quorum

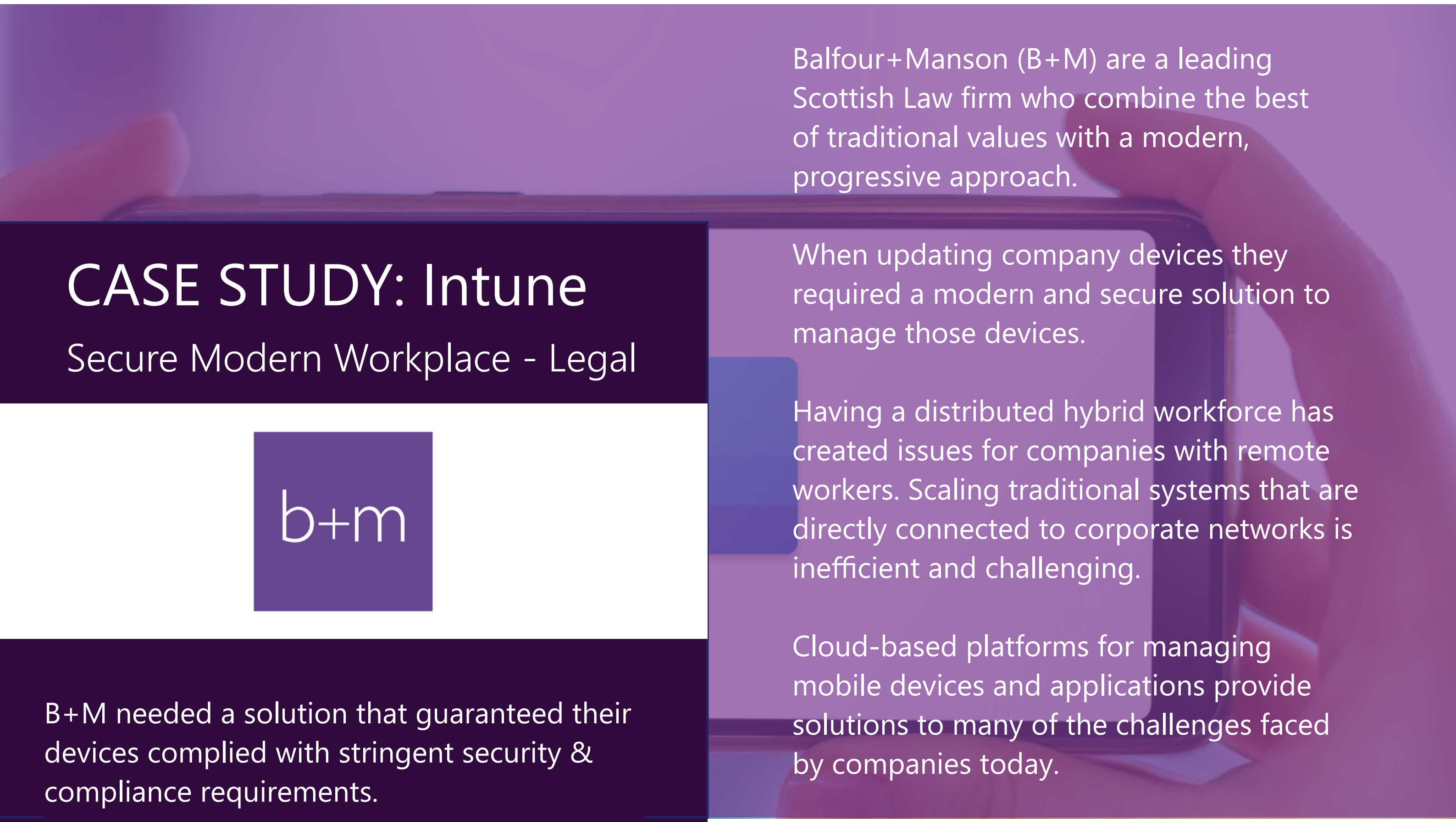
☎ 0131 652 3954
qnrl.com

marketing@qnrl.com

CASE STUDY: Intune

Secure Modern Workplace - Legal

b+m



Balfour+Manson (B+M) are a leading Scottish Law firm who combine the best of traditional values with a modern, progressive approach.

When updating company devices they required a modern and secure solution to manage those devices.

Having a distributed hybrid workforce has created issues for companies with remote workers. Scaling traditional systems that are directly connected to corporate networks is inefficient and challenging.

Cloud-based platforms for managing mobile devices and applications provide solutions to many of the challenges faced by companies today.

B+M needed a solution that guaranteed their devices complied with stringent security & compliance requirements.

They had replaced 90 company handsets and chose to configure Microsoft Intune to automatically deploy company configuration policies and applications to each device straight out of the box.

Intune is a fully-featured solution for mobile device management (MDM) and mobile application management (MAM) and was selected because:

- It supports all major operating systems. Though the project focussed on Apple iOS devices, Intune allowed B+M to support personally owned handsets.
- It integrates well with other Microsoft products B+M already use and third-party systems such as Apple Business.
- It was included in B+M's existing Microsoft 365 licenses and required no on-premises infrastructure, minimising cost.

The benefits of Intune for B+M include:

1 Enables employees to work safely from any location & device.

2 Safeguards company data & maintains compliance standards

3 Improved end user experience

Solution - Quorum conducted a full review and update of the mobile device and application management policies deployed to B+M's mobile devices to support the following scenarios:

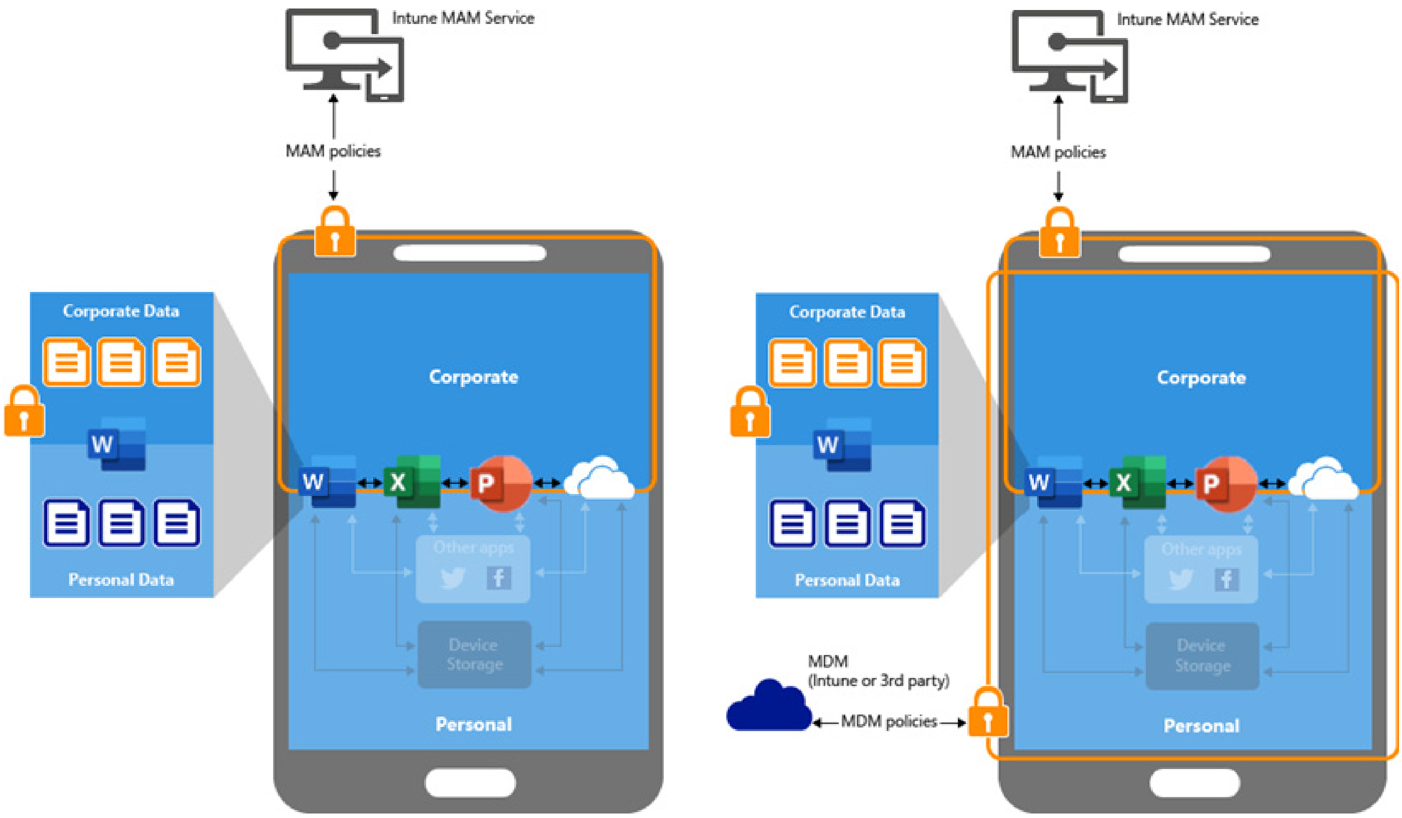
- Personally owned Android and iOS devices (Bring Your Own Device - BYOD)
  * Mobile application management (MAM) only
- Corporate-owned iOS devices for business use only (COBO)
  * Mobile application management (MAM) and mobile device management (MDM)

BYOD devices were secured with mobile application management (MAM) only, whereas corporate-owned devices had both MAM and mobile device management (MDM) applied.

Mobile Application Management

Quorum configured MAM policies to secure B+M's data at the application level. These policies keep company data in an encrypted "bubble" on devices and restrict the transfer of information in and out. Company data is kept and managed independently of personal data, making MAM an ideal solution for personal/BYOD devices.

The MAM policies set up by Quorum block access from devices that do not meet the business' compliance standards (e.g., jailbroken/rooted devices). Following best practice, Quorum also applied slightly less restrictive MAM policies on corporate-owned devices, even though the devices themselves were secured with MDM. This layered approach to security further improved B+M's security posture as data would still be protected even if the device were to be breached.



Mobile Device Management

B+M's primary focus was MDM for their corporate-owned devices. Quorum configured Intune MDM for:

- Automatic installation of core business applications.
- Deployment and protection of company email accounts.
- Updated device security controls to protect company data
- Blocking of unnecessary consumer-focused features (e.g., Apple Game Centre)
- Evaluation of all devices against company compliance requirements

Further to the full review and implementation of MDM, Quorum also configured Apple Business for B+M to:

- Register all company mobile devices with the company, ensuring Apple's Activation Lock feature never locked them out.
- Integrate & synchronise with Microsoft Intune.
- Enforce automatic enrolment of new devices in Intune MDM without the need for any manual setup by IT staff, speeding up the process for deploying/redeploying devices to end users. Provide additional controls over device features by "Supervising" iOS devices, allowing for further customisation to meet B+M's security needs and improve user experience.
- Streamline application deployment by taking advantage of the Volume Purchase Programme (VPP) to allow apps to be automatically installed without the need for a linked Apple ID.

Conditional Access

Quorum also updated B+M's existing Azure Active Directory Conditional Access policies to enforce device compliance and/or app protection policies for access to company data.

Testing & Deployment

Quorum carried out extensive user acceptance testing (UAT) to confirm that all configurations functioned as intended and satisfied the requirements of B+M. After UAT was finished, Quorum collaborated with B+M to roll out new devices and configurations with the least amount of end-user disruption possible.

Outcomes

Following the completion of the project, B+M can now be confident that company data is secured on all mobile devices. Azure Active Directory & Intune's monitoring and reporting tools provide verifiable evidence that compliance requirements are being met.

Company-owned (COBO) devices can be located or entirely wiped remotely via MDM. Personally owned (BYOD) devices can have company data wiped via MAM. In addition, Intune's remote management tools provide the company with options for remotely taking action when a device is lost or otherwise compromised.

Thanks to the integration with Apple Business, devices can be deployed or redeployed without requiring IT staff to intervene, speeding up the process of getting new employees up and running and reducing IT overhead.

B+M now has a solid and well-managed platform to grow upon.

Gareth Erskine,
Head of
Service Delivery,
Quorum

"Implementing Intune managed devices now allows B+M's IT department to manage updates in a controlled manner and dramatically improves the security of business devices.

Moving to the MDM solution has improved the end user experience, especially for new staff joining the firm. Devices can be pre-built and shipped directly to employees without any hands-on support from IT. The user would receive the new device in the box, power it on for the first time and enter their B+M email credentials, the device would then talk back to Intune and pull down all the business applications and security policies. This makes for a greater end user experience, especially for our new staff joining the firm."

Quorum continues to engage closely with B+M and is well-positioned to quickly mobilise specialised consultants as needed to keep the business current, secure, and effective thanks to our current understanding of and close working relationship with them.