Malware Protection Guide: Defensive Layer 2

# Malware Protection Guide: Defensive Layer 2

**Parent topic:** [Malware Protection Guide - Overview](malware-protection-guide-introduction.html)

## Introduction

This guide explains the types of controls that need to be implemented to form the second of three layers of defence. This guide is a sub-page to the [Malware Protection Guide](malware-protection-guide-introduction.html).

### Who is this for?

This Malware Protection information is mainly intended for in-house Ministry of Justice (MoJ) Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other MoJ bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the MoJ, will also find this information helpful.

## Defensive Layer 2: Preventing malicious code from being executed

Layer 1 might not always prevent malware from reaching the network. Assume that malware can and will reach MoJ devices at some point. The next layer of protection prevents malicious code from taking effect. The tables below outlines ways in which you can help prevent malicious code from executing.

|  |
| --- |
| Do |
| ✔ Ensure that all systems and endpoints are scanned by anti-malware software. See [Note 1](#X52fe95f57f0cc7af439a32b57dedafd1ca95ada) for more details. |
| ✔ Ensure that if you are developing a new Microsoft Windows based system, that the MoJ's Windows Defender enterprise anti-malware software for Microsoft environments is configured to regularly scan it. Contact the OST for further information on how to do this. |
| ✔ Ensure that if you require additional anti-malware scanning functionality because of a higher malware risk, or you have non-Microsoft Windows systems, then other anti-malware vendors can be considered. You must discuss your selection with the [Cyber Assistance Team](#contact-details) and the [Operational Security Team (OST)](#contact-details). See [Note 2](#X5446c47ddc2b8ff0993c96630e7b55a7748f47a) for more details. |
| ✔ If you are designing or developing a system which you expect to be at high risk of malware, you should ensure it is built with sandboxing capability in order to minimise the impact of malicious code executing on endpoints. |
| ✔ Use hardened devices including approved and assured Gold Builds. Further information can be found in the Technical Controls guide. Contact the [Cyber Assistance Team](#contact-details) for more information. |
| ✔ If you are developing or modifying networks, you should consider what protective monitoring is required. Contact the [OST](#contact-details) for details. Protective monitoring required can include Intrusion Prevention Systems (IPS) & Intrusion Detection Systems (IDS) to monitor, alert and block suspicious activity. These systems should feed monitoring data to the MoJ OST's central monitoring capability. |
| ✔ When developing new systems and services, or updating or maintaining them, ensure that you refer to the security requirements detailed in the MoJ Software Development Lifecycle (SDLC) guidance. Contact the [Cyber Assistance Team](#contact-details) for more information. |
| ✔ Ensure production environments are segregated from other systems. Prior to going live, ensure this environment is assessed against the relevant top 20 [Center for Internet Security Controls](https://www.cisecurity.org/cybersecurity-best-practices). |
| ✔ If you are configuring host-based or network firewalls, ensure inbound connections are configured as deny by default. Outbound connections should also be denied by default on network devices such as firewalls, to prevent viruses avoiding proxies when leaving the MoJ's systems. You should review these rules at least once every three months, to ensure they allow only necessary traffic. |
| ✔ Ensure that all systems have agreed maintenance windows for patching. These maintenance windows must meet the Service Level Agreement timescales outlined in the [Vulnerability Scanning and Patch Management Guide](vulnerability-scanning.html). |
| ✔ Where possible, you should enable automatic updates for operating systems, applications, and firmware. |
| ✔ Use versions of operating systems and applications which receive wide general support. This means they can take advantage of up-to-date security features, and so reduce vulnerabilities. |
| ✔ Use automated code scanning services to help identify malicious and vulnerable code, including for open source applications or services. See the Secure Development Lifecycle guidance for further information. |

|  |
| --- |
| Don't |
| ✖ Enable macros if you are using productivity suites unless there is an approved business case for doing so. For help on this point, contact the [Cyber Assistance Team](#contact-details). Macros should be disabled by default. |
| ✖ Design systems to use multiple consecutive firewalls for systems processing OFFICIAL information. The exception is where the firewalls act as a contract enforcement point between two entities that are connecting to each other. In this case, the firewalls are structural devices that help define the boundary of responsibility rather than providing security. See the [NCSC guidance](https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_5) for further information. |
| ✖ Delay implementing security patches on infrastructure when possible. See the [Vulnerability Scanning and Patch Management Guide](vulnerability-scanning.html) for further information. |

### Note 1

Important: Those who manage anti-malware software must ensure that:

* it is in a working state
* it is set to receive updates at the highest possible frequency
* it is updated automatically with the latest virus definitions and updates
* scans are scheduled regularly or as external devices are added
* any findings are reviewed, and
* any anti-malware alerts are reported to the [Technology Service Desk](#contact-details) and the [Operational Security Team (OST)](#contact-details).

### Note 2

Important: Anti-malware tools must:

* scan at least daily
* provide regular software updates
* have a Self-Protect Mode enabled
* have Clean/Quarantine capabilities
* provide regular reports and alerting to administrators
* prevent anti-malware services from being shut down without authorisation
* have defined responsibilities for maintaining, updating and reviewing the solution
* have defined test response and recovery plans to outbreaks

## Contact details

* Contact the Cyber Assistance Team for advice on protecting against malware - [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)
* Contact the Technology Service Desk to report suspected malware:Telephone: 0800 917 5148.
* Contact the Operational Security Team (OST) - [Operationalsecurityteam@justice.gov.uk](mailto:Operationalsecurityteam@justice.gov.uk)