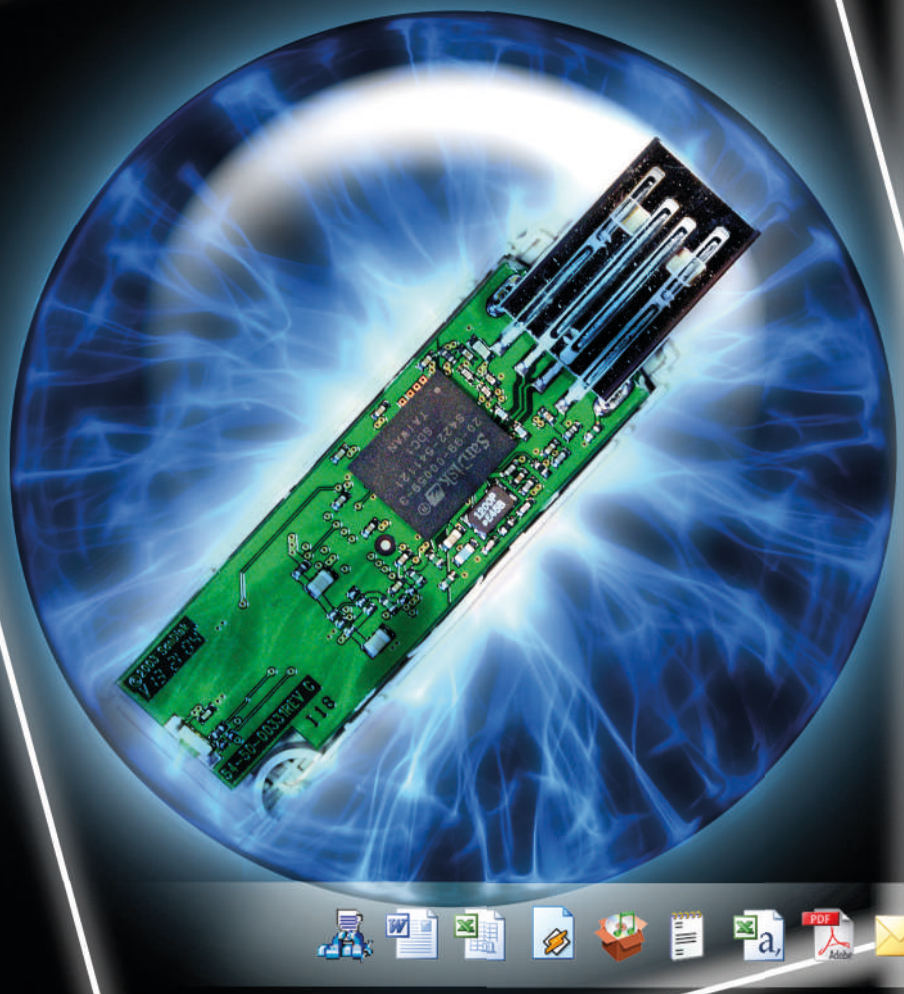
XRayWatch

...and you see EVERYTHING



itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 München

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

www.itWatch.info
info@itWatch.de

XRayWatch - Simply See EVERYTHING

Closing of Data Leaks

Do you know what data users exchange? With **XRayWatch** you protect company confidential information against data theft and the company network against hostile or unauthorised data contents, i.e. embedded executables.

Proactive Protection against the Forbidden

Forbidden files, e.g. executables shall not intrude your net - neither in clear nor embedded in other objects (encrypted zip-archives)! With **XRayWatch** you define who or which application may access (read or write) which data where (in the network, on the local harddrive or on portable storage) on thin or fat clients.

Log the Permitted

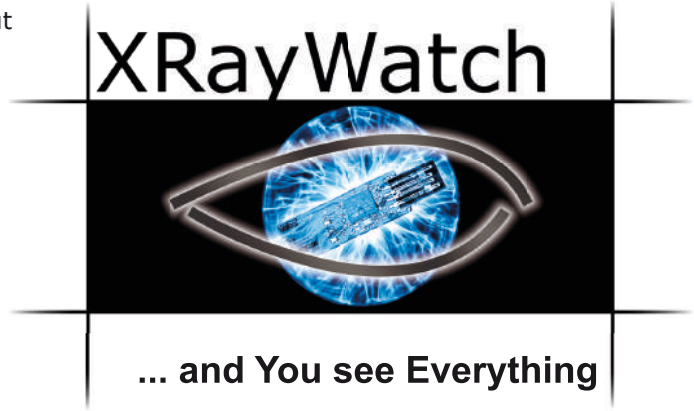
Users read and change information. Prohibitions constrain the day-to-day business. For sensitive information a conservation of evidence is important: Who patched the Login.exe of a board member work station with a Trojan Horse? Who read the contents of an ad-hoc message for the stock exchange before publication and took it along? **XRayWatch** quickly and efficiently helps you to answer these urging questions.

Secure Deleting/Erasing

XRayWatch enables you to securely delete files, folders and their meta-information from data storage devices, so that they will not be reconstructable any more, even with the use of forensic means.

XRayWatch controls the file access of all users according to central guidelines. The user and application rights are defined independently from each other, on network shares, local directories or portable devices, i.e. USB sticks, CD/DVDs, cameras etc. – a guideline can be defined in a few minutes. Because of the fact that the file names may be misleading, XRayWatch also enforces a detailed content control (pattern match) of all files and the detailed monitoring of all activities. Together with PDWatch the customer is able to define which data require encryption.

- Not only file names but also file contents are checked by pattern matching
- A general company guideline can be refined to any level based on White and Black List. Both White and Black Lists are supported for content and file names



- Who may read or write which files with what application on which location?
- Virtual data gates reduce costs

...and much more at www.itWatch.info

Secure execution for the rest

Local data-gate: Decryption and decompression in a local quarantine – then the context will be checked in clear format. Depending on the result, the data will be blocked and securely deleted, approved or forwarded to an execution within a secure central gateway.
Central data-gate: Identical to the ReCoBS-Definition of the German BSI (Federal Office for Information Security) the execution is being separated from the display. Contents are being controlled by **XRayWatch** in the Remote controlled System as well as on the user's PC according to central policy. This system prevents malware from invading the internal net and at the same time allows for usage of all active contents in a secure way.

Check Contents - Not File Names

Companies check the content and file names of exchanged data with their firewalls and mail-gateways. Why only there? **XRayWatch** offers the semantic and syntactic analysis of the contents of a file in any desired detail. Renaming of files is no threat. This check is adjustable by the customer. Plug-Ins allow for the integration of third-party-products – "Company confidential" is therefore technically enforced by the mandatory use of encryption with company keys.

Compliance

Data Protection Acts require special protection measures for the storing of personal data to portable media. With **XRayWatch** you identify individual-related data data, block its export or enforce an encryption e.g. with **PDWatch**.

Local Safe

With **XRayWatch** you control which data go in and out of the safe. The user can only access the data in the local safe with special trustworthy programs – the customer defines these programs. With **PDWatch** and **XRayWatch** you implement the most complex requirements in **Endpoint Security** and **Information Leakage Prevention**.

FSXRW-190417en