, applications, virtual machines, and databases) in your system that will require patching.

2 MONITOR

Software vendors, cybersecurity companies, and patch management software can let you know when a patch is available for your software and hardware.

3 EVALUATE

When you get a notification that there's a new patch available, decide if it's worth rolling out on your systems. Is it a critical security update or just a minor UI tweak that can wait until later?

4 TEST

Try out worthwhile patches on a test server or a staging server before letting them near production, just in case it causes configuration drift or has a weird effect on dependencies

5 BACKUP

Make sure that you've backed up systems and data recently before rolling out a patch (especially one that applies to critical infrastructure).

6 SCHEDULE

Plan your patch deployment to cause the least disruption, like during planned maintenance windows or when system usage is low.

7 DEPLOY

You can roll out patches manually on a one-by-one basis, or use automated patch management to deploy them right when you want.

8 DOCUMENT

Verify the patch was rolled out to the correct systems by checking reports, logs, and validation testing.

9 COMMUNICATE

Let your stakeholders know when a patch is on the way as well as how it could impact their use of the software you're patching.