



[Secure Mobile Computing with SafeGuard®]

Helping you keep control  
of your data ...

**utimaco**<sup>®</sup>  
safe ware

# Exceptional performance

Utimaco Safeware has been solving businesses' security concerns with specialized IT products and solutions since 1983. We are committed to the ongoing development of groundbreaking security innovations, with a third of all our staff working on future-oriented data security solutions from within our Development and Quality Assurance departments. Working alongside leading IT companies like Microsoft®, Intel®, IBM®, Lenovo, HP® and the Trusted Computing Group™ (TCG) we can ensure that users of our SafeGuard security products are always one step ahead.

As global market leader for secure mobile computing solutions Utimaco employs more than 230 staff, in the US and in seven locations throughout Europe. From these offices we manage a comprehensive partner network that operates across all major countries world-wide. Among our customers are high-profile organizations like the Canada Revenue Agency, European Commission, (German) Postbank, Pricewaterhouse Coopers, Reuters, Ministry of Justice (Netherlands), Cartier, Microsoft Germany, Statoil, Sandvik, Austrian Defence Ministry (Bundesministerium für Landesverteidigung der Republik Österreich), Zürich Versicherungs-Gesellschaft (Swiss Insurance Company), FöreningsSparbanken AB and Reckitt Benckiser, to name a few. Organizations like these value their long-term investment in security and have come to depend on the reliability and easy to use nature of Utimaco's security solutions.

The success we are enjoying is not only down to the high level of quality recognized throughout our entire product range, but also the user-friendliness of our software, our excellent support services and our ability to deliver products that fully address the demands of the market.

Utimaco Safeware AG shares have been listed on the Frankfurt stock exchange since 1999.

# [ SafeGu



## Exceptional solutions

The security of a company's information is critical to its success. Confidential data demands around the clock protection from a barrage of threats from both inside and outside the company. These might include hackers and even disgruntled employees. Mobile devices like notebooks and PDAs are often the weakest link in an organization's security.

The responsibility for IT security lies with senior management and the consequences of getting it wrong can be serious. Not only can a **company's assets be at risk**, but also if private customer details fall into the wrong hands, fines, negligence claims and other **legal actions** are a likely outcome. Not to mention **damage to the company's reputation** and **loss of trust** suffered as a result of negative publicity.

Utimaco's SafeGuard range of products sets new standards in every area of IT security. Or at least, that is the opinion of IT analysts and technical journalists, who regularly test and evaluate the SafeGuard products. For example, "Secure Computing Magazine" gave our SafeGuard Easy solution maximum points in a survey it performed in 2005.



# [SafeGuard®]

## Mobility – the key to operational and financial efficiency

Advances in mobile computing devices, mobile applications and data transfer technologies have turned the vision of “mobile business” into a reality. For many areas of business mobility is literally opening up a whole new world of opportunities.

These days employees can take their company data with them wherever they go, on their notebooks, PDAs, smartphones and the like, processing it while on the move. Furthermore, Plug & Play functionality enables them to easily connect mobile peripheral devices like USB memory sticks, digital cameras or Wireless LAN access points to their mobile device, giving them the ability to hook up to the company network over the internet, from anywhere at anytime. The arrival of Wireless LANs and Bluetooth has opened up an efficient route for transferring large quantities of data.

The benefits of a “mobile office” of this kind are enormous. It gives employees a means to lay their hands on all the information they need as soon as they need it, quickly and easily downloading it from the corporate network and updating it on site. This leads to faster and better customer service. Traveling time is no longer lost and no time is wasted in transporting data. The collective savings in time, money and effort are substantial, as are the productivity gains from significantly speeding up business processes.

# Mobility – the hidden risks

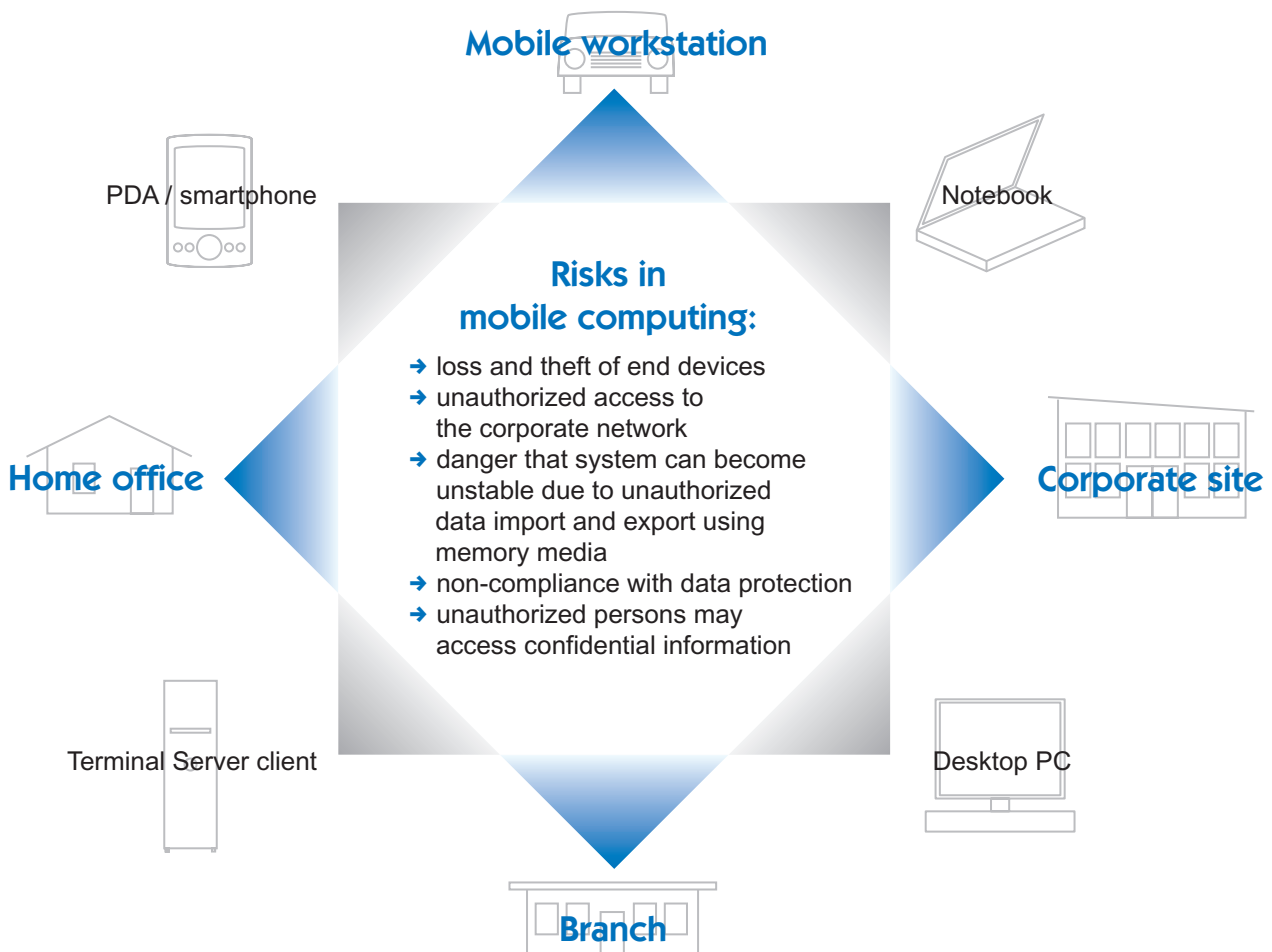
Unfortunately there's a downside. Despite all of its benefits, mobility creates weak points that open the door for data theft, industrial espionage or attacks on the network. Traditional security measures are not equipped to deal with these.

The problem is, confidential data stored on employees' mobile devices is no longer "behind" the corporate firewall, but "in front of it". The very fact that mobile devices are so portable means they are easily lost or stolen, along with the confidential data saved on them. Additionally, Plug & Play functionality allows unsecured data exchange with the mobile device. The design of today's notebooks, PDAs and smartphones makes getting round security rules relatively straightforward.

Small mobile high capacity storage devices can easily be copied or disappear - along with the confidential data stored on them.

Accessing the corporate network via public networks allows users to circumvent the company firewall.

The SafeGuard product family effectively blocks unauthorized users from attacking the corporate network whether they are attempting to do this as an outsider or from within the network. SafeGuard is a highly-developed, software suite that provides maximum mobile security.





[SafeGuard®]

**Different industries,**



The **managing director** downloads e-mails from the corporate server, processes them, updates the appointments calendar and reschedules meetings.

The **sales director** has a presentation on the future product strategy for the company saved on their notebook, for delivering to customers. Before visiting the customer they also load the company's revenue history and contacts log from the central IT server.

Just before a budget meeting with the branch managers, the **financial director** goes online to fetch the current revenue report and cost analysis.

The **insurance agent** can access the current product range and pricing models while on site with the customers. If the insurance holder's situation changes, the insurance agent can immediately give a new quotation.

The **service technician** for a mechanical engineering company can receive job details via a wireless link with the office, including extensive customer details, a map of directions and maintenance instructions. This allows for more flexibility and better time management when processing the orders.

## different tasks, the same security requirements

The **consultant** needs to be available at all times. At the hotspot in the airport lounge they download recent e-mails and check for any amendments to project reports. In the evening they discuss the project reports with the project team during a net meeting from their hotel room.

The **auditor**, who is constantly on the move, keeps their customer's financial data on the notebook for convenience and works on the audit report on the go.

The staff of a **mobile nursing service** have PDAs which they use to store their personal job plan, patient details and scheduled visit times. They enter the time they spend for each job onto the device and periodically transmit the information to headquarters for billing.



# [Safe

In the **hospital** the PC integrated into the “mobile kardex” (rounds trolley) has a wireless radio link with the central system, which the doctor can use to access patient data, notes on medication intolerance, x-rays and so forth. The kardex is used as a workstation for capturing information by doctors and other health care professionals. Data access is strictly controlled in each case.

A **software developer’s** main concern is delivering results. Working from the “home office” allows them to unleash their creativity without interruptions, and plan their time to suit themselves. An additional benefit of the “home office” is that it cuts down the employer’s office space requirements and reduces the company’s operating costs.

A young mother raises her child, while furthering her career by **teleworking** from home. Her company can continue to benefit from her knowledge, experience and willingness to contribute, without requiring her to be physically present in the office.

**All of these users and their companies have one thing in common: the need for security against the potential risks arising from their mobile working environments.**





Guard®

# [SafeGuard®]

## Mobile security, made to measure

Mobile security means protecting the device, the stored data, the application and the data transfer. Using the various solutions within the SafeGuard family companies can keep a real grip on all security risks: **SafeGuard security modules** provide optimum protection while **SafeGuard system management modules** allow them to manage all aspects of IT security effectively and effortlessly. **SafeGuard's convenience modules** make the employees' work easier and ensure that users readily accept and comply with security policies.

### SafeGuard security modules

The SafeGuard **access control function** makes certain that only authorized users can work with a particular device. Using state-of-the-art technologies such as smartcards, handwriting and fingerprint recognition, or symbol passwords, it is possible to set up individualized barriers to access.

SafeGuard's innovative **authorization function** regulates user rights for devices, applications, files and interfaces. This makes it impossible for anyone to sneak potentially disruptive software into the company, change programs, or save, export and import data without proper authorization.



SafeGuard's **data encryption function**, which is completely invisible to the user, ensures that confidential data stays confidential, regardless of whether it is saved on a PC or mobile device, or is being transferred over a network.

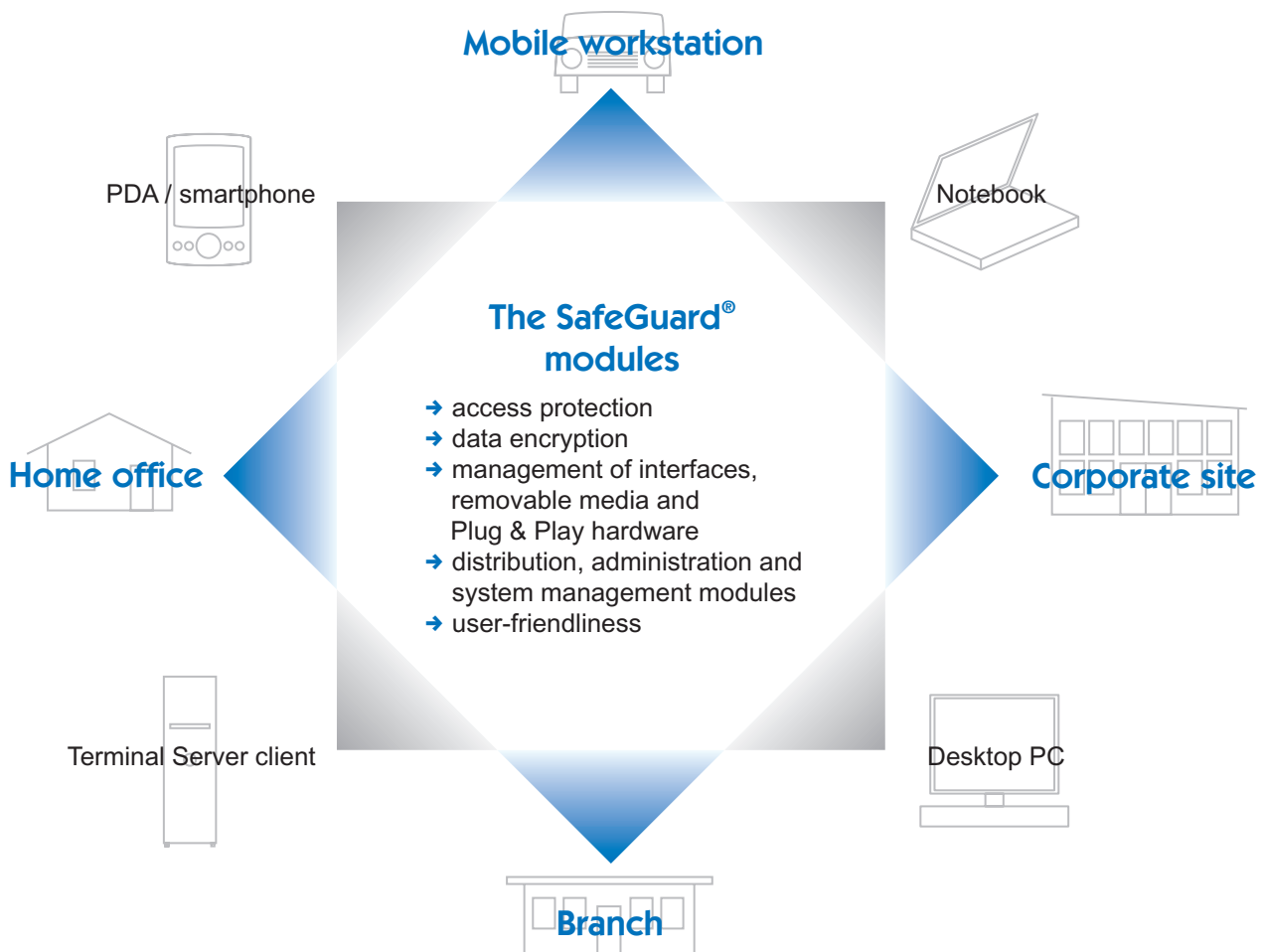
SafeGuard can be customized so that data is encrypted to meet the individual data protection needs of an organization. This includes encrypting individual files, providing a secure file folder, or encrypting the entire hard disk. This also applies to heterogeneous user groups, where only authorized staff should have access to the data. Even when computer devices are disposed or leased equipment is returned, the data still remains confidential.

SafeGuard's **functionality for managing Plug & Play** devices prevents them from being connected without permission. That means it is no longer possible to read out data to a memory stick that has been inserted while the device owner isn't looking. Neither is it possible to spy on or corrupt the device, and in the worst case scenario the corporate network too, with a wireless LAN access point that was illicitly connected without being detected.

With SafeGuard's **removable media management function**, companies can regulate the use of mobile data media like diskettes, CDs and DVDs. Among other things this makes it possible to implement version control for software, catalogues, price lists and legal regulations. Unauthorized software is frequently the cause of system crashes and preventing its use invariably increases system availability.

A woman with sunglasses on her head, wearing a white button-down shirt and grey trousers, is talking on a mobile phone. She is carrying a black briefcase. The background is a blurred outdoor setting with a blue tint.

**[SafeGuard®]**



### SafeGuard system management modules

SafeGuard supports complete separation of system administration responsibility and **security administration** responsibility. This ensures that even the system administrator can't compromise data confidentiality; which is especially critical when IT system operations are outsourced.

SafeGuard **Auditing** logs all events involving security, groups them in accordance with freely-definable rules, and creates a report.

The SafeGuard **emergency procedure** provides a means to 'unblock' authorized mobile staff if they have forgotten their device password. This means that the end device is immediately available again and productivity remains consistently high.

### SafeGuard convenience modules

Users can securely log on to several applications simultaneously using SafeGuard **Single Sign On**. This means they no longer need to remember a list of individual passwords for each application.

SafeGuard's data encryption functionality is completely invisible to the user, making life much easier for them. Data is encrypted automatically in the background, so there is no need to change normal working practices and it is impossible to make a mistake using it.

## [SafeGuard®] – the results speak for themselves

### “Power-on” and “power-off” device protection

Thanks to easy-to-install data encryption software, which **encrypts the entire hard disk** transparently, corporate data is safe from the threat of unauthorized access even when the mobile device is stolen or lost. This applies even if the hard disk is removed from the device.

Moreover, the ability to **encrypt the Windows operating system and system configuration** prevents unauthorized users booting from diskette, or using alternative booting methods to hack the system. Not even “hacker tools” can decrypt the protected files, no matter where they are located on the device. In fact linking data encryption with **authentication** before the system boot on Windows devices, or immediately after switch on in the case of PDAs, guarantees optimum protection, whether the device is switched on or off. **The encryption of data**, whether stored locally, **on the server or on a mobile storage** device, ensures powerful protection against misuse during operation or by the system administrator.

### Ensuring system and data availability

The ability to manage Plug & Play devices and removable media, combined with application-specific file access rights, provides users with effective protection against possible attempts to sneak in viruses or manipulate the system via peripheral devices. SafeGuard’s high reliability, combined with the fast but secure emergency procedure, ensures maximum system and data availability everywhere, and at all times.

### Protecting confidentiality

The SafeGuard encryption function provides extensive protection for information on devices and data media. It offers proven reliability and is easy to use, guaranteeing the maximum defense against the misuse of confidential data, no matter where it is located on the system.

## [SafeGuard®]

## Efficient and secure mobile computing

- **Effective, total protection for mobile devices**
- **Reliable, field-proven security**
- **Simple implementation of company-wide security policies**
- **Complete data confidentiality, even with outsourcing**
- **Effortless integration with existing system management tools**
- **Easy to manage, maintain and distribute**
- **Problem-free integration in heterogeneous infrastructures**
- **Highly scalable for large organizations**
- **Very user friendly**

# [SafeGuard®] – individual solutions

	SafeGuard Advanced Security	SafeGuard Easy	SafeGuard PrivateDisk	SafeGuard PrivateCrypto	SafeGuard LANCrypt	SafeGuard PDA
<b>SafeGuard system management modules</b>						
<b>Security management and distribution</b>	◆	◆	◆		◆	◆
<b>Auditing</b>	◆	◆	◆		◆	◆
<b>Emergency procedure (password reset)</b>	◆ <sup>(1)</sup>	◆	◆		◆	◆

<b>SafeGuard convenience modules</b>						
<b>Single Sign On</b>	◆	◆ <sup>(2)</sup>	◆ <sup>(3)</sup>		◆ <sup>(4)</sup>	◆ <sup>(5)</sup>

<b>SafeGuard security modules</b>						
<b>Data encryption</b>						
Operating system, system data, system configuration and temporary files		◆				
Fixed data media (such as entire hard disks)		◆			◆ <sup>(6)</sup>	
Mobile data media (such as diskettes, CDs/DVDs, USB memory sticks, ZIP disks)		◆	◆		◆	◆
Data folders		◆	◆	◆	◆	◆
Individual files			◆	◆	◆	◆
E-mail attachments				◆		◆
Backup/recovery			◆		◆	
<b>Access control</b>	◆	◆				◆
<b>Authorization</b>	◆					
<b>Plug &amp; Play device management</b>	◆					
<b>Removable media management</b>	◆					

<sup>(1)</sup> e.g. Loss of Smartcard

<sup>(2)</sup> Via Secure Auto-Logon (SAL)

<sup>(3)</sup> Automatic logon to several Private Disks possible

<sup>(4)</sup> In combination with SafeGuard Advanced Security

<sup>(5)</sup> Logon on VPN solutions possible

<sup>(6)</sup> Apart from the boot system hard disk



[www.utimaco.com](http://www.utimaco.com)

**Utimaco Safeware Inc.**

10 Lincoln Road  
Suite 102  
Foxboro, MA 02035  
USA  
Phone +1 (5 08) 543 10 08  
Fax +1 (5 08) 543 10 09  
sales.us@utimaco.com

**Utimaco Safeware Ltd**

Ash House  
Fairfield Avenue  
Staines  
Middlesex  
TW18 4AB  
UK  
Phone +44 1784 224 225  
Fax +44 1784 224 229  
sales.uk@utimaco.co.uk

**Utimaco Safeware AG**

P.O. Box 20 26  
DE-61410 Oberursel  
Germany  
Phone +49 (61 71) 88-0  
Fax +49 (61 71) 88-10 10  
info.de@utimaco.com

**www.utimaco.com**

Utimaco Safeware Partner:

