SUPPORT YOUR CYBER ESSENTIALS PLUS CERTIFICATION WITH TRUSTD

Sub-category	No.	Cyber Essentials question	How Trustd helps
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:** Trustd enables you to ensure that both BYOD and company-owned devices are compliant. (Note that if you have an EMM or MDM (e.g. Mircosoft Intune or SOTI) it may only cover company-owned).
	A2.6	Please list the quantities of tablets and mobile devices within the scope of this assessment. *Please Note: You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed.*	**Visibility:** By connecting the Trustd app with the Trustd console, you gain visibility of each device make and OS version that is used for work (and therefore within scope). Trustd also enables zero-trust restriction to company data. This means that shadow IT becomes visible as Trustd validates compliance of devices before granting access to company data.
Secure configuration	**A5.9**	When a device requires a user to be present, do you set a locking mechanism on your devices to access the software and services installed? Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.	**Passcode enforcement:** The Trustd app for Android and iOS devices is detects if a locking mechanism is set. If no locking mechanism is detected, the user and IT admins are alerted. The user is then guided to set a locking mechanism and their access to company data is automatically revoked from mobile devices until a locking mechanism is detected.

Sub-category	No.	Cyber Essentials question	How Trustd helps
Patches and updates	**A6.1**	Are all operating systems and firmware on your devices supported by a vendor that produces regular fixes for any security problems?	**Out-of-Date, Unsupported, Rooted (Android) or Jailbroken (iOS) OS detection:** On Android, Trustd highlights devices with security patch levels >6 months out of date. On iOS, Trustd highlights devices with patch levels >14 days out of date. Trustd detects iOS devices and iOS/Android versions which are not supported. High-risk device statuses can be used with Trustd's zero-trust conditional access to restrict access to organisational data from vulnerable, compromised and unsupported software.
	A6.3	Is all software licensed in accordance with the publisher's recommendations?	**Root (Android) / Jailbreak detection (iOS):** Both Google and Apple strongly advise against rooting/jailbreaking devices. Trustd 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?	**Out-of-Date OS detection:** On Android, Trustd highlights devices with security patch levels >6 months out of date. On iOS, Trustd highlights devices with patch levels >14 days out of date. **Root (Android) / Jailbreak detection (iOS):** Both Google and Apple strongly advise against rooting/jailbreaking devices. Trustd detects if a device has been rooted or jailbroken. High-risk device statuses can be used with Trustd's zero-trust conditional access to restrict access to organisational data from vulnerable, compromised and unsupported software.
Malware protection	**A8.1**	Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either: A - Having anti-malware software installed and/or B - Limiting installation of applications by application allow listing (For example, using an app store and a list of approved applications, using a Mobile Device Management (MDM solution)) or C - None of the above, please describe	

Sub-category	No.	CyberEssentials question	How Trustd helps
	A8.2	If Option A has been selected: Where you have anti-malware software installed, is it set to update in line with the vendor's guidelines and prevent malware from running on detection?	**AI-powered anti-malware (Android only):** The Trustd 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	If Option A has been selected: 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):** The Trustd app's Android malicious website protection scans web links and performs realtime cloud lookups to detect malicious content. The Trustd On-device VPN for Android and iOS detects and blocks known malicious websites whilst browsing the web. Both known malicious signatures and the Deep Learning models are checked for updates daily.
	A8.4	If Option B has been selected: 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, Trustd detects if the device has been rooted or jailbroken.
	A8.5	If Option B has been selected: 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 maintain 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 good security policy, processes and training around mobile app safety.

We designed Trustd MTD to make it easy for businesses to protect their mobile devices from attack. We're Cyber Essentials certified ourselves, so we know that by using the Trustd MTD console and deploying the Trustd mobile security app on your employees' iOS and Android phones and tablets, you can tick off 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.

trustd mtd
from traced