



**GW-TEL<sup>®</sup> Secure APS protects automated workstation PCs, e.g. in measurement, E2E monitoring or for unattended presentations, from unauthorized access and misuse in case of theft.**

## GW-TEL<sup>®</sup> Secure APS

Whatever the scope of application - whether in automated process lines, as monitoring systems in service level or availability management, as stand-alone presentation systems - today, PCs are often being used as autonomous systems, that is, without a user operating it.

These systems are subject to increased demands related to their security, in particular if they are used to process data or workflows from real application environments.

A concrete example, among others, are monitoring systems (robot PCs, client simulation agents, performance test driver PCs etc.) which, without user interaction, work in existing production environments and use real system and application accounts as well as real customer data.

This is where GW-TEL<sup>®</sup> Secure APS comes in, protecting these systems by applying a multi-layered security scheme.

Automated systems, as a rule, perform the Windows<sup>®</sup> boot process independently, then log on to the system via auto-login and finally, start the self-controlled process.

Now, GW-TEL<sup>®</sup> Secure APS steps in as early as during the boot stage: it installs the relevant system drivers to prevent an external access to keyboard and mouse.

In a second stage, drivers for hiding the screen contents are installed which prevent a tracing of the executed process steps from a possibly connected monitor. An essential feature here is the hardware-based control of this 'screen blackening': governed by the graphics controller, it enables - as opposed to 'regular' screensavers - the further operation of applications, for instance via a control script.

To protect the applications themselves, as well as sensible data like user accounts or system-internal information, from being misused even in case of theft (e.g. the hard disk being removed and attached to another system), the third stage is the encryption of the hard disk, optionally as a whole or partition-wise. This is done, via an appropriately powerful cryptography algorithm, as 'on-the-fly' encryption, i.e., while the system is running. The performance of the workstation PCs is not being affected by this.

For the configuration of the system, a corresponding remote console can be used. So, the central management of systems, e.g. in a distributed monitoring environment, is still possible.

All company names, product names and trademarks used are normally trademarks or registered trademarks of the relevant companies. Copyright 1996-2011, Geyer & Weinig EDV-Unternehmensberatung GmbH. No responsibility can be taken for any mistakes or errors of presentation. We reserve the right to restrictions resulting from further development.



### **Performance features:**

- Multi-layered security scheme for automated workstation PCs
- Shutoff of keyboard and mouse support on booting
- Deactivation of screen display on a directly connected monitor. Due to the virtualization of the screen, it is still possible to operate applications via the corresponding drivers (script-, program-driven etc.).
- "On-the-fly" encryption and decryption of specific hard disk partitions or of the hard disk as a whole
- Remote access via TCP/IP

### **System requirements**

#### **GW-TEL<sup>®</sup> Secure APS**

#### **System requirements for XS-Agents for RTF**

##### **Platform:**

- Microsoft<sup>®</sup> Win32 standard platform

##### **Operating system:**

- Microsoft<sup>®</sup> Windows<sup>®</sup> XP SP3
- Microsoft<sup>®</sup> Windows<sup>®</sup> 7
- recommended Windows<sup>®</sup> 7

##### **Processor:**

- Minimum Intel<sup>®</sup> Pentium<sup>®</sup> 4, 2,5 GHz
- recommended Intel<sup>®</sup> Core<sup>™</sup> 2 or
- AMD Athlon<sup>™</sup> X2

##### **RAM:**

- Minimum 1024 Mbyte
- recommended 2048 Mbyte or more

##### **Hard drive:**

- around 100 MB required in continuous operation
- around 150 MB required in addition for the installation, if installed from the local hard drive
- around 1 GB in addition recommended as a cache for measured data, if longer offline run times required
- around 10 GB recommended in addition as cache for network data, if network troubleshooting required

**The actual sizing of the system is determined in the scope of the relevant customer projects.**

All company names, product names and trademarks used are normally trademarks or registered trademarks of the relevant companies. Copyright 1996-2011, Geyer & Weinig EDV-Unternehmensberatung GmbH. No responsibility can be taken for any mistakes or errors of presentation. We reserve the right to restrictions resulting from further development.