



Cyber Essentials Malware Protection Guide

Defender Antivirus | Application Allow Listing | Ransomware

WINDOWS 11 & SME EDITION

01 — EXECUTIVE BRIEF

Purpose and scope

Malware protection is one of the five Cyber Essentials technical controls. This guide gives SMEs a practical way to check endpoint protection, introduce application allow listing where suitable and improve resilience against ransomware.

The operating principle

Choose a compliant malware protection mechanism for every in-scope device. Verify that it is active and effective, record exceptions and reassess when devices or policies change.

The guide focuses on supported Windows 11 endpoints, including standalone workgroup PCs. Server, mobile, cloud and specialist devices require separate platform-specific review.

Audience: SME owners, IT administrators, managed service providers and Cyber Essentials assessment leads.

Requirements basis: Cyber Essentials Requirements for IT Infrastructure v3.3 (April 2026). Additional ransomware safeguards are identified separately from the scheme's mandatory controls.

02 — REQUIREMENTS

Understand the malware protection control

Cyber Essentials v3.3 describes two approaches: anti-malware software for Windows and macOS devices, or application allow listing for in-scope devices. Sandboxing should not be assumed to be a separately listed route under this version.

The anti-malware route requires software kept updated as recommended by its vendor, prevention of malware and malicious code running, and prevention of connections to malicious websites.

The allow-listing route requires an actively approved application list and enforcement of appropriate code-signing controls. Merely allowing all signed applications is not sufficient.

Required versus recommended

Tamper protection, Controlled Folder Access, EDR, isolated backups and recovery exercises are valuable safeguards, but should not be presented as individually mandatory requirements of the Cyber Essentials malware protection control.

Assessment sequence: Inventory → Configure → Verify → Record evidence → Reassess.

03 — SECUREX7 WORKFLOW

From endpoint inventory to assurance

1. Discover. Identify all in-scope devices, Windows versions, protection products and responsible owners.
2. Assess. Check supported endpoint security settings, active antivirus status, security intelligence currency and relevant exceptions.
3. Prioritise. Distinguish missing protection, weakened configuration and unjustified exclusions from lower-risk observations.
4. Remediate. Follow vendor-approved instructions and document any change that might affect business applications.
5. Verify. Recheck the actual device state and retain evidence of the completed action.

Do not confuse presence with protection

A green status icon or successful scan is not by itself evidence that all Cyber Essentials malware protection requirements are satisfied.

04 — MICROSOFT DEFENDER ANTIVIRUS

Configure Windows protection

Microsoft Defender Antivirus is included with supported Windows 11 editions and can provide the anti-malware mechanism. Confirm it is the active provider; a third-party antivirus may place Defender in passive mode.

- Open Windows Security → Virus & threat protection and review the protection status and alerts.
- Under Manage settings, confirm real-time protection is enabled.
- Review cloud-delivered protection and automatic sample submission against company policy.
- Check protection updates and confirm security intelligence is current.
- Under App & browser control, review SmartScreen and malicious website/download protection.
- Review exclusions and remove broad or unjustified exceptions.
- Consider enabling tamper protection as an additional safeguard.

Check your management context

Labels and available settings differ by Windows version, edition, antivirus provider and whether the device is centrally managed.

05 — OBSERVE BEFORE CHANGING

Verify Defender with PowerShell

Use read-only PowerShell commands to record the current configuration. Run from an elevated PowerShell session where required.

```
Get-MpComputerStatus | Select-Object AMServiceEnabled, AntivirusEnabled, RealTimeProtectionEnabled, AntivirusSignature  
LastUpdated
```

```
Get-MpPreference | Select-Object DisableRealtimeMonitoring, DisableBehaviorMonitoring, DisableIOAVProtection, ExclusionP  
ath, ExclusionProcess
```

Record the output alongside the device name, Windows build, installed antivirus provider and review date. Interpret the results in context: one Boolean value cannot demonstrate complete compliance.

Do not disable protection for testing

Avoid turning off Defender, altering exclusions or modifying policies simply to confirm that a control exists. Use observation and approved test procedures.

06 — EVIDENCE AND RISK

Defender assessment checklist

- Windows version is supported and the device appears in the inventory.
- An effective anti-malware product is active and functioning.
- Real-time malicious-code prevention is operating.
- Security intelligence and engine updates meet vendor recommendations.
- Malicious website connections are blocked through the chosen protection stack.
- Exclusions are narrowly scoped, justified and approved.
- Ordinary users cannot casually disable protective controls.
- Remote and intermittently connected devices are included.

Suggested evidence fields: Device / User / OS / Product / Real-time status / Intelligence updated / Web protection / Exclusions / Checked by / Date / Action.

SecureX7 evidence

SecureX7 can assess supported endpoint security configurations and help explain remediation. Controls not supported by deployed integrations still require manual or third-party verification.

07 — APPLICATION CONTROL

Application allow listing explained

Application allow listing changes the default decision from “run unless recognised as malicious” to “run only when approved”. It can provide an alternative Cyber Essentials malware protection approach when implemented to the scheme requirements, or an additional layer alongside antivirus.

App Control for Business: Windows policies can restrict executable code and scripts; availability and management vary by edition and deployment.

AppLocker: Supports executable, installer, script and packaged-app rules, including audit-mode testing.

Smart App Control: Offers reputation- and signing-based protections on supported Windows 11 devices, but is not automatically equivalent to a fully administered allow list.

Baseline rule

Do not use a broad “all signed applications” rule as a substitute for explicit approval. Avoid writable-path exceptions that let users run arbitrary code.

08 — PILOT AND DEPLOY

Introduce allow listing safely

1. Inventory applications. Record business applications, installers, scripts and maintenance tools.
2. Define approval. Identify authorised publishers, versions, code-signing requirements and exception owners.
3. Audit first. Use audit-only mode where supported and review potential blocks.
4. Pilot carefully. Test line-of-business applications, updates, sign-in and recovery operations.
5. Enforce in stages. Expand only when support incidents and blocked events are understood.
6. Review continuously. Reassess approvals as applications, roles and threats change.

Rollback is part of deployment

Keep a documented emergency approval and recovery process so a mistaken allow-listing rule does not prevent legitimate work or device recovery.

09 — RANSOMWARE RESILIENCE

Reduce likelihood and limit impact

Ransomware can enter through phishing, stolen credentials, vulnerable services or malicious downloads. Prevention matters, but SMEs also need to contain incidents and restore business operations.

- Maintain effective anti-malware and malicious website blocking.
- Keep users as standard users and use separate administrator accounts.
- Apply critical security fixes promptly and restrict exposed remote access.
- Consider Controlled Folder Access, testing business applications before broad deployment.
- Maintain isolated, offline or immutable backups and protect backup administration.
- Test restoration of critical files and business systems.
- Prepare a short incident plan naming who isolates devices and contacts IT support.

Backups are essential good practice

Backups and restoration tests are strongly recommended for ransomware resilience, but they are not a standalone mandatory Cyber Essentials technical control.

10 — SME IMPLEMENTATION

A practical four-week plan

Week 1 — Establish the baseline. Inventory in-scope devices and confirm the protection mechanism, real-time status, updates, web protection and exclusions.

Week 2 — Close the gaps. Correct disabled or outdated protection, remove unjustified exclusions, restrict unnecessary local administrator rights and record evidence.

Weeks 3-4 — Add resilience. Pilot allow listing where appropriate, review Controlled Folder Access, validate backup isolation and perform a test restore.

Ongoing — Maintain assurance. Review configurations regularly and after significant changes; investigate devices that have stopped reporting.

For workgroup PCs

A shared inventory, consistent per-device checklist and named owner can be sufficient for a small organisation. Central management reduces manual effort as the estate grows.

11 — AUDIT-READY EVIDENCE

Final assessment checklist

- Every in-scope device is identified and assigned an appropriate protection mechanism.
- Mandatory requirements are checked against the selected approach.
- Exceptions and failed checks are remediated or formally escalated.
- Configuration evidence is dated and attributable to the correct device.
- The organisation has an owner and process for ongoing monitoring.

Suggested evidence pack: scoped device inventory; antivirus status exports; dated security intelligence checks; web protection settings; exclusion approvals; application control policy and audit results where used; remediation history; and re-verification records.

Turn point-in-time assessment into a process

SecureX7 helps connect discovery, configuration assessment, remediation guidance and verification, making it easier to demonstrate sustained improvement rather than a one-off check.

12 — MAINTAIN THE BASELINE

References and limitations

Authoritative references

- NCSC — Cyber Essentials Requirements for IT Infrastructure v3.3.
- NCSC — Cyber Essentials resources and guidance.
- Microsoft — Virus & threat protection in Windows Security.
- Microsoft Learn — App Control for Business.
- Microsoft Learn — AppLocker and application-control feature availability.

Limitations: Microsoft feature availability, settings and interfaces change by edition and release. Antivirus status depends on the installed provider. Application allow-listing policies should be tested on representative devices before enforcement.

Review cadence: Revalidate after major Windows releases, security product changes, significant incidents or changes to Cyber Essentials requirements, and at least annually.

This is a practical guide, not an official Cyber Essentials assessment. Certification is issued by an IASME-authorised Certification Body.

SEE YOUR ESTATE.

Prioritise risk. Remediate with confidence.

SecureX7 brings asset visibility, configuration assessment, contextual risk prioritisation, clear remediation guidance and verification into one practical cybersecurity posture platform.

Turn a malware protection checklist into an operating control

Use SecureX7 to identify configuration weaknesses across supported endpoints, understand priorities and verify corrective action.

[Start a free trial](#) · [Request a demo](#) · [Contact SecureX7](#)

www.securex7.com