Cyber Essentials

Date: 13 Oct 2022, 3:44:58 PM

Cyber Essentials is a Government-backed, industry-supported scheme to help UK-based organisations protect themselves against common online threats. We've explained below how Trustd supports your compliance with Cyber Essentials on mobile devices, and you can use this in your Cyber Essentials Plus application.

Section
A2.1
Description
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.
Trustd MTD feature
Visibility: Trustd console 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).
Compliant*:
Yes

Section
A2.6
Description
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. All devices that are connecting to cloud services must be included.
Trustd MTD feature
Visibility: By connecting the Trustd app with the Trustd console in corporate mode, you gain visibility of each device model 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.
Compliant*:
Yes

Section
A5.3
Description
Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials?
Trustd MTD feature
Passcode enforcement: Monitor compliance to your security policy with the Trustd app, which can detect whether the password or passcode is set on the device.
Compliant*:
Yes

Section
A6.1
Description
Are all operating systems and firmware on your devices supported by a vendor that produces regular security updates?

Trustd MTD feature
Out-of-Date OS detection and root detection (Android) / Jailbreak detection (iOS): On Android, Trustd highlights devices of which their security patch level is 6+ months out of date. On iOS, Trustd highlights devices with a patch level more than 14 days out of date and is supported from iOS 13+.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 Trustd's zero-trust conditional access to restrict access to company data for vulnerable, compromised and unsupported devices.
Compliant*:
Yes

Section
A6.3
Description
Is all software licensed in accordance with the publisher’s recommendations?
Trustd MTD feature
Root detection (Android) / Jailbreak detection (iOS): Both Google and Apple strongly advise against rooting/jailbreaking devices. Trustd detects if a device has been rooted or jailbroken.
Compliant*:
Yes

Section
A8.1
Description
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)?
Trustd MTD feature
To cover your organisation's smartphones and tablets, you'll probably need to select both options A and B. Refer to the answers below.
Compliant*:
Yes

Section
A8.2
Description
(A) Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access?
Trustd MTD feature
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.
Compliant*:
Yes

Section
A8.3
Description
(A) Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?
Trustd MTD feature

AI-powered anti-phishing (iOS and Android): Scans web links for malicious content, via Safari on iOS, and the Trustd AI-powered Link Checker on Android. Both known malicious signatures and our Deep Learning model are checked for updates daily.

Compliant*:

Yes

Section

A8.4

Description

(B) Where you use an app-store or application signing, are users restricted from installing unsigned applications?

Trustd MTD feature

Root detection (Android) / Jailbreak detection (iOS): As unsigned apps can usually only be installed from rooted or jailbroken devices, Trustd detects if the device has been rooted or jailbroken.

Compliant*:

Yes

Section

A8.5

Description

(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?

Trustd MTD feature

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.

Compliant*:

Yes

Device details

This is a list of devices that can be used for section A 2.6.

Platform	OS version	Make	Model	Count
android	32	Google	Pixel 4a	7
android	31	Google	sdk_gphone64_x86_64	3
android	33	Google	Pixel 6a	2
android	30	Google	sdk_gphone_x86	2
android	32	Google	Pixel 4 XL	1
android	29	HUAWEI	BLA-L09	1
ios	15.5	Apple	iPhone SE 2nd Gen	4
ios	15.6.1	Apple	iPhone SE 2nd Gen	1
ios	15.3	Apple	iPhone 7	2
ios	15.4.1	Apple	iPhone 7	2
ios	15.2.1	Apple	iPad Pro 12.9 inch 5th Gen	1
ios	15.5	Apple	iPad Pro 12.9 inch 5th Gen	1
ios	15.6	Apple	iPad Pro 12.9 inch 5th Gen	1
ios	15.5	Apple	iPhone 12 Pro Max	2
ios	15.6.1	Apple	iPhone 12 Pro Max	1

Platform	OS version	Make	Model	Count
ios	15.2	Apple	Simulator	1
ios	15.6	Apple	iPhone 8	1
ios	15.5	Apple	iPhone SE	1
ios	unknown	unknown	unknown	1

* we cannot guarantee that all devices are compliant with the CE assessment scope criteria, however, based on the information currently available from the devices reporting into your Trustd dashboard, no unresolved compliance breaches have been currently identified