FIELD EFFECT™

5 tips for better software patch management

Vulnerable software presents security risks for businesses of any size, but staying ahead of critical updates and patches can be a complex, time-consuming challenge.

The fact is, effective patch management requires continual coordination of multiple elements. That's why we've provided a few steps to help you stay on track.

Here are five tips to help you improve your patch management process.

01

Identify: Understand the assets you need to protect.

A solid understanding of the assets that exist in your IT environment is the first step toward better patch management. Armed with a clear picture of your operating systems, applications, versions, owners, as well as the security measures you have in place — you can then define the software absolutely critical to your business and prioritize protection.

As workforces continue to evolve, adding more endpoints and applications to manage across multiple locations, maintaining an ongoing inventory of assets can help you keep up with software updates and patching requirements.

02

Prioritize: Know the threats to your critical assets and assign priority.

The reality is, the number of systems and applications that require maintenance updates or patches can be overwhelming for any IT team.

Set the right priorities and assign criticality levels by identifying the threats targeting your business-critical assets — and the risks to your business, if unpatched or updates are missed.

For example, which applications pose the most risk, in terms of customer impact or production downtime, if compromised? What are the consequences of delaying specific updates?

Technologies like threat monitoring tools can also help by quickly identifying vulnerable assets and mapping these to critical updates to prioritize remediation.

03

Verify: Validate the authenticity of your patches and updates.

Software updates and patches help businesses gain high performance, ensure uptime, and improve security. But without proper verification or testing after downloading these, you could put your configurations, settings, applications, and hardware at risk.

Always check the source and authenticity of updates and patches for legitimacy. Each should include a digital signature that shows the origin and identity of the software and validates its integrity.

Depending on your infrastructure, the updates you've prioritized, and the trust level with your software vendors, you can then determine whether to deploy or continuing test.

04

Apply: Turn on automatic updates.

Ensure automatic updates are always turned on and working — this is one smart way to lighten the manual work of updating and patching.

Tools like IT automation software, as well as threat monitoring platforms, can also streamline aspects of the patch management process. These may include capabilities for identifying vulnerable software and mapping these to critical patches, scanning for missing patches, ensuring auto updates are working properly, downloading newly-released patches, deploying based on your specific policies, and even reporting on the status of applied updates.

For example, Field Effect's Covalence platform provides continuous monitoring and detection of threats and vulnerabilities across your entire network and hybrid workforce — and delivers prioritized alerting that indicates the severity of vulnerabilities and the specific updates needed.

05

Document: Define your patch management process and policies.

Outlining the policies, procedures, and tools for patch management provides the ultimate blueprint for keeping systems up and running, ensuring business continuity, and reducing security risk.

Define the systems and software that demand the highest priority, and assign roles and responsibilities. Are specific tools needed to monitor, detect, and respond to vulnerabilities or automate your patching process?

Regular review and audit are also critical to measure your success — for example, measuring mean time to patch (MTTP) and leveraging products like Covalence.

Documenting this identifies potential issues, provides internal visibility for the function, and ensures the right resources and process.

Were these tips helpful?

Share it with partners or colleagues who may want to learn more about improving security for their business. If you have any questions about steps your organization can take to defend against cyber threats, our experts are here to help.

fieldeffect.com
letschat@fieldeffect.com

Canada and the US
+1 (800) 299-8986

United Kingdom
+44 (0) 800 086 9176

Australia
+61 1800 431418

FIELD EFFECT