

Mobile Device Management



Are your mobile devices protected from cyber-attacks?

Managing your remote workers' mobile devices across the cloud and business operations has never been more critical to the long-term success of your business. Each year cyber security breaches are evolving and hitting record levels, with many of these across the past 12 months being the result of the loss or security breach of mobile devices.

Are you securely managing your remote users' tablets, smartphones and laptop computers? Does your company encourage a Bring-Your-Own-Device (BYOD) culture, or do you provide your employees with company-owned devices? Risk Based Security's 2019 'Data Breach QuickView Report' stated that 1,903 breaches were reported in Q1 of this year, exposing approximately 1.9 billion records.

What measures are you taking to prevent new and evolving threats from gaining a foothold inside your IT network and accessing your valuable data?

What is Mobile Device Management (MDM)?

MDM is a type of security software that allows your IT administrators to monitor, manage and secure your employees' smartphones, tablets and other endpoints. Not only does it keep your employees devices safe and secure; it also protects your companies critical data too and will reduce the risk of it being permanently lost from your business.

MDM solutions can prevent sharing of data to and from other applications, meaning it can protect against data loss, as well as malicious breaches. Data transfer can be blocked to and from a device by activating USB and NFC (Near Field Communication) blocking. Application control is possible, providing control over what can and can't be accessed on a device.

MDM allows you to implement best practice policies for passcodes and passwords, App blacklists and security, which will help ensure the cyber robustness of your corporate network while giving your users the flexibility to work more efficiently from their own devices. It's also possible to enable automatic device wipes for when a user enters the wrong passcode within the specified number of attempts permitted.

Why do you need an MDM solution?

Today it's commonplace to read or hear about laptop computers being left on trains or stolen during a burglary when they've not been locked away securely. The same applies to stories about smartphones and tablets being stolen in public or left in the back of taxis. Both your business and personal data is put at risk if this happens to you.

Another issue with tablets and smartphones is that they aren't necessarily as secure as desktop PCs and laptops, because they're not sold with pre-installed malware protection.

MDM will allow you to manage all your company's mobile devices with a single mobile device software product. This will provide the end-to-end security you need across your mobile apps, network and data that your employees' devices access. For example, MDM will let you enforce device encryption, ensuring that staff can't have company data on them unless it's encrypted. In some cases, a stronger passcode security policy can help reduce the insurance premium for your mobile devices.

Should one of your company's mobile devices go missing, subject to it being connected to a network, you can immediately access it remotely and activate a factory reset. If your device is switched off, it can be set to carry out a remote wipe the next time it gains an active connection. MDM will also allow you to remotely remove non-authorized access to your company network, which can be important if someone resigns and you wish to shut down their remote access.

However; you don't need to worry about losing personal data, because MDM settings allow you to split your data between work and non-work. This means that items such as your photos and contacts can be separated, so that they're not affected by device updates and wipes.

The bottom line: MDM will give you the exact control you need to protect your data against loss, theft and unauthorised sharing.

How can Tribeca help?

Contact a member of our team today to find out which MDM software can help you secure your workforces' mobile devices and ensure that they're encrypted and follow compliance policies.

"Tribeca provided invaluable consultancy when we recently acquired a new company. We would have struggled to have the data and systems migrated to our platform without their knowledge and support in a project with tight timescales. Tribeca enabled us to finish the project on time and on budget."

Jason Kennard - Go ETF

Additional information

www.tribeca-it.com
www.tribeca-it.com/about
www.tribeca-it.com/services/business-it-support
www.tribeca-it.com/about/testimonials

Get in touch today to book a meeting with our experienced team to discuss your needs:

☎ 08000 122 225

✉ info@tribeca-it.com

🌐 www.tribeca-it.com

📍 16 Berkeley Street, London, W1J 8DZ