

**Patch Management**

Updated September 2021

Version 2.0

**Contents**

[**Patch management** 3](#_Toc84321620)

[**Patching Processes** 3](#_Toc84321621)

[**Reasons for Patch Management** 3](#_Toc84321622)

[**Types of Patches** 4](#_Toc84321623)

[**1.** **Security Patches** 4](#_Toc84321624)

[**2.** **Bug-fixing Patches** 4](#_Toc84321625)

[**3.** **Performance and Feature Patches** 4](#_Toc84321626)

[**How to protect yourself** 4](#_Toc84321627)

[**Assessment of importance** 4](#_Toc84321628)

[**Automatic and Managed Updates** 5](#_Toc84321629)

[**Make Patching Easier** 5](#_Toc84321630)

# **Patch management**

Patch management is about keeping your devices and software on computers up to date. This reduces the likelihood of attacks due to vulnerabilities in your operating systems or applications. Prompt updating, (patching) is essential for effective cyber security in order to reduce the risk of a data breach.

# **Patching Processes**

A typical patch management system requires four main steps:

**Scanning** Checking devices or groups of devices for available patches

**Assessing** Analyse the scan results to determine available patches and their level of importance

**Deploying** Selecting the patches and applying the changes to the selected devices in a planned and scheduled way which minimises impacts to users

**Monitoring** Verifying that deployment is completed successfully

Patches often require downtime as systems may need to reboot to successfully apply the updates.

# **Reasons for Patch Management**

**Security** Patch Management fixes vulnerabilities on your software and applications that are susceptible to cyber attacks

**System uptime** Managing updates allows you maximise the likelihood that your systems will run smoothly, which means your system stays ‘up’ and running.

**Compliance** Data Protection legislation requires appropriate technical controls and patch management is a necessary part of compliance.

**Updated features** As well as bug fixes, vendors use patches to add features and functionality, allowing you to get the best from your systems and applications.

# **Types of Patches**

## **Security Patches**

Patch management is important due to the speed of change within the cyber sector. Hackers will search constantly for new ways to exploit vulnerabilities. Vendors use patches to protect newly discovered security issues which have been identified in between installation and the current timeframe.

## **Bug-fixing Patches**

Some patches fix application errors and bugs encountered by users of the application or system. This will significantly improve the user experience, make work more efficient and reduce the time IT support staff spend answering user support calls.

## **Performance and Feature Patches**

Software companies constantly invest in research and development to bring new applications to market, remain competitive, and keep improving their offering. Updates can improve the performance of your systems and add more features, making them a cheap way to keep adding functionality.

# **How to protect yourself**

The UK Government’s Cyber Essentials Scheme includes the requirement to keep software and hardware updated, and ensure it is licensed and supported by the vendor. Where the patch fixes a vulnerability and is classed as ‘critical’, it needs to be applied within fourteen days of release.

Successful Cyber Essentials certification includes free cyber insurance. Visit our Education Data Hub website: <https://educationdatahub.org.uk/cyber-essentials>

# **Assessment of importance**

Vendor vulnerability classifications will help you analyse the importance of the patch. It is recommended that full deployment takes place within the following timescales:

* Critical or High 14 days
* Medium 21 days
* Low 28 days

# **Automatic and Managed Updates**

Part of the problem of maintaining software patches is remembering to perform the updates.

In a perfect world you could install new patches the second they become available for all of your assets, but this would have a significant impact on users. Instead, have a strategic approach which fits around school processes and working hours to make updates security focused and convenient.

Where possible, set systems and devices to update automatically or deploy patch management software. It is essential that users allow updates to run and don’t keep postponing them.

To meet with Cyber Essentials requirements, schools need to implement a policy preventing the use of any end-of-life software or devices. This isn’t always possible from a budgetary perspective, but do ensure a rolling program of investment for devices. Implement compensating controls if possible, so the vulnerability is mitigated without being fully patched.

# **Make Patching Easier**

1. Maintain an up-to-date inventory of all your software and devices, with strong asset management and an awareness of the operating systems in use.
2. If possible, standardise systems and operating systems to the same versions to make patching faster.
3. Remove outdated devices from use and uninstall unnecessary software.
4. Keep track of your firewalls and antivirus products. Ensure you know who is monitoring the logs and how often.
5. Classify the risk to your systems, prioritising critical systems and software.
6. Roll out patches to small batches of assets to reduce the likelihood of issues and reassess assets to ensure patching was successful.