SUPPORT YOUR CYBER ESSENTIALS PLUS CERTIFICATION WITH TRACED

Sub-category	No.	Cyber Essentials question	How Traced ensures compliance
Scope of assessment	**A2.1**	Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to apply for insurance.	**Visibility:** Traced Control enables you to ensure that both BYOD and company-owned devices are compliant. (Note that if you have an EMM or MDM (e.g. SOTI) it may only cover company-owned).
	A2.7	Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system versions for all devices.	**Visibility:** By connecting the Traced app with Traced Control in corporate mode, you gain visibility of each device model and OS version that is used for work (and therefore within scope). Traced also enables zero-trust restriction to company data. This means that shadow IT becomes visible as Traced validates compliance of devices before granting access to company data.
Secure configuration	**A5.3**	Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?	**Passcode enforcement:** Monitor compliance to your security policy with the Traced app, which can detect whether the password or passcode is set on the device.

Sub-category	No.	Cyber Essentials question	How Traced ensures compliance
Patches and updates	**A6.1**	Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?	**Out-of-Date OS detection and root detection (Android) / Jailbreak detection (iOS):** On Android, Traced highlights devices of which their security patch level is 6+ months out of date. On iOS, Traced highlights devices with a patch level more than 14 days out of date and is supported from iOS 13+. In all cases, the high-risk device status can be used in conjunction with Traced's zero-trust conditional access to restrict access to company data for vulnerable, compromised and unsupported devices.
	A6.3	Is all software licensed in accordance with the publisher's recommendations?	**Root detection (Android) / Jailbreak detection (iOS):** Both Google and Apple strongly advise against rooting/jailbreaking devices. Traced detects if a device has been rooted or jailbroken.
	A6.4	Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release? Describe how do you achieve this.	**Out-of-Date OS detection (iOS only):** When a new version of iOS is released, the Traced app alerts the user with a reminder to update. If a user fails to update within 14 days, the device becomes high risk and an alert is sent to the administrator.
Malware protection	**A8.1**	Are all of your computers, laptops, tablets and mobile phones protected from malware by either A - having anti-malware software installed, B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or C - application sandboxing (i.e. by using a virtual machine)?	To cover your organisation's smartphones and tablets, you'll probably need to select both options A and B. Refer to the answers below.

Sub-category	No.	CyberEssentials question	How Traced ensures compliance
	A8.2	(A) Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access?	**AI-powered anti-malware (Android only):** The Traced app's Android malware app engine scans apps at point of install and alerts users to uninstall immediately if malicious. The malicious signatures and Deep Learning model are checked for updates daily.
	A8.3	(A) Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?	**AI-powered anti-phishing (iOS and Android):** Scans web links for malicious content, via Safari on iOS, and the Traced AI-powered Link Checker on Android. Both known malicious signatures and our Deep Learning model are checked for updates daily.
	A8.4	(B) Where you use an app-store or application signing, are users restricted from installing unsigned applications?	**Root detection (Android) / Jailbreak detection (iOS):** As unsigned apps can usually only be installed on rooted or jailbroken devices, Traced detects if the device has been rooted or jailbroken.
	A8.5	(B) Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?	**Anti-malware (Android):** The AI-powered malware detection engine identifies high risk apps. You should use this in conjunction with a good security policy based around the ICO guidelines for Mobile App safety, and followed by all staff.

traced
Mobile security, employee privacy

We designed Traced to make it easy for small and medium businesses to protect their mobile devices from attack. We're Cyber Essentials Plus-certified ourselves, so we know that by using Traced Control and deploying the Traced mobile security app on your employees' iOS and Android phones and tablets, you can tick off all these requirements.

Talk to us and we'll help get you set up and running quickly, and can even put you in touch with a Cyber Essentials advisor who can answer other questions you might have about your business' security operations.