

## Device Control with DeviceWatch

### Real-time Security Awareness

Companies avoid enforcing too hard security policies. Develop your security culture in your company and keep your employees informed using centrally organized measures instead of simply restricting users. **itWatch** products enable a “soft” start providing an on-demand training how to use the critical technologies securely before or while using and *during the session*. It is specifically important to find agreeable solutions concerning restrictions and special rights of VIPs in your company. A “soft” start is recommended here as well as clarifying questions concerning liability and arising risks in real-time.

### Personalising of Mobile Data Storage

Mobile storage devices may be personalized for users and/or groups. User rights may be granted on personalized storage devices only. No serial number is necessary.

### Offline Approval

Granting of security critical actions to users will be done on algorithmic checks – One time pass, challenge response, token, etc. may be required

### Friendly Net

The customer can apply automatic recognition of „friendly networks“ hooking in any algorithmic routines. Consequently Friendly Network connections will be recognised in real-time and others - as a result - will be terminated.

### Sometimes Security is a Moving Target

Your company is flexible - so is our security policy aligning in real time to your needs - reflecting the situation of your IT-infrastructure. Subjects such as obligation to approval, knowledge level of the employee, proof of relevance to project for critical actions - all of this and more will automatically be reflected in real time with central policies on the point of usage.

### Event-driven Change of Policy...

...will enable the setting of any policy in real-time based on customer-defined events such as e.g. “attempt to activate Bluetooth interface”.

## Encryption and Data Leakage Prevention with PDWatch

### Company Key – and all Data stay within your Firm

In addition to encryption with personal keys for all or some specified files the usage of company keys may be enforced on a user and group oriented level based on file names and /or their contents. Company key usage is limited to the companies PCs. Data loss and circulation outside of the company is therefore effectively prevented. A firm may centrally administer as many company keys as necessary, e.g. for sites, departments or projects, and manage groups of PCs using them.

### Compliance – Using content-sensitive Encryption

Data Protection Acts require special protection of personal data like social ID numbers or customer data when stored on portable media. Mandatory encryption by **itWatch** fulfils those requirements. File name, the user, devices used, the location of storage and content determine the classification. Automated processes manage the required logging and the approval of the users in real time. Trivial data will be transported unencrypted. The privileged user will continue to hold all rights, but the liability transfer can be logged.

---

## XRayWatch

---

### Embedded Objects – consistent Scanning

The pattern matching of **XRayWatch** does not just check the data header but the whole data file guaranteeing a consistent scan for all kinds of possible data leakage. Thereby, embedded executables or other forbidden file types embedded in a word-document or masqueraded as any other file type – abusing it as a “transport container” - will be discovered and blocked. This being a Unique Selling Point (USP), **itWatch**'s pattern matching stands out against the competing products in the market.

---

## DEvCon

---

### Information to the Point of Need

With the cascading architecture of **DEvCon**, you can forward any necessary information to the point of need in real-time, e.g. all active WLANs to the network admin, new processes /devices /applications /networks to the inventory database, plug & play errors to the help desk, security threats to the security officer. For all logged events you can decide if you wish to transfer those from the client to a central service and there you decide if just show them in your real-time viewer, forward them to another central service or a third party product or write them in any data base of your choice. Forwarding means, you may provide all desired information to other **DEvCon** instances or third party products (such as Tivoli, IDS, Patrol, etc.).

---

## New Module – ApplicationWatch

---

### Discover a cost-efficient Application Control eventually

**ApplicationWatch** enforces your security policy “what programs will be locally available” for all computers in your network. **ApplicationWatch** prevents the usage of malware or non-licensed software and protocols attempted access from unauthorized personal. The administration will be done centrally using security policies as usual in **itWatch** products.

While other products on the market just offer White List administration, **itWatch** will let you choose between Black and White List. Mixed installations are perfectly fitting the needs of the market since the enforcement of Black List definitions on dynamic computers allows a quick and cost-efficient administration of the application control.

---

## Contact Us

---

### Find out in detail about our innovations and contact us at

Email: [Info@itWatch.de](mailto:Info@itWatch.de)  
Phone: +49 (0) 89 / 620 30 100  
Fax: +49 (0) 89 / 693 92 804  
or  
Visit us: [www.itWatch.info](http://www.itWatch.info)

**itWatch GmbH**  
Stresemannstraße 36  
D-81547 Munich