DeviceWatch

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

DeviceWatch@itWatch.de
www.itWatch.info

DeviceWatch – Cost-efficient and Secure Use of Devices

The Security Threat

Any devices connected to a PC, i.e. via USB, PCMCIA, Bluetooth, Firewire etc., immediately start to communicate - whether desired or not. Comfortable plug & play mechanisms in Microsoft Windows 2000, XP; Vista or W7 do not provide central administration mechanisms. Therefore, security threats occur. However, removable storage devices are not the biggest risk. Passwords that are exchanged via wireless keyboards - without knowledge of the network department - or insecurely configured wireless networks are even more critical.

The Solution

DeviceWatch enables the central management of all interfaces and devices according to the PC and user group or user. Just to set devices „on“ or „off“ does not meet today's market requirements. Therefore, many further criteria can be taken into account such as time, system condition, active network connections or active processes for real time decisions. Of course, single functions of multifunctional devices (e.g. modems and memory of smartphones) can also be authorised individually.

Personalising of Storage Devices

Mobile storage devices can be personalised for users and/or groups and, consequently, user rights may be granted on personalised storage devices only. No serial number is necessary. By these means low cost storage devices turn into high class, secure transport media.

Off-Line Approval

Granting the rights for security critical actions to users can be done on algorithmic checks – one time passwords, challenge response, token, 4-eye-principle, self-approval for VIPs. etc.

DeviceWatch enforces your company guideline: “Who may use which device and/or port under what circumstances?“ in a cost-efficient and secure way. As our customer, you decide with your IT security policy which technologies and which user groups should be administered via a Black or White List - as a result, your operating costs are lower - the complexity of the policy exactly meets your requirements.

- Block devices when they are not registered
- Self-approval for VIPs - combined with an electronic contract and proof of evidence

... and You pull the Strings

- Event driven device activation /deactivation in real-time

… and much more at www.itWatch.info

Compliance

The company may be held liable for the use of illegal DVD copying hard- and software or TV cards where the charges have not been paid. **DeviceWatch** provides a cost-efficient overview and usage control and therefore creates provable compliance.

Real-time Security Awareness

Companies tend to avoid the immediate enforcement of hard security policies. **itWatch** products enable a “soft” start providing an on-demand training how to use the critical technologies securely before or while using. It is specifically important to find agreeable solutions concerning restrictions and special rights of VIPs – e.g. using self-approval combined with the obligation of logging, thus clarifying the issues of liability in real-time – without administration.

Friendly Net Profiling

With automatic recognition of “friendly networks“ in real-time, hooking in any algorithmic routines as plug-ins, e.g. the VPN status, you can decide whether the detected network connection - as a result - will be terminated and which security policy is valid in this network.

Cutting Costs

Often, expensive specialised hardware only differs in a few functions from more common products, i.e. in serial numbers, user authentication or automated encryption of memory sticks. DeviceWatch adds high-end functionality to cost-efficient devices (Mandatory Auto-encryption, Personal Storage media …).

FSDW-110212en