

ReCApps

Remote Controlled Application System



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.de
info@itWatch.de

The thread potential

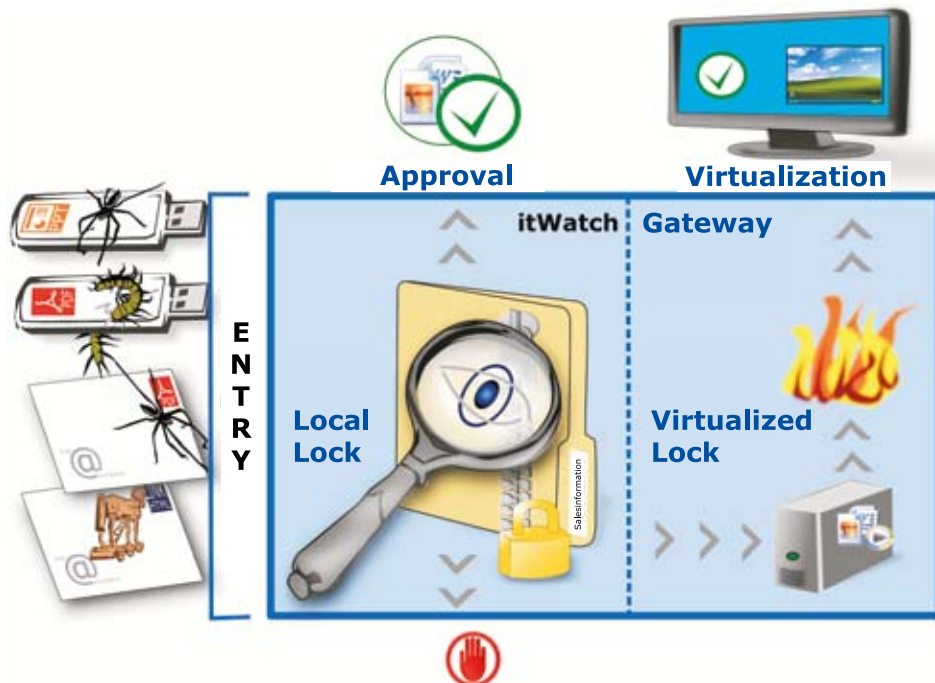
- By clicking the link in a „friend's“ email a worm, Trojan or any other malware is being installed.
- USB stick's or CD's that were handed over during an Event may contain Spyware to collect your data and upload it encrypted via http-s into the internet.
- Your communication partner passes you sensible data encrypted on an USB stick. How can you make sure, that the data does not contain risky macros?
- Hacked web pages of respectable companies distribute malware i.e. BBC (TecChannel 17.02.2011)

The challenges

- Blocking of external storage devices or of certain web pages prevent reasonable business processes.
- Content filters at gateway's or on firewall's are only effective regarding data in clear text - for the reason of data privacy protection often the ssl encryption of the traffic must noch be broken.
- It is not reasonable to simply forbid web pages with active contents.
- The recovery and cleaning of contaminated systems cost time, resources and money.
- Sensitive Information is being published at Wikileaks or fall into your competitors hands.
- Encrypted and zipped files and archives have to be checked in clear text.
- Interdictions put a stop to content and productivity.

1. The integrated lokal lock:

Decryption and recursive decompression of files are realized in a local quarantine. There the contents are checked in clear text. Depending on the result and according to centrally defined guidelines single filters are either blocked, safely deleted or passed over to a third party for further investigation. User access during inspection will be technically prevented. Therefore the computer may not be infiltrated by malicious code. Additional Hardware and prolonged walks are not necessary anymore.



2. The virtualized lock:

From the users point of view truly efficient work environments demand the possibility to execute critical actions immediately. Critical actions could be the very simple clickon a problematic URL, downloading executables from the Internet or installing nameless Applications from an unknown data storage device. For secure operation of browsers the BSI (German Federal Office of Information Security) presented ReCoBs, a concept which allows safe internet surfing through outsourcing the browser execution into a DMZ. The itWatch solution uses this process not only for secured operation of browsers but for all unplanned actions which are relevant to security:

- Automatic outsourcing and execution in a virtualized environment behind firewalls or in the cloud.
- Handling or view of critical data that has to be imported to the client from foreign data storage devices or unsecure applications.

In the „remote controlled session“ the user has all relevant rights (i.e. for installation) without putting the productive environment at risk. The content is controlled within the remote controlled system as well as on the user's client following the central guidelines, there for no malicious code can infiltrate the internal network, while the user can still access all active content and view any data. Additionally the user will get fully automated support for printing and data transport. A default reset of the remote controlled environment eliminates the eventually imported critical changes before the user's next start. Personalization of the remote controlled session for the user's log on can be realized through user profiles. Content Users that can access everything independently without putting the internal systems to risk can create efficient IT environments.