ApplicationWatch

You Define What's Running!

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

www.itWatch.info
info@itWatch.de

ApplicationWatch - Control and Protection for Applications

Do you still have a clear view?

Applications do not necessarily do what users or the company wants them to do. Malware has many characteristics, e.g.:

- Game software, that just costs time
- Software with parts of malware – e.g. a mail plug-ins or a modified DLL loading blind copies of each email to the internet
- Software conflicting with compliance goals, e.g. copy-programs violating co-pyright
- Resources used contrary to the compa-ny guideline, e.g. WebEx, Skype, 0900 Dialer, that cause high charges
- CD/DVD Burn programs that support potential data theft
- Attack software which automatically analyses and abuses weak spots within the company's network

Those are just some of the reasons why you should always know all about who uses what applications– and block the malware.

Central Real Time Monitoring

With its real-time monitoring, ApplicationWatch gives you an overview of all executed applications (also portable apps!) inclusive usage statistics on frequency and duration of use. Where and when has what application been started and termi-nated? The attempted start of prohibited applications can be found in the logs. Or just inform the head office of the new - still unknown - applications in real-time.

Data Loss Prevention (DLP)

Insecure applications must neither read any confidential contents nor modify executable files. Or they may only be started within an "unsecure data-gate". A browser may only load certain Plug-Ins from the internet and my not upload any sensible data to the internet. Active code, no matter where it comes from and how it is compressed, will automatically be run in an intentionally "un-safe area" without putting the productive environment at risk. Skype may only access its configuration data! Protect old appli-cations also from new attacks - Client Server or local - without having to adjust any code. Grant trustworthy applications – e.g. your CAD -programs – the access rights the user does not have and by this protect your data from unwanted leakage.

ApplicationWatch determines what programs in which situations will be available for the user, where they are run (virtualization) - and to which data these programs have access. ApplicationWatch prevents the usage of malware, spyware, malicious code and non-licensed software and logs critical accesses of the applications.

- Actual status of all exe-cuted applications including usage statistics allows for cost-efficient black-list-blocking alongside whi-te-list approach

... and you define what's running!

- Easy lock down of all malware
- No upload of sensitive data via browser or ftp, logging of sensitive email attache-ments.

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

Black- und White-List-Blocking

ApplicationWatch lets you choose between White List and Black List per computer and use scenario. In black-list-modus, the real-time monitoring even allows to react to all „new", still unknown applications at once and put them on the black list. Allow applications only according to specific situations, e.g. Sky-pe only in a hotel, or a self-approval for applications, then resul-ting in a complete monitoring or in the execution within a virtual environment – this allows for cost-efficient operation.

Protection of all work stations

The control of portable apps is also possible for CITRIX©, any thin or zero clients. The **Endpoint Security Suite** by **itWatch** protects you also from application plug-ins such as WebEx within the Internet Explorer and enforces together with **XRayWatch** its own scope of rights for each application.

FSAPW - 190417