Manage Data, Not Devices: Device Management vs Secure Containers

-A SOLITON WHITE PAPER-

Soliton®

Back when we all worked in offices (do you remember those days?), we used company-owned devices, connected to the network. It was practical; IT departments managed all the computers and had complete oversight.

But things are different now. While many companies still have networks, more of us than ever before are remote or hybrid workers — and we want or need to use our personal devices for work. For IT departments, this makes things more complicated. Privately-owned devices, not managed by IT, introduce new security risks. Devices are no longer just in the office. They're out in the world, travelling, mobile, and in the homes of employees, exchanging company data on private devices using unsecured Wi-Fi.

How to enable effective hybrid working: device management vs secure containers

When people work remotely, there are two high-level strategies companies can adopt. The first and most common strategy is device management.

Essentially, with device management, IT departments manage the endpoint — the computer, workstation, mobile phone, tablet or any other device connecting to the network. Companies will typically provide homeworkers with necessary devices, say a PC, and that PC has all the required business software on it. It's managed from inside the network, meaning IT still has control. But this approach is expensive for the business. You have to pay for the device. You have to buy software to manage it. You have to control it. You have to think about and mitigate all the risks in all the places. But it is a widespread strategy, used to enable remote and hybrid working.

For the user, device management also has downsides. The device is a business PC. If they want to use it for personal reasons, it probably isn't allowed. And if they change jobs, the computer likely will need returning, meaning if they have used the device for personal use, they might lose personal data or IT management could lock them out.

Users often end up having two devices - a personal device and one owned and managed by the company - as using the business PC for personal use is risky.

The alternative to supplying devices is getting people to use personal devices for business purposes. However, this isn't ideal. It adds complexity: IT teams must keep all the different devices and OS up to date. It may also lead to privacy invasions, as with MDM you can see what people are doing on their devices. So what else can companies do? **This brings us to the second strategy: Using a secure container.**

What exactly is a secure container?

A secure container is an application installed on a device. The user installs the app on their device and allows the company to control that app and the data inside the app — but, importantly, not the device.

It works a bit like an embassy. When you look at an embassy from the outside, that's a little part of one country inside another. The UK embassy in Tokyo, for example, is UK territory and law, operating within Japan. The secure container on the personal device is similar. Users allow an embassy of their company on that remote device. A container on a personal device, like a home computer or private phone, means it's not the device managed; it's the container. It's a little piece of the business on your device.

The secure container partitions the corporate data from the rest of the device. By doing this, IT maintains full control over the data inside the container, while keeping corporate data separate from other (personal) data on the device. This technique prevents corporate data leakage to the device and reduces the risk of data contamination by viruses or malware on the device.

Even if the device isn't secured, unauthorised users can't access the data inside the container. The company controls the container and configures the security settings. They can lock users out after 10 seconds, ask for a PIN code or require two-factor authentication. All data inside the container is encrypted, and data can be wiped remotely. Even if the device is compromised, the corporate data inside the container is still secure. Secure containers are much cheaper and faster to deploy than device management. But more importantly, it's non-intrusive to other apps or data on the device. Companies cannot view or accidentally delete personal data on devices, which would breach privacy laws in some European countries.

Secure containers = less to manage and improved mobility

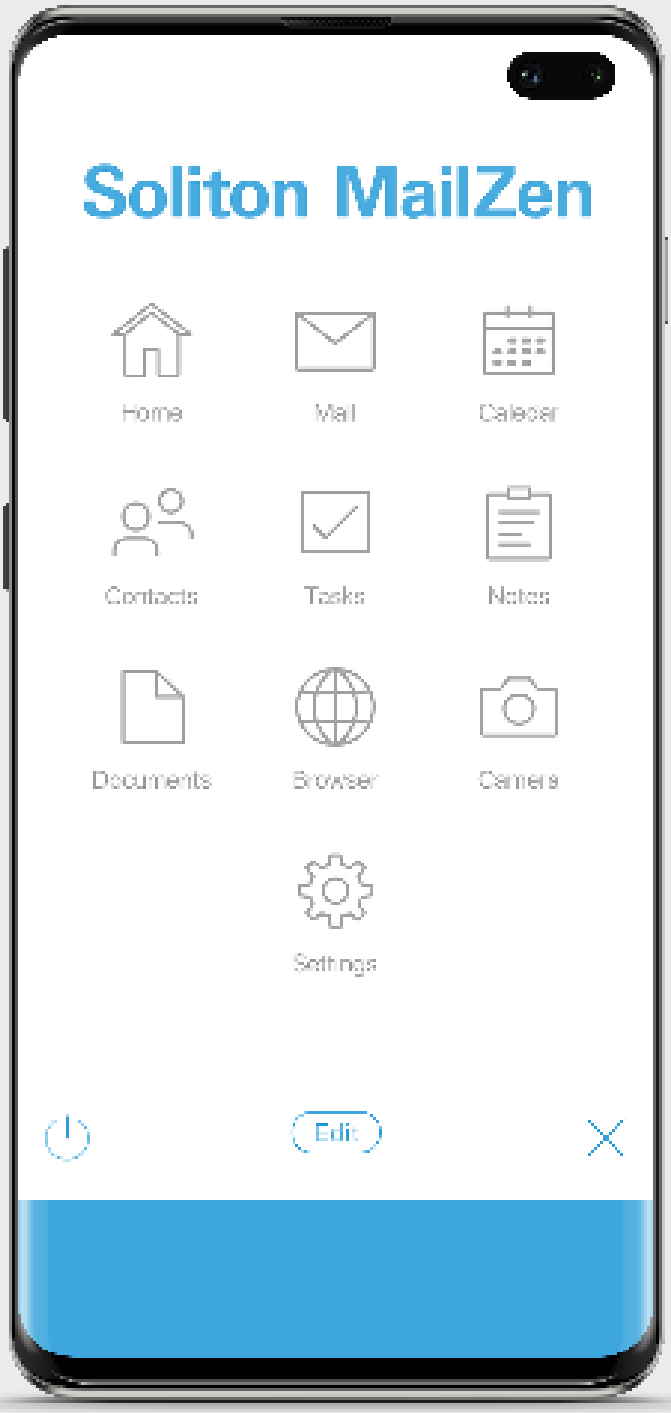
Keeping up with new security-related issues that emerge with new features or changes in applications is a headache for IT departments. Updates to Windows and macOS, as well as new iOS and Android releases, introduce new risks, which IT teams need to remember to manage.

For IT teams using the device management strategy, this means you have to keep track of everything. You have to continuously understand all different device types, all the operating systems and apps, to manage them. And this is a very costly thing. It takes time, and there's always the risk you forget or overlook something. With a secure container, you don't have to worry about these updates.

Manage data, not devices: Secure containers in practice

Soliton's MailZen solution combines a broad set of standard business functions in a single application, designed for iOS and Android. Company data, including phone numbers, contacts, calendars, files and photos, are stored inside the secure container. It's safe for remote workers to use these assets, no matter how well (or poorly) their device is secured.

> "They can download files from the server or the cloud to a secure part of the phone, which is encrypted. Users can access documents and files when offline, read them and make some edits and amends. Then, when back online, they can upload those files again."



They can also take photos within the container and upload them directly to the business server, so they never end up on the phone itself. Images can include information about private individuals, which should not end up on personal devices. For example, companies and local authorities take photo to track fly tipping incidents could include personally identifiable data.

Mailzen does more than protect company data — it can also partition company data from personal data. As a result, company assets are never "contaminated" with private data, which avoids GDPR-related problems. MailZen works for Microsoft Exchange, but also in the cloud with Office 365. Using MailZen for O365 gives you all the flexibility of O365 services, plus the peace of mind of a safe working environment.

But secure containers aren't just about phones and tablets — solutions are also available for PCs and Macs.

When to pick device management over secure containers?

Importantly, you can also combine the two; it's not necessary to have one or the other. It's perfectly fine if you have some places where you need device management and a pool of other people where you choose to have this secure container on their device because it's less intrusive.

It's not a competition between the two strategies. It's about using the approach that best fits your needs, your users and your devices.

The key to decide which approach makes sense comes down to functionality: Can the user do everything they need within the container, or do they require additional functionality?

Secure containers are separate places on personal devices, which have a set of applications required for work, for example, business email apps, the calendar or the contact lists. It could include access to specific business services that users can access within the container. But users cannot change these functions; it's not up to the user to install a new app inside the container. It's not an open architecture.

In some scenarios, where users require functionalities not available inside the container, device management may be the best approach. Device management also makes sense if the device is company-owned. Though, even if you own the device, there are some complications with device management, because users still retain privacy rights.

This point about functionality may make some companies concerned that secure containers won't include everything they need. But for the most part, this is unfounded. **The secure container balances a broad set of standard business functions, within a very secure environment, that is managed by the business, without any risks for the personal device and the personal data.**

Keeping personal data out of the enterprise

International businesses have to consider the local laws of the countries where they operate. You need to comply with the local law, and that isn't easy. Container solutions aren't necessarily the answer in every situation. But being less intrusive on the device (and therefore less intrusive to the user) often means it's preferable to device management.

Equally important with a secure container is the separation of private and business data. For example, when you have multiple email profiles on your phone, it's easy to make mistakes and send business emails out of your personal email account. By separating the two, company data never ends up in a place where a local app can access it.

Three is a clear separation between what the company owns and what the private person owns and controls. It's not an invasion of your phone. It's just installing another app. For instance, it's impossible for a user to download a file from the server and store it on their phone, where any other application can use it. Everything stays inside that container.

Benefiting the users, as well as the company

It's great for the company because they know that their company data is not going to leak out. But it's also good for the user. When they're using their device outside of work, they just see their apps, photos and emails; all work data is separate, and nobody is tracking their activity on the device. They can switch off from work, and still use their device for personal reasons. But they still have the flexibility to work at any time they want.

For the business, they have way less to worry about, and they get much more assurance around the data. It mitigated the risk to an acceptable level. And IT also is happy, because they have way less to manage. IT departments are busy; they don't want to control thousands of devices if it's not necessary.

The right solution depends on you and your situation. Based on your requirements and your budget, you can decide which strategy to use: Device management, secure containers or a combination of both. Need some help figuring it out? Contact us through the Soliton website, and one of the team will get in touch!

ABOUT SOLITON

Soliton Systems specialises in IT Security and Ultra-Low Latency Video Streaming, and is headquartered in Tokyo, Japan. Our current CEO and founder, Nobuo Kamata, PhD has been a technology-oriented leader and pioneer since 1979. Soliton has a strong vision to innovate solutions to logically satisfy the needs of our customers, without adding complexity.

Soliton Systems has continuously set new standards in performance, quality and reliability in our areas of expertise: Cyber Security, Mobile Live Broadcasting and Public Safety. For more info, visit www.solitonsystems.com.

SOL202104

EMEA office
Soliton Systems Europe N.V.
Barbara Strozzilaan 364, 1083 HN Amsterdam, The Netherlands
+31 (0)20 896 5841 | emea@solitonsystems.com
www.solitonsystems.com