**The Benefits and Risks of Automated Patch Management**

As more employees are working remotely and IT structures have moved to the cloud, cyber-attacks have also become more sophisticated. Senior executives are concerned about data security and on the lookout for ways to improve the security posture of their organization. More than ever, patch management is now the key to reducing cyber threats. One of the best ways to cater to this is automated patch management. Not only does it reduce the burden of manually patching from time to time, it also helps patch multiple operating systems, third-party applications and provides detailed reporting. It also saves time, resources and finances while improving security.

Let’s have a look at some of the benefits of automated patch management and the risks associated with it.

# Security

It is the main reason why companies want an automated patch management solution. One of the reasons of releasing patch updates is fixing security vulnerabilities in a system that can otherwise be exploited by malicious people or software that intends to disrupt and damage your system.

By applying security patches on time, there is a high chance of preventing security breach from occurring, along with all other issues that arise as a result of a breach, such as data loss and theft, reputational damage, or legal penalty.

# Employee Productivity

A system with automated patch updates helps boost productivity within the workspace. Patches often introduce fixes to vulnerabilities in previous version or improve a program’s performance. Manual patching can be hard and troublesome for some employees. When they don’t have to worry about such issues, it not only saves them time but also improves productivity.

Moreover, in many data breach incidents, it’s not only the sensitive stolen data that results in losses. Many times, it is the downtime after a breach incident that adversely affects productivity at workplace. This effect can be a system that slows down due to malware activity, a congested network, a breakdown of applications critical to the business, or completely compromised systems that need to be reinstalled.

# Productivity of IT Department

Productivity in terms of IT department as a result of automated patch management can be measured easily. If we calculate the number of people and time required to manually patch the systems, and then compare it with the time and resources saved by using automated system, we can measure the benefit in terms of productivity. For companies with larger networks of more than 25 to 30 computers, the time and resources required for patching are so high that many companies either don’t do it or perform patching only on limited critical systems.

# Compliance

Organizations belonging to different industries are now obligated by different security standards to comply with their regulations. More regulations and laws now impose best practices on companies and having fully patched systems is one of the requirements of all security frameworks.

Particularly for industries such as financial, healthcare, and government, these regulations are now almost mandatory to comply with. Some of these standards include Health Insurance Portability and Accountability Act (HIPAA) for healthcare, Payment Card Industry Data Security Standard (PCI DSS) for financial sector and [payment card](http://www.cardzgroup.com/ContactLessSmartCard.html) companies, ISO 27001, General Data Production Regulation (GDPR), and Family Educational Right and Privacy Act (FEBRA), etc. in general.

Failing to comply with these can result in legal consequences, financial penalties, losing opportunities or even losing the business.

# Staying Updated with New Features

Patches not only enhance security, they also provide extended functionality with new features and support for other platforms. For organizations, this means that they can find new opportunities and improve their services.

# The Associated Risks

With these and many other benefits of automated patch management, there is no question that it is a recommended practice for organizations that prioritize security. However, one must consider and be aware of the associated risks and handle them appropriately.

Where automated patch management can improve the security posture of an organization, it can increase its operational risk at the same time. For instance, for a critical application that cannot stand even a minute of downtime due to its revenue loss repercussions, using automated patch management is not advisable.

The risks also depend upon the type of infrastructure being used. If an organization is manually deploying and managing its infrastructure, it’s not reasonable to use automated patch management. In other words, this means that automated patch management is preferable if your entire process of software deployment and management is automated.

Furthermore, if an application is outdated or brittle, automating its patch management is again not a good idea. The more advanced and updated your application is – particularly native to cloud infrastructure – the easier ways you can find to automate your patch management. This will ensure that its repeatable, feasible and less risky.