PrintWatch

Data Leakage Prevention - Control, Evidence and Overview also on Printouts

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 Munich

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

info@itWatch.de
www.itWatch.info

PrintWatch

itWatch GmbH

– Data Leakage Prevention –
Control, Evidence and Overview also on Printouts

PrintWatch enables you, to control the information stored in your company on their way to the printer, before they reach the paper as a long term, uncontrollable "data store". Thus, **PrintWatch** closes one of the last gaps, where sensitive company information can leak.

PrintWatch

- Identifies print commands for sensitive documents, sets them apart from those for uncritical documents, thus contributing consistently to your Data Loss Prevention (DLP) strategy.
- Is able to permit or prohibit the printout for specific documents, users or groups according to the centrally defined security policy.
- The printout's content itself is brought in realtime in a future-proof, standardized intermediate format. Thus the content of the document, which is to be printed, is documented, and you can restore the exact printout at any moment. If needed, the intermediate format can be encrypted transferred into a long term archive.
    - PrintWatch identifies automatically identical printouts and doesn't transfer or centrally store them once again.
    - Even the slightest changes of the initial file are noticed, in which case the file is stored anew.
    - Due to the standardized intermediate format it is guaranteed, that there are no dependencies on the printer drivers, the printers or other infrastructure components, and the information can be restored anytime exactly without differencies on any other infrastructure.
- The report engine of the itWatch Security Suite enables you to search when, where, who, why and how many printouts of a certain document have been produced. You can achieve a complete over view due to the export control of the other modules of the **itWatch Security Suite**.

Threats:

- If not marked properly, printouts can be mingled with other papers and documents, so that for the security check it is hardly possible to estimate the criticality.
- Printers with security function are very expensive. Especially very sensitive information is not to be printed on every standard printer.
- A privacy incident without valid evidence leads to a general suspicion of all persons with a read permission and thus to trouble in the organization.

Challenges:

- A control commitee is permitted to view sensitive information but not to print it.
- By the standard means of the operating system you can assign, block or share printers, but you can't take the sensitivity of a document as criteria for deciding, who can print the information on which printer and in what manner.
- Only combining information like who, what, why, how many copies, on which printer, allows for the necessary granularity for critical information.

PrintWatch by itWatch is the Perfect Solution For SMB And Enterprise

With **PrintWatch** it's your own decision, which documents, on which printer, which user prints out and what additional information is archived and added to the printout. Thus you are always informed on who, when, why, which document with what content, how many copies, on which printer is printed out. The solution logs all this data for every printout and stores it audit-proof. Besides, your company is compliant with the requirements for the long term archiving as well.

PrintWatch monitors all print processes, logging only those, which by file type and identifier in the header or by the user are classified as critical.

This way it is guaranteed, that all the information for a critical print command on local or network printers are always available, and can be searched for with the help of simple reports. No user has a modifying access to the data.

PrintWatch doesn't support all operating systems -- please check beforehand.