

Cyber Essentials Plus Assessment Report

Assessment of:	Cannon Technologies Ltd
Assessed by (Certification Body)	SupPortal UK Ltd
Assessed by (Assessor name)	Richard Andreae
Assessed by (Lead Assessor name)	Richard Andreae
Date of assessment visit	25/09/2020
Date of report:	2020-10-02

Cyber Essentials Plus certification can only be issued by a licensed Certification Body.

You can confirm the authenticity of this report by contacting IASME Consortium

+44 (0)3300 882752



1. About this report

Cyber Essentials Plus is the audited version of the Cyber Essentials information security standard. Cyber Essentials requires organisations to have a number of technical and procedural controls in place to improve their information security in order to mitigate common internet-borne cyber attacks. Cyber Essentials Plus is a series of tests that provide a further level of assurance that these technical controls have been successfully implemented within an organisation.

This report is a record of the Cyber Essentials Plus audit of Cannon Technologies Ltd against the Cyber Essentials standard that has been carried out by Richard Andreae of the Certifying Body SupPortal UK Ltd.

Cyber Essentials provides assurance that a number of key information security controls are in place within an organisation. For further assurance, the IASME information security standard provides a broader set of controls that enable good information security governance across an organisation.

1.1. Summary of findings

Cannon Technologies build and design Transportable Modular Data Centres for government and defence. They are located at the one site in New Milton, the IT infrastructure they have in place is well manage by an outsourced IT company Bourne Technologies. They have a bespoke ERP/MRP system in house which is also managed by Bourne Technologies. All the sever equipment is in its own secure comms room. The users mostly work from Windows 10 desktops in addition to the ERP system they use Office 365 productivity tools, AutoCAD and Adobe. These machines are built from a single image. Patching is managed remotely as a service to ensure all patches are installed within 14 days of release. I would recommend that a twice-yearly security audit is performed to check all devices in the network are up to date and secure.

The assessor has concluded that Cannon Technologies Ltd has passed the required tests and should be awarded the Cyber Essentials Plus certification.

If a test has not been passed successfully, the assessor has provided feedback within the relevant section.

1.2. Evidence of activities

In carrying out the audit, the assessor will have carried out a number of technical test and have seen documentary evidence. This evidence forms the basis for the assessor's recommendations and where appropriate has been included in this report.

2. Scope

Cannon Technologies is located on one site, it has a public IP subnet of 51.148.115.160/29. The internal networks consist of 3 subnets 192.168.2.0/24 (Downstairs subnet) 192.168.3.0/24 (Upstairs subnet) and 192.168.100.0/24 (servers and infrastructure subnet)

Certain items will be out of scope for the Cyber Essentials Plus assessment. Notable exceptions are listed below:

Company Website excluded because located with cloud hosting provider and as such not required part of Cyber Essentials Plus scoping requirements

3. External Testing

3.1. Test 1 – Remote vulnerability assessment

This test was awarded **PASS** by the assessor

The test did not identify any vulnerabilities that were scored 7 or higher on CVSS v3 during the testing of the external IP addresses.

4. Internal testing

A suitable sample set of devices was selected as follows:

Cannon Technologies have 3 Windows 2019 Servers one of which is a terminal server, 43 Windows 10 1909 desktops and 5 Windows 1909 Laptops. The sample of devices included 1 terminal server 192.168.100.199 and 4 Windows 10 1909 pcs 192.168.2.31, 192.168.3.43, 192.168.3.44, 192.168.3.47. There were no mobile devices included in the scope of this assessment

4.1. Test 2 – Review of device patching

This test was awarded **PASS** by the assessor

No vulnerabilities were identified for the tested devices that were scored 7 or higher on CVSS v3 and that met the parameters listed in the Cyber Essentials Plus guidance.

4.2. Test 3 – Review of malware protection

This test was awarded **PASS** by the assessor

It was identified that Cannon Technologies Ltd is using the following methods of malware protection in their organisation:

- A - Anti-malware software

A - Anti-malware software

Anti-malware software is correctly installed and configured on all devices that rely on this method

4.3. Test 4 – Review of protection against malware sent by email

This test was awarded **PASS** by the assessor

The standard set of test files was sent to each End User Devices in the sample set via email.

All of the malware test files were successfully blocked by the End User Devices.

All of the non-malware test files prompted a suitable warning or opportunity to cancel before opening for all End User Devices

4.4. Test 5 – Review of protection against malware delivered through a website

This test was awarded **PASS** by the assessor

The standard set of test files was attempted to be accessed via a website on all End User Devices within the sample set.

All of the malware test files were successfully blocked by the End User Devices.

All of the non-malware test files prompted a suitable warning or opportunity to cancel before opening for all End User Devices



CERTIFICATE OF ASSURANCE

Cannon Technologies Ltd

13 Queensway, Step Lane Ind. Est., New Milton, Hampshire, BH25 5NU

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME

NAME OF ASSESSOR : Richard Andrae

CERTIFICATE NUMBER : IASME-CEP-001063

DATE OF CERTIFICATION : 2020-10-02

PROFILE VERSION : February 2017

RECERTIFICATION DUE : 2021-10-2

SCOPE : Whole Company

CERTIFICATION MARK



CERTIFICATION BODY

SUPPORTAL

CYBER ESSENTIALS PARTNER



IASME
CONSORTIUM