vicarius

CYBER ESSENTIALS · UK COMPLIANCE

vRx for Cyber Essentials certification

Cyber Essentials compliance platform. Supporting the UK government Cyber Essentials scheme

Cyber Essentials is no longer optional for UK organisations. vRx is one platform that scans, fixes, and produces the evidence you need to support your certification.

What is Cyber Essentials?

What is Cyber Essentials?

The UK Government's minimum cyber security standard, backed by the NCSC and managed by IASME. Mandatory for government suppliers and increasingly required across financial services, healthcare, legal, and defence supply chains.

CE vs CE+

Cyber Essentials
vRx scans your environment, fixes every gap, and produces the pass/fail evidence for your self-assessment.

Cyber Essentials Plus
Same platform, same reports. You share vRx's pass/fail assessment reports with an external NCSC-approved certification body who conducts an independent technical audit.

The five controls

1 Firewalls
Block unauthorised access at every network entry point.

2 Secure configuration
Remove defaults and lock down every device and system.

3 Access control
Restrict admin rights and enforce strong authentication.

4 Patch management
Apply critical updates within 14 days across all systems.

5 Malware protection
Protect every device against ransomware and malicious software.

How vRx gets you there | Scan and remediate per control

Control	vRx scan	vRx remediate
Firewalls and secure configuration	Maps every open port, exposed service, and misconfigured device, showing exactly where your boundaries are at risk.	Flags misconfigured assets and tracks every configuration fix through to completion.
Patch management	Identifies every unpatched vulnerability across your estate, prioritised by exploitability.	Automates patch deployment across Windows, macOS, and Linux meeting CE's patch timing requirements, with a complete record of every action.
Access control and configuration	Validates access control configurations and flags every setting that falls short of CE requirements.	Handles complex configuration fixes, from tightening admin privileges to enforcing security policies, ensuring every control is demonstrably in place.
Malware protection	Scans every device for known malware-related vulnerabilities and unprotected entry points that could expose your environment to attack.	Deploys configuration-based protections and scripted fixes to ensure malware defences meet CE requirements across all devices and operating systems.

The process | From scan to certificate

DISCOVERY → **vRx**
Maps every active host and device

SCAN → **vRx**
Network and vuln scan, CE* scored

REMEDIATION → **vRx**
Patch, script and config fix

REPORT → **vRx**
Pass/fail evidence CE* and CE+* ready

CERTIFY → **Certify**
NCSC-approved 3rd party body

vRadar is the scanning engine built inside vRx | Certification is awarded by an NCSC-approved body

*CE: self-assessment

*CE+: 3rd party audit

One platform. Scan. Fix. Certify.
vRx combines a native scanning engine with built-in remediation. UK organisations get the evidence they need for CE self-assessment and the pass/fail assessment they can present during a CE+ certification audit.

Compliance coverage
CE – self-assessment evidence
CE+ – report for 3rd party audit
PCI-DSS | HIPAA | CMMC

info@vicarius.io

AICPA SOC