SecurePIM
by Virtual Solution

MOBILE SECURITY DESPITE BYOD: **PROTECTION OF CORPORATE DATA IN SECURITY CONTAINERS**

Members of staff bring their own smartphones to work, use them to send emails with attached contract files, access the company's network when commuting on the train and even open their personal Facebook app with their devices. In such circumstances, how can IT managers protect corporate data (such as sensitive clientinformation, for instance) from being accessed by third parties without violating data protection legislation? This cannot be done with Mobile Device Management solutions, especially in BYOD situations. The use of security containers – preferably with apps – is a solution that enables the full protection of corporate data even in the event of the loss or theft of a device, while at the same time granting members of staff the highest level of user-friendliness possible.

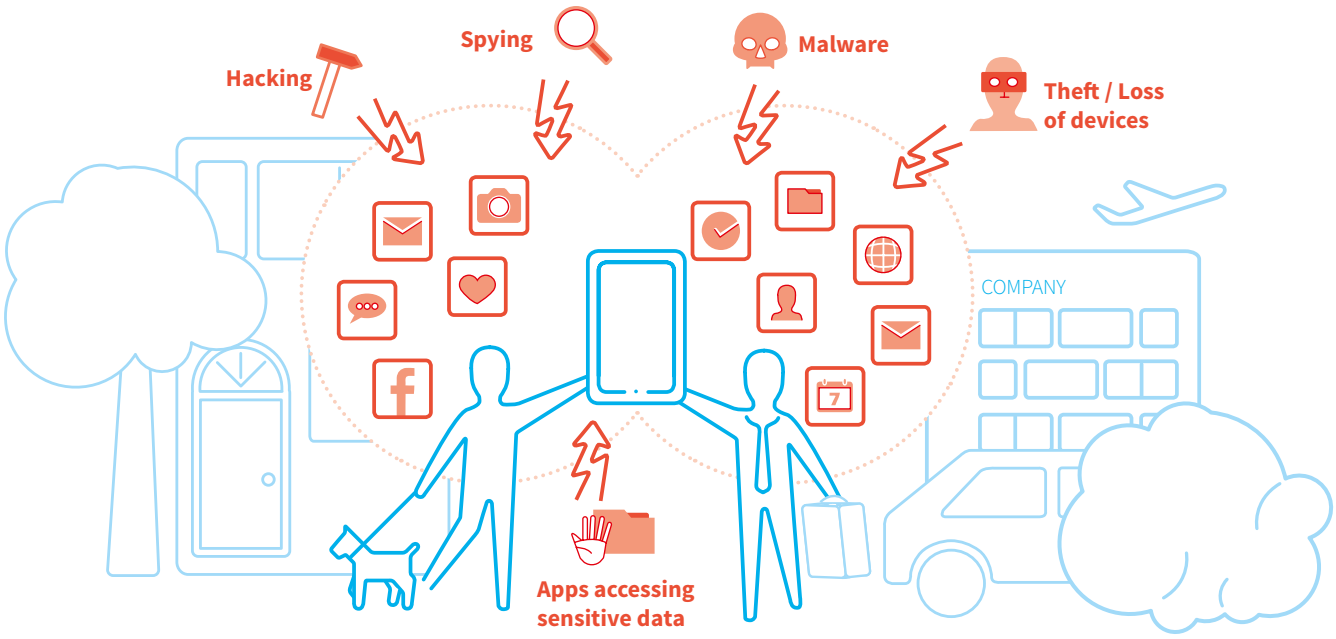
This is where we come into play. SecurePIM is an application produced by Virtual Solution AG. It is a mobile app that provides protection in all the domains mentioned above. This security app carries the "100% security made in Germany" seal of approval. For instance, amongst others, Virtual Solution AG cooperates with Germany's Federal Office for Information Security (BSI) to develop solutions for mobile terminal devices in highly sensitive fields of work.

Today, one company out of four is of the opinion that working from traditional office desks with compulsory physical presence at one's place of work is becoming increasingly outdated. This is the outcome of a recent BITKOM survey carried out amongst 1,500 managing directors und HR managers. Mobility has been part of corporate daily business for a long time now. Both employees and employers are convinced of the advantages of flexible job models. For example, employees can manage their work-life balance better, they save time and are more motivated because they can choose where and when they work. On the other hand, companies cut costs relating to offices, offer more attractive jobs and their staff's productivity and effectiveness increase.

The evolution of the employee

past	today
Work 9.00 - 5.00	**Work anytime**
Work in a corporate office	**Work anywhere**
Focused on inputs	**Focused on outputs**
Climb the corporate ladder	**Create your own ladder**
Use company equipment (COD)	**BYOD**

Problems & Risks



How can this be achieved? By using mobile terminal devices, whether in the form of company-owned smartphones and tablets or the staff's personal terminal devices, the latter model being known as "Bring Your Own Device" (BYOD). Both models represent important challenges for IT managers relating to maintaining control over the many different terminal devices in use and the data stored on them. This is particularly difficult when it comes to dealing with sensitive client data, which require high-level protection. Companies whose members of staff use their own terminal devices are obviously at risk, such as in the event of the loss or theft of a device, or if they fall prey to a cyberattack.

In addition to this, however, there are additional risk factors, such as the use of personal apps like Whatsapp or Facebook, which often access information present in other applications on the phone, such as contacts lists, for instance. The results of a survey performed by the Global Privacy Enforcement Network (GPEN) last year are a cause for true concern: 75 per cent of all apps access at least one sensitive function on a given device.

Corporate documents, business-related emails, appointments and business contacts should remain strictly segregated from personal data, not only for reasons linked to data protection, but also often as a result of compliance rules. Thanks to the SecurePIM security app, highly sensitive and business-related data are stored in a fully impenetrable container. This secure container provides the necessary security on both Android and iOS devices, while at the same time being very user-friendly and therefore well-accepted by users. Today, security and user-friendliness can go hand in hand indeed!

In BYOD environments, MDM solutions are not fully adequate

Often, companies' hands are tied due to legislation when it comes to the protection of data on personal terminal devices. Why? Because these devices are the staff members' personal possessions. This means that if an employer wants to access such devices, he/she must have legal grounds to do so. As a result, IT administrators have to deal with a series of questions, such as: "How can I prevent the loss of internal corporate data?", or "How can personal and corporate data be separated from one another, without violating IT data protection regulations?".

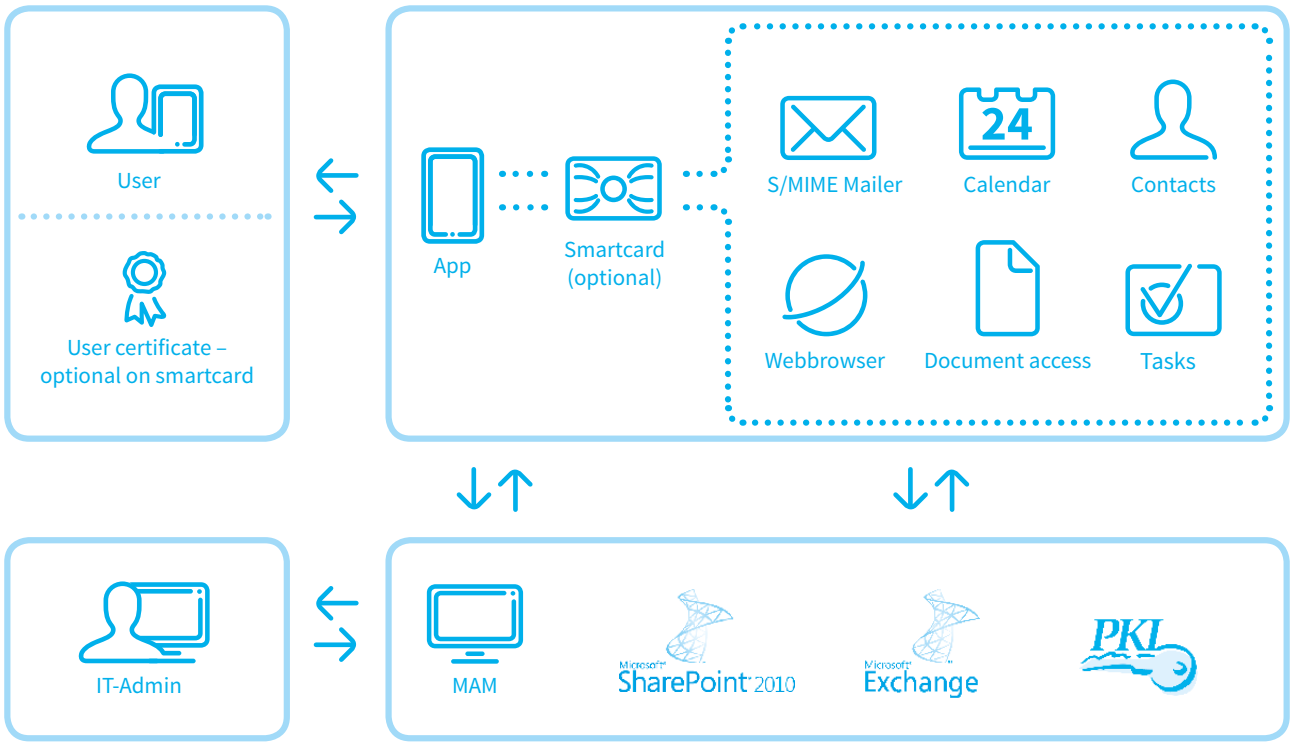
Many companies do not implement appropriate solutions for mobile security. This fact is also demonstrated by the current IDC study entitled "Enterprise Mobility in Germany 2014/2015". According to this study, currently, only 57 per cent of all German companies that deal with the issue of enterprise mobility in one way or another actually implement an MDM (Mobile Device Management) solution. The primary goal of MDM solutions is the centralised management of mobile devices. They detect which devices are being used and by whom, and what software versions and apps are used. Thanks to this type of centralised system, specific device settings can be predefined. However, MDM systems are only able to manage functions that are envisaged by the manufacturers of the devices in question. This means that it is impossible to freely increase security levels. In addition, MDM solutions cannot be implemented in BYOD environments due to the legislation in place, because companies are not allowed to control personal terminal devices.

Storage of corporate data in the app:
companies now rely on separate secure containers

In order to circumvent the disadvantages presented by MDM systems, nowadays, companies are relying on what is known as secure containers. On any given terminal device, a separate area is cordoned off, where corporate data can be managed and – most importantly – be protected in accordance with the rules in place. The company's IT department is in control of this separate container. In order to make the switch from the corporate to the personal area of the device as easy as possible for the users, security apps that pool all corporate documents, emails, contacts and appointments are the ideal solution. This means that highly sensitive corporate data, tasks and the web browser are protected from third-party access, and members of staff can access their company's internal CRM solution without incurring any security risk, for instance.

These security apps also allow for scalable security levels. The company itself can define the measures required for user authorisation, such as passwords that must fulfil certain requirements, for instance, or the use of smartcards, which guarantee the highest security level possible. The application of these kinds of external authentication components permit the protection of corporate data in the event of the loss or theft of a device, because it is impossible to access the security container without them. In addition, this type of app and the data stored in it can be deleted fast and easily via remote access. Professional app solutions go even further: they automatically encrypt all data which are sent or received via the app and stored in the container. In the course of data transmission, CRL checks are also performed. If the certificates are not valid, access is not granted.

System Architecture



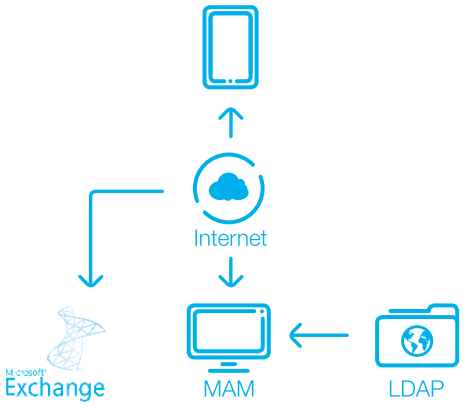
What should companies pay attention to when choosing a mobile security solution?

When deciding which specific security solution to choose, the following six criteria should be taken into consideration:

+ **User-friendliness:** Even the best solution will not serve its purpose if it is not implemented by the users. In order to increase the staff's acceptance of the solution, the chosen app must be user-friendly. Ideally, one should choose apps that have a user interface (UI) that is similar to the iOS or Android ones, so that users are already familiar with it due to personal experience. With SecurePIM, all business operations can be performed in one single app. Access your business emails, contacts, appointments and documents centrally, without having to switch apps.

+ **Integration:** It is important that the security solution should be able to be seamlessly integrated in the company's existing public key infrastructure (PKI). Keys, passwords and the like can still be used, which means that the efforts required for the integration of the solution are significantly reduced. SecurePIM can be easily and seamlessly integrated into the company's IT environment, and its integration is fast.

Integration



+ **Server solution:** A mobile security solution should also always be a server solution. Contrary to the cloud alternative, the data must always remain the property of the company. In the worst case scenario, all the company's data located in SecurePIM can be immediately blocked. The personal data on the devices are not affected by this at all.

+ **Made in Germany:** When collaborating with a service provider, it is important to know that none of the corporate data will be stored on U.S. territory. Servers must be located in German data centres and thus be subjected to German data protection rules.
The SecurePIM app was developed by Virtual Solution AG, a German software company. All security-related areas of the app and its management portal are developed exclusively by this manufacturer, making it "100% security made in Germany".

+ **Scalable security:** When choosing a security solution, it is important to be able to select different security levels and processes independently of the manufacturer, as opposed to being limited to the devices' functionalities. The security level of SecurePIM can be adapted to the requirements at hand. TLS authentication, container encryption and S/MIME encryption can take place via a smart card or user certificates. Data saved on mobile devices are encrypted with a key length of minimum 2096 bits.

+ **Central management:** In order to reduce the administration efforts required, it must be possible for the management and configuration of the security solution to be performed centrally, via a Mobile Application Management Portal. The Mobile Application Management Portal is a fundamental component of SecurePIM. Thanks to this Portal, your IT Department can configure and manage the SecurePIM app on all individual users' mobile devices centrally.

Conclusion

The fact is that the borders between the personal and corporate use of mobile devices are gradually being broken down. Employees use the same device to access their Facebook app and send sensitive corporate data via email. For IT administrators, it is becoming increasingly difficult to maintain control over the data and respect compliance rules without infringing on applicable data protection provisions. The implementation of security containers makes it possible to fully separate corporate and personal data. Thus, IT managers can define the required authorisation mechanisms to access the segregated company container and impose the defined guidelines for this area. In this manner, corporate data are protected even in the event of the loss or theft of a terminal device. In addition, a professional comprehensive solution also offers the possibility to manage and configure the app via a central portal.
Result: IT managers can focus on their real duties and push innovations forward that directly impact their company, making it more successful.

Visit our webpage:
www.securepim.com

Virtual Solution AG
Board of Directors: Andreas Eder, Dr. Raoul-Thomas Herborg
Executive Chairman: Dr. Boris Mariacher
District Court of Munich HRB 202166, USt.-ID DE813833087

Blutenburgstraße 18
80636 Munich, Germany

T +49 – 89 – 30 90 57-0
F +49 – 89 – 30 90 57-200

mail@securepim.com
www.securepim.com

Cooperation

Allianz für Cyber-Sicherheit

SecurITy made in Germany