

IT Security

IT Security

Do you Need to Back Up and Protect Data and Files?

Data is an asset. It must not be damaged, lost or end up in the wrong hands. There are many potential threats, from carelessness and malware through to industrial espionage and data theft. And there are many ways of accessing data too. It is stored on various media, transferred through the network, carried around on laptops or memory sticks. You need to be in control of your data again and able to determine who can do what with it. You need to protect your data from all kinds of threats ...

Tailoring Security to your Needs

The Problem

A company's documents, files and data are usually located on servers and local computers, stored on backup tapes and carried around on laptops or memory sticks. Often, it is hard to know how many copies there are of an important document on the company's computers and which data has been worked on on private computers over the weekend. Your problem is that you can no longer guarantee data security. This also concerns threats from viruses, Trojans and spyware. Without an integrated concept, even your firewall and virus scanner are not much use.

The Solution

To ensure data security, you need firstly a plan and secondly effective interaction between all the tools employed. Decide which data and files need to be protected and which employees are permitted to perform which actions with them. Then decide which tools can be used to ideally put your concept into practice. With baramundi Management Suite, this could be as follows:



- baramundi Managed Software: Updates and patches of standard software in the form of ready-to-deploy software packages
- baramundi Patch Management: Destroying security gaps in Microsoft products
- baramundi Device Control: Backing up data flow in the network and offline
- baramundi Application Control: Controlling applications
- baramundi Disaster Recovery: Backing up and restoring data
- baramundi Personal Backup: Backing up personal settings and data

The Process

In the first step, you ensure that known security gaps are closed. For Microsoft operating systems and software, [baramundi Patch Management](#) does this automatically. As soon as Microsoft patches are released, they are automatically loaded onto all affected devices. You can use [baramundi Managed Software](#) to monitor the standard software of other manufacturers for new versions, updates, and security-related patches. You receive packets which have been security checked and optimally prepared for deployment.

In the second stage you take over control of the data flow. [baramundi Device Control](#) allows you to determine exactly which data can be accessed and how. Right down to the smallest detail: for example, you can restrict download volumes for individual computers or users, enable files for certain groups or individuals, prevent saving to memory sticks, and much more. It also works for laptops that are currently offline. Access to data can also be securely encrypted. This means that stolen hardware does not automatically result in access to your data.

IT Security

In the third step, you specify what which software is permitted to do in the network. For this, you can rely on [baramundi Application Control](#) and its white list concept. It will not allow unknown software to be run at all. New Trojans and spyware that are not yet known to your anti-virus software do not present a threat. Software cannot be used until the administrator or an authorized user allows it – and then only strictly within the rights assigned to it.

In the fourth step, you make provisions for an emergency. Hardware failure, vandalism, fire – there are many possible causes of corrupted data. With [baramundi Disaster Recovery](#), you back up all your valuable data and files on the network or on external data carriers. If you should lose data, you can then restore normal operation in just a few clicks of the mouse.

In the fifth step, you take care of your personal data and settings. A company's data backup usually leaves out personal settings. [baramundi Personal Backup](#) backs up your office settings and your personal settings as well. This means that any new computer is quickly and comprehensively personalized. Once you have set up [baramundi OS-Install](#) and [baramundi Deploy](#), you can run Personal Backup so that the settings from your old computer are immediately available again.

The Result

The modules of baramundi Management Suite put your security concept into practice and ensure:

- Clear rules that apply to everyone
- Secure data and files
- Controlled data flow in the network
- Protection against unknown applications
- Planned data backup and recovery
- Backups of personal settings and files

All settings and rules are controlled with baramundi Management Suite. Because all modules access the same database, you avoid losses due to interface problems and incompatibility. You are the master of your own data again.