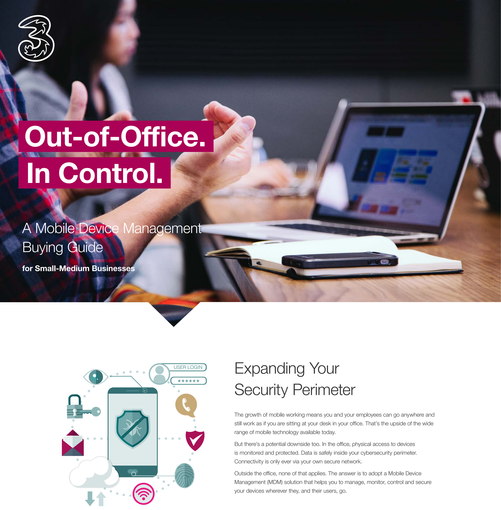

Out-of-Office. In Control.

A Mobile Device Management Buying Guide

for Small-Medium Businesses

Expanding Your Security Perimeter

The growth of mobile working means you and your employees can go anywhere and still work as if you are sitting at your desk in your office. That's the upside of the wide range of mobile technology available today.

But there's a potential downside too. In the office, physical access to devices is monitored and protected. Data is safely inside your cybersecurity perimeter. Connectivity is only ever via your own secure network.

Outside the office, none of that applies. The answer is to adopt a Mobile Device Management (MDM) solution that helps you to manage, monitor, control and secure your devices wherever they, and their users, go.

What MDM *Must* Deliver *Most*

Managing your mobile fleet is a big job that only gets bigger as your business grows. It's also getting harder as cybersecurity risks and data protection legislation grow. MDM is a single, centralised solution that makes it easier for you to give mobile users what they need and stop cyber criminals getting what they want.

Maximised security

Security can't wait. MDM can instantly deliver your security policies to any or every device on your network. If the worst happens and the security of a device is compromised, you can remotely lock or wipe the device to protect your business data.

Improved control

With MDM you have complete control over mobile devices on your network, including Bring Your Own Device (BYOD) handsets, tablets and laptops. You can remotely deploy apps and security policies to any or all devices. You can group devices by location, business function or any criteria that fit your needs. You can give users only the features and access they need and that you want them to have.

Optimised monitoring

No matter how many mobile devices you have on your network, with MDM you can monitor them from a central administration console. You can keep track of where devices are and what apps they're running, keep tabs on their health, and be alerted if unauthorised access is attempted.

Beyond BYOD

Many businesses begin considering MDM because they are considering adopting a BYOD policy, but MDM can do much more than help you keep employee-owned devices secure.

Even without BYOD, your company-owned mobile devices need managing.

MDM not only allows you to remotely and easily deploy, manage and update all devices, whether company or employee owned, but also the apps they run and the tools they use. Updates can be automated for further time-saving.

MDM also gives you the necessary information and control to cut costs, e.g if there are data-hungry apps you'd rather not allow access to, they can be restricted remotely.

With the introduction of GDPR, knowing what data is where and who can access it is essential for legislative compliance. MDM gives you insight into, and control over, data and data access on mobile devices.

Because MDM can manage all devices, apps, platforms and data regardless of their location from a single central console, your network security perimeter extends beyond your physical premises and out as far as the most distant device.

To look at it another way, security once stopped at the office door and now it goes with every device, wherever it goes.

Security that sets you free

Whether at home, on the road, or at a customer's premises, employees expect to be able to work as they would at their desk in their office.

That means:

- seamless connectivity
- access to all the tools, apps and data they need
- effortless collaboration with colleagues.

For the employee, that's the dream. For whoever's responsible for IT, it's a nightmare.

However, when MDM puts security concerns to rest, the benefits of mobility can be fully explored without risk.

- Mobile devices can be loaded with native-like browser and email apps that replicate what your employees are used to using. No training overheads, no disruption, no loss of productivity.
- Employees can be contacted by customers as easily as when they're in the office: helping to enhance customer satisfaction and improve customer retention.
- Work doesn't get left behind on the desk at 5.30pm. Wherever the mobile device goes, the work can go too, so productivity increases accordingly.
- Employees can carry out all their tasks wherever they are, rather than wasting time returning to the office to access the company network.

Choose what you use

MDM for SME is like an SME - it can start small and grow significantly.

At its most basic, you can use MDM to simplify the management of devices, by making it easy to centrally install updates in an automated and controlled way.

Using your MDM solution to monitor devices will enable you to ensure your employees adhere to company policies. It gives you a view of the sites they access, the apps they download and the tools they use for company business.

If you offer BYOD, MDM can scale up to include 'sandboxing', which keeps personal and business data separate and within a secured environment on the device.

Going beyond company policies, you can also use MDM to monitor, track and report on compliance to meet GDPR legislation requirements.

Whichever MDM solution you choose, you should be able to tailor it to suit your needs, regulations and policies: from identity management and password regulation to access limitations and blacklists. Then as your business expands and the number of mobile devices in your estate grows, and your monitoring, security and compliance needs change and grow, your MDM solution should be able to scale with you. However big your business gets, your mobile estate will never get too big to easily manage from one central console.

> "Anybody who has corporate data on a device should have it managed - there can be no excuses."
>
> Padraic Murphy, Enterprise Mobility Solutions Architect, Three Ireland

Just Managing v Mobile Device Management

Tony's Coffee Break

Tony from the sales team is out on the road, visiting a customer's site. After his site visit, he calls in to a motorway service station for a coffee and to catch up on his emails, send some customer data to a colleague, and finish a report using one of the corporate apps on his mobile.

Unfortunately the station is crowded. Although he manages to squeeze a couple of print-outs, his phone, a large cappuccino and a Danish onto the small table, it's not long before someone bumps the table and coffee and pastry go everywhere.

By the time Tony's gathered his sleeveless and his thoughts, he realises his phone has gone...

Tony without MDM...

When he thinks about all the confidential business data stored on it, and the fact that his password is "Password1", he feels very jittery. And it's not because of the coffee.

Tony with MDM...

Quicker than a barista can make a latte, he borrows a mobile, calls the office, and his missing phone is wiped of all data and apps within seconds. He celebrates with an almond croissant.

The Essential Questions

Before you invest in an MDM solution, there are some essential questions to ask - of yourself and of potential vendors. Here are those questions and the answers you would expect to hear from a reputable vendor with an MDM solution that's right for your business.

Q. Do I really need an MDM solution?

A. If you have anything over 20 devices in your mobile estate, MDM will save you time and money. Even with fewer devices, you will still see savings in terms of time spent on device management, support and configuration. With a smaller estate, only you can decide if that's worth the investment. Though remember, you can opt for a basic solution now, then as your business and your mobile estate grow, a good MDM solution will grow with you.

Q. How will the solution integrate with my existing infrastructure?

A. Whether Cloud or On Premise, MDM can leverage your existing infrastructure for user-authentication. Implementation time will vary depending on the size of the deployment, but with a cloud based solution there should be no integration issues.

Q. Which mobile platforms are supported?

A. Although MDM supports multiple platforms, devices and operating systems, certain devices function much better in an MDM environment; primarily iOS and Samsung Android.

Q. Who will manage the system once it's implemented?

A. A correctly set-up solution should require little-to-no day-to-day management, but you should be able to manage the system yourself and tasks such as enrolling and wiping devices. Ideally your vendor will provide a service desk to deal with any issues which may arise.

Q. Will the solution scale with my business?

A. Any MDM solution should be able to scale up (or down) as your business or its mobile fleet does the same. Alternatively if a Hosted solution is available, it will allow you to deploy a basic configuration with the most common policies. You could then invest in a larger scale solution when you need it.

Q. How are user licences managed?

A. One of the biggest advantages of adopting an MDM solution is flexibility, and user licensing is no exception. User licensing should be transparent, easy to manage and aligned to your business needs. A solution that offers per-user or per-device licencing will ensure you have complete visibility over how many licences are in use, and gives you the freedom to scale up or down as and when required.

Q. How can MDM help me to manage BYOD?

A. An MDM solution will enable management of any devices registered on the company network, whether they are company owned/supplied or personal devices allowed under a BYOD policy. The solution will ensure even personal devices are governed by your company security policies, and will allow you to install apps and tools so that business data is managed in exactly the same way as on company-owned devices.

Q. How will MDM reduce costs?

A. Unmanaged mobility can cost as much as 20% more than MDM.1 This is the result of overage charges, device downtime, service support and losses in productivity and efficiency. If you are unable to audit and secure data on unmanaged mobile devices, there is also the additional risk of fines for GDPR non-compliance.

1 http://bluehillresearch.com/blue-hill-finds-managed-mobility-services-deliver-a-three-year-roi-of-184/

Q. How does MDM fit with my existing security policies?

A. In many cases, companies will already have a security policy for their desktops and laptops, but this doesn't extend to mobile devices. MDM enables you to extend your existing security policies to cover all mobile devices used by your employees for business purposes.

Q. What support is available?

A. A properly set-up MDM solution should require little or no support, however a service desk should be available for 24/7 technical support if required.

To find out more, contact your Three Ireland account manager

We would love to discuss your business needs and answer any questions you may have.

1800 330 303 or GET A CALL BACK