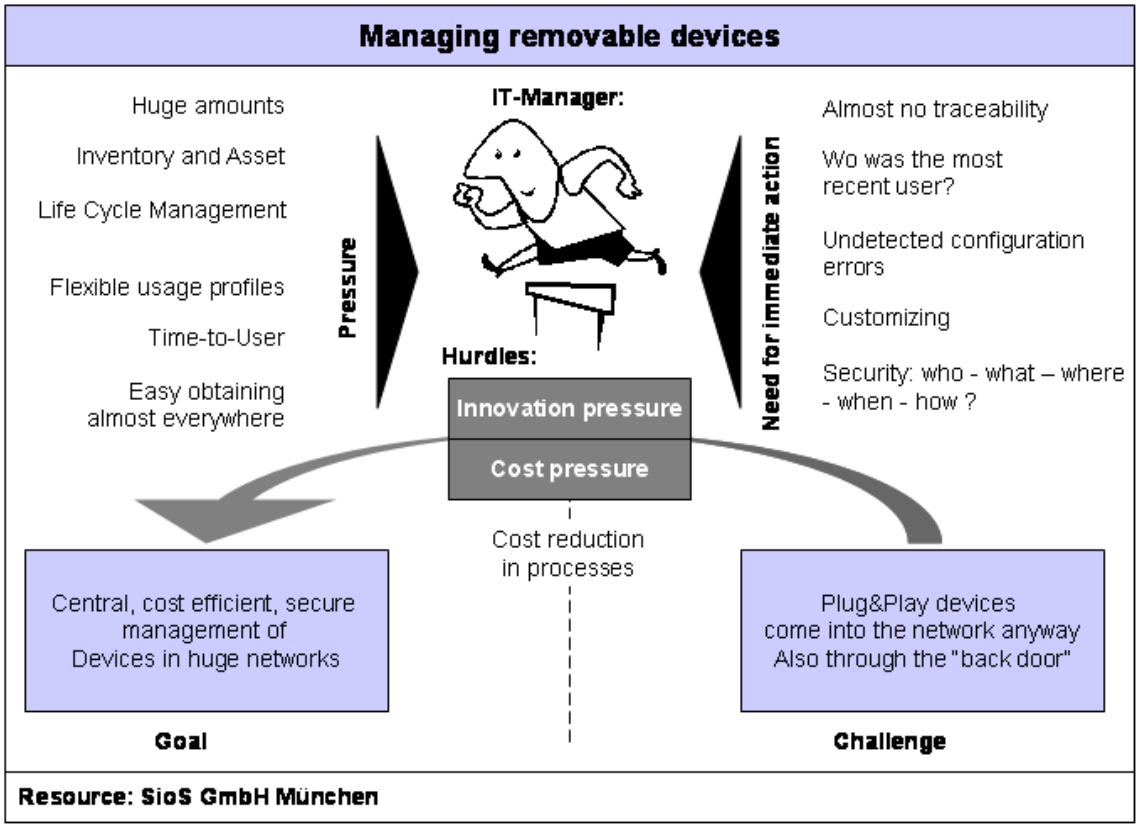
A NEW CHALLENGE FOR IT-MANAGEMENT

With a growing number of interfaces in todays clients (USB, PCMCIA, Infrared, Bluetooth, Firewire, WLAN ...) the multitude of peripheral devices and the spectrum of usage in the value adding processes of the enterprise grows as well. The IT-Department thus faces complex challenges in managing these peripheral devices.



Secure Deployment – Central Control of all Devices

Along with the utilization of removable devices **security** threats arise, so that usability and security are incompatible at first and have to be joint together with the use of an appropriate centrally managed tool. Once the secure and controlled use of removable devices is achieved, the complete **inventory** of all devices and of course some of their usage statistics (Who, where, when, how etc.) are required - a need, which is hardly reflected in detail by any of the classic inventory tools. Integration into **systems-management** is another requirement to Device Management: Device-specific events have to be integrated in „realtime“ into environments like Tivoli or OpenView, Plug-and-Play Errors must be sent to the central Help Desk, missing device-drivers have to be installed „on demand“, just to mention a couple of requirements in that context. In additon to the technical challenges there is a strong need to integrate the Device Management into already existing business-processes like: purchasing and validation of hardware, granting of access, Life Cycle Management of Security Policies or auditing.

SOLUTIONS

Security

DeviceWatch allows the centrally controlled secure deployment of all devices in a network. It allows to efficiently manage all interfaces USB, Infrared, PCMCIA, SCSI, Bluetooth, Firewire etc., all device classes like mass storage, cellular phones, smart card reader/writer, PDA, network communication devices, modem, printer, mouse etc. It enforces the centrally defined security policy for using or blocking of devices, even functions of devices, device-classes or interfaces. Any decision may be made on user or user-group basis network-wide or on defined PCs.

Centrally managed **Content Filter** protects your company network against the importing of forbidden data and protects the companies information assets from being exported to foreign environment. It allows an in depth analysis of the file contents in realtime.

Encryption with **PDWatch** allows you to implement your requirements to the confidentiality of company-owned-information with a centrally managed Security Policy. The encryption may be enforced mandatory or on a user decision on the basis of the type of media a user wants to store the information on.

Content Filter and Encryption help you to control the flow of information at the network-border on all PCs according to the existing company policy.

CDWatch gives you the opportunity to allow complete or restricted use of centrally authenticated media (CDs or DVDs). Centrally managed policies enforce the execution of company-specific profiles like installation-skripts. Time-frames for the usage are centrally organized and decentrally controlled.

Secure Deployment – Central Control of all Devices

Systems Management

DeviceWatch DEvCon processes your requirements for the deployment of removable devices. All requests related to the network-wide use of modern removable devices from the perspective of systems management are being served - easy to use - from the central Console.

Process Integration

All technical functionality wouldn't be of much use without the integration in already established processes. Therefore

- **Acquisition** processes like
  - **Application**,
  - **Approval**,
  - **Inventory,**
- **Gaining of statistical data concerning usage and possible optimization,**
- **Auditing** and
- **Life Cycle Management**

of both security and inventory are integrated and may interface to Management Frameworks like IBMs Tivoli, HPs Open View and many more.

An itWatch GmbH Product