**Understanding Patch Management**

Patch management is the process by which the updated codes on various applications, hardware, and software are identified, acquired, tested, and deployed. This is done at scale because enterprise environments involve hundreds or even thousands of systems. If these attempts are made to be done manually even after having a big team, it would be impossible. Additionally, it also carries the risk of unintended errors. This is the reason why patch management is carried out via automation. They are used to fix any kind of bug, closing of security holes, and also add new features. The function of patch management is not only limited to securing the network and making it reliable and operational but is also essential for staying compliant with security and privacy regulations.

**What does Patch Management include?**

The process of patch management includes the following steps.

1)It is used for listing all the devices, operating systems, and apps.

2)To decide what software versions to standardize on.

3)It is needed to categorize patches based on risk and priority.

4) It is used to test patches in isolated environments.

5)It is used to run a pilot of patches on several samples.

6) It is used to validate patches and find out if there are any missing patches

.

7)It is used for planning and rolling out patches.

8)It is also used for documenting patches, vulnerabilities, results of the test, and also deployments.

**Advantages Of Using Patch Management**

Most software companies release patches regularly. To cite an example, Microsoft releases most patches on the second Tuesday of every month, which is commonly known as Patch Tuesday. Patches are released on a regular and consistent basis and this, in turn, is beneficial in mainly three ways. These are the following.

1)To mark and label the vulnerabilities concerning security issues as attackers and malware attackers know to look for unpatched systems.

2)To fix bugs and improve the overall stability and performance of the software.

3)To introduce new features. These new features are introduced to keep up with the rapid growth of the innovation in cloud-based software.

The increase in cyber-attacks in recent years as well as the growth in remote work makes patch management a very important and vital thing. There are different organizations out there that invest in a policy of patch management. These organizations that invest in a patch investment policy establish patch management which is a comprehensive process and use the appropriate software tools that will likely be successful in making their IT systems an overall improving one including the improvement in reliability, security, and current with the latest advent technology.

**Why do we need Patch Management?**

There are various uses of patch management. Patch Management is used by different organizations for different reasons. Some of them are as follows.

**1)Security reasons**

Patch Management is used to fix all sorts of software vulnerabilities that are prone to cyber-attacks. Thus, it benefits organizations to reduce risk concerning security issues.

**2) System Update**

Another task of Patch Management is to make sure that all the software and the applications run smoothly and are updated from time to time.

**3)Feature development**

In addition to bug fixing and security management, Patch Management is also used for updates of the functions and features. This patch management makes sure that the best, updated, and most reliable features are offered.

**4)No Monetary fine**

If any organization is not using patch management for some time, there is a risk of hitting some fines concerning money. Successful patch management makes sure that the organization complies.

**References**

1)<https://www.rapid7.com/fundamentals/patch-management/#:~:text=Security%3A%20Patch%20management%20fixes%20vulnerabilities,run%20smoothly%2C%20supporting%20system%20uptime>.

2)<https://www.techtarget.com/searchenterprisedesktop/definition/patch-management#:~:text=Patch%20management%20is%20the%20subset,security%20holes%20or%20add%20features>.

3)<https://www.manageengine.com/patch-management/what-is-patch-management.html>

4)<https://www.itarian.com/patch-management.php>

5)<https://www.gfi.com/patch-management>

6)<https://www.crowdstrike.com/cybersecurity-101/patch-management/>

7)<https://www.redhat.com/en/topics/management/what-patch-management-and-automation>