

Endpoint Security made easy... ...Risk management from the beginning

Get to know risks and inventory fully automated and control them

You are aware that...

especially larger companies and organisations do realise the need for security **measures against security leakage points**. But what exactly are the most urgent actions against the most dangerous risks? And where to start? In the following **project outline** we would like to

illustrate how easy and fully automated you can collect real data from your PCs in production therewith becoming able to better evaluate **all actual existing risks** and **potential infringements of the currently existing instructions** as well as substantiate your possible need for internal actions and resources. Our products will accompany you through all project stages.

Stage	Expense ca. in pd	Reached goals, positive effects
"Collecting"	0,5 - 2	Complete inventory of all devices, applications, data files and of the associated potential risks
Defining security (for clearances) and systems management targets	1 - 2	Representation of the business culture and technical security on 100 % of the PCs possible
Soft Roll-Out	1 - 2	User acceptance – fine tuning of use cases without any administrative expenses; Security Awareness
Going Live during service	0,5	Compliance, audit guarantee, overview, efficient course of actions

Project stage „Collecting“ – Identify existing risks (as-is-analysis)

As-is-analysis of the following aspects – the **itWatch** standard policy, which is included on delivery, already covers most facets¹:

- ◉ Identification of
 - ◉ Devices and ports in use with details concerning e.g.
 - ◉ Time of usage
 - ◉ Size of data volumes (used capacity/ free capacity)
 - ◉ Serial numbers or other individual attributes of certain devices
 - ◉ Critical types of data files on exchange: *.exe, *.mp3, ...
 - ◉ Exchange between
 - ◉ Network shares and local PC
 - ◉ mobile volumes and local PC
 - ◉ Shadowing² of critical types of data files
 - ◉ File size and/or other individual attributes of certain files
 - ◉ Applications
 - ◉ Time of usage by users
 - ◉ Individual attributes of certain applications
 - ◉ Connected nets
 - ◉ Net connection time
 - ◉ Individual attributes of certain nets
- ◉ Benchmarking of departments and/or locations concerning criteria such as data export
- ◉ Client installations on the desired amount of PCs
- ◉ Administration stations, DEvCon Server, DCReport, DCView and data bases

The collected data materials will now be aligned with all existing guidelines and standing instructions. A final report of the results (also with audit report if necessary) will then present the analysis of data and the resulting risk evaluation.

¹ It is also possible that only variations of the already existing guide line or standing instruction will be collected. That will help to make the report significantly more clearly summarised.

² Shadowing is the complete logging of data contents.

Project stage 2: Defining goals for clearances and security and systems management

Keeping clearances while gaining more security:

IT-Security does not have to be complicated and need not necessarily hinder employees from working effectively. Also, additional work loads in helpdesk or in administration are nothing unavoidable. On the contrary: with **itWatch**, you can easily realise the concept of "*zero administration – full security*" (Ask us for more information on this matter). Some users still have to be able to execute certain actions in a special situation (such as on weekends), even though the action might not be in accordance with the general policy

No problem: The approval for the logging of all actions involved in the "violation" will automatically be accomplished via dialog in real-time. As soon as the user agrees to the central logging of his actions, the device(s) in question will be unlocked without any further administrative action, of course audit and compliance safe.

Security targets:

- User shall not import executable programs (*.exe, *.sys, *.dll ...) into the system – also not as embedded objects in Word documents.
- No executing of any portable applications, whether it is on the PC itself or in a terminal server session? Allowing exceptions such as the company-owned tariff calculator via U3 on white list?
- Temporary personnel, interns, trainees etc. shall transport any company data only encrypted on mobile volumes, so the risk of data leakage is avoided.

Systems management targets:

- With **itWatch**, the help desk is already notified of the device error, before the user can phone it in.
- Driver updates will only occur on demand.
- Virus scanner will be automatically executed on external media
- Logging only where necessary, no net killer applications through shadowing
- Personalised data volumes
- PDA's with user assignment/classification and fully automated secure synchronisation
- Updating of the inventory on any third party product

More targets you find in our white paper "USB-Sicherheit" unter www.itWatch.de/USB_Sich.pdf

Project stage 3 – Soft Roll-Out

Soft Roll-Out:

Many administrators fear the day the stricter security policy will come into effect - and cut off some of the former "privileges". In case a "VIP"-user loses certain authorisations, then at least one phone call to the admin seems to be unavoidable. With the products of **itWatch**, you already start communicating with the user

during the soft roll-out in the desired level of detail on how the future company policy will affect the user. So the communication (possibly about how to maintain the right) takes place, when the prospective forbidden action takes place. The transition period can be defined by time and/or number of "free" actions by user group.

Project stage 4 – Going Live

Going Live:

The Policy that until now only „reported“ or delivered data about the type and extent of transactions, will now go live. Changes on the policy will of course always be logged audit safe.

Interested? Then contact us now

Info@itWatch.de for product inquiries,
PR@itWatch.de for press inquiries,

By phone +49 (0) 89 / 620 30 100
Or **visit us:** www.itwatch.info

itWatch GmbH
Stresemannstraße 36
D-81547 Munich

itWatch – Security that thinks ahead!