Patch Management as a Service

Are your systems and applications always secure and stable?

The technological evolution comes with its own set of challenges: new vulnerabilities around security, need of availability around the clock, demand for prevention of unwanted entry. As a service provider, you are asked to deliver security and visibility with continuous control of networking and IT environments. Every minute, every hour, every day; 365 days a year… irrespective of the size of your business and your in-house IT resources.

Patching

Let's take a closer look at patch management, for example. Not the hottest IT topic of today. In fact, it may even be boring and absolutely uninteresting for non-technical IT users, which probably most of your end users are. However, if you want to guarantee them availability of secure and stable services at all times, patch management can't be ignored.

Business benefits

How does patch management benefit your business?

From a technical perspective, managed patch management basically stops a high amount of risk and avoids disruptions and down-time for end users. It also avoids extra corrective costs. Because we define a whole patch and update schedule with you, you are sure that your systems, software and devices are kept up-to-date and secure. Your IT becomes more preventative, making sure that everything is secure.

From a business point of view, patch management helps protect your company brand. Unpatched environments are very well known to be the easiest and first target for hackers to access networks. If something as bad as this happens, the brand is ruined. Public opinion will be that your business is not up-to-date and is not following the correct procedures. Reliability is at stake, customers can turn to the competition and the company's brand and reputation are undermined.

Vulnerability risks due to delayed patch management

But does patch management have top priority in your company? You have a fixed number of IT staff, with lots of other work in progress and limited time. Patching costs your technical staff valuable time and money, which you prefer to spend on other IT work. And besides, how knowledgeable and up-to-date are they with patch management and updates, when they only work on it occasionally? Lack of time, limited experience and budgetary considerations are, in a nutshell, the most common reasons why service providers often unintentionally postpone patching and run vulnerability risks, which can easily be avoided.

Gain security, compliance, reliability and compatibility

Patching takes valuable time and money

Many service providers do not have sufficient or sufficiently skilled IT engineers to perform patching in a scheduled manner. Sometimes, it is also a matter of budgeting, because it can be quite expensive to have your staff perform patch management instead of doing other IT work or have them work overtime. Patching is a repetitive and, therefore, time consuming process for the IT department. A managed service solution can be a valuable alternative and result in fewer invoiced hours and a smaller overall IT support bill.

Patching – Gains

Gain security, compliance, reliability and compatibility

Patches are developed for a reason. Installed timely and correctly, they protect systems against hacking attempts, cybercrime and privacy risks. Is your organisation working with the information security standard ISO 27001? Then you know that patch management and updates according to a set schedule is an important issue for compliance. And if that is not enough, your services will also benefit greatly from improved reliability and compatibility when patches and updates are followed-up and installed in a timely and accurate way.

Professional patch management means: security

Patches are developed for a reason. Ignoring to install them makes systems vulnerable to hacking attempts, cybercrime and privacy risks. Would you want to run the risk of losing crucial data or experiencing an embarrassing security breach, due to unpatched vulnerability? Failing to patch has a huge impact on security issues creating vulnerability and unprotected entries into networks or devices. Patching keeps your systems, applications and devices - and therefore those of your end users - up-to-date, ensuring that no vulnerability to exploits is available on your network.

Professional patch management means: compliance

Patching is important for compliance, e.g. for organisations working with the information security standard ISO 27001. The standard has requirements around patch management and updates according to a set schedule in place and a process of managing that. Patching helps your organisation keep your information assets secure in accordance with ISO 27001 standards and be compliant at all times.

Professional patch management means: reliability

Within IT, changes can happen at lightning speed. Features that work fine today can suddenly no longer work tomorrow. If you want to keep your systems and services up and running reliably and avoid degrading performance for your end users, you have to be on top of those changes. One of the remedies is to make sure patches and updates are installed regularly, timely and correctly.

Professional patch management means: compatibility

One of your top priorities as a service provider is to ensure compatibility between different applications and operating systems. This way you guarantee continuity for your end users. If a vendor upgrades to another software version or changes operating functions, you must know the impact on all devices, applications, and operating systems that are connected to ensure compatibility. Are your infrastructure or applications not up-to-date? Then compatibility problems quickly arise. Professional patch management as a managed service solution helps you avoid compatibility issues.

IMS Patch Management by Insight

Insight manages and deploys patches and updates across the on-premises infrastructure, infrastructure in the cloud, applications and end user devices, and provides detailed reporting on this. Insight eliminates all the management for service providers, including managing all the tools and the deployment and packaging of those updates. You do your business, we make sure you can.

Why Insight?

When your servers need patching, you do not want to bother your end users. Instead of having your own IT staff work beyond business hours or even at night, let Insight schedule patch management for you.

1. IMS brings specialist knowledge and a full century of industry experience, hardly achieved by any individual business.
2. 24/7/365 monitoring services, multi-lingual service desk, serving all over the world.
3. Worldwide coverage: we work in any location where you need patch management.
4. Customised services to suit the needs relevant to your business.
5. Pre-pilot, pilot and full patch to guarantee uninterrupted service and consistent performance.
6. High standard, pre-planned schedules, planned with you.

According to the expert...

"Our partners find it a great advantage that we can perform patch management 24/7 and have the expert knowledge and experience. For some we take over patching completely, for example for smaller companies. For others we are the 'extra hands and brains', such as for medium-sized to larger companies. If a partner has a certain maintenance window, then we always have the team available to work within this timeframe. All our partners have to do is let us know their needs, requirements and wishes and we do the work for them."

Al Calamita, IMS Consultant with Insight's Hybrid Cloud team

For more information please contact your Insight Account Manager.