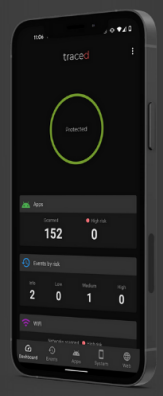
WHY INTEGRATE TRACED WITH MICROSOFT INTUNE?

Support zero-trust Protect employee privacy Stay compliant

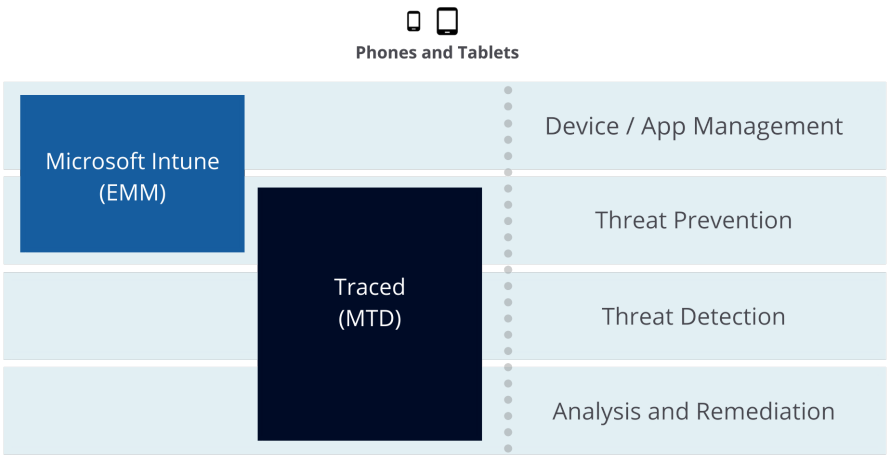


Microsoft Intune only deals with the management side of mobile devices, and can help to put a secure fence around sensitive data. It doesn't offer any means to detect or remediate mobile threats.

Microsoft Intune is an **Enterprise Mobility Management** solution, meaning it is designed specifically for managing mobile devices. As part of managing your organisation's devices, it can deploy policies, apps, and configuration to them.

Where it falls short is with its gaps in security, as it doesn't provide any threat detection, analysis or remediation capabilities out of the box. So it can't block phishing, stop malware, guide users to remove threats, identify permissions abuse on Android, or scan WiFi networks for attacks.

Many organisations have recognised the need for basic mobile security and adopted some form of EMM or MDM. However, they've run into some significant challenges, and that's led to the creation of MTD solutions - to address those challenges and shore up the threat protection aspect of mobile security.



Traced are specialists in mobile threats, and our protection is designed around identifying and stopping them – not repackaging desktop protection as a mobile solution.

And because Traced works for Intune-managed devices ***and*** unmanaged devices (think BYOD) you're ensuring every device that accesses business data is compliant with your security policies and is protected against mobile phishing, Man-in-in-Middle attacks, device vulnerabilities, and malware from apps or malicious websites.