SI.L2-3.14.2

System & Information Integrity

Malicious Code Protection [CUI Data]

"Provide protection from malicious code at designated locations within organizational systems."

Objectives

[a]

Designated locations for malicious code protection are identified.

[b]

Protection from malicious code at designated locations is provided.

Key Discussion Points

Designated Locations:
[a] requires identifying WHERE protection is deployed — endpoints, email gateways, web proxies, and network boundaries. All must be documented.

Definitions Current:
Anti-malware with outdated definitions is significantly less effective — daily or more frequent definition updates are the expected standard.

Alerts Must Be Reviewed:
Deploying anti-malware generates alerts — those alerts must be reviewed and acted on. An unreviewed quarantine report satisfies no part of this control.

Servers Included:
Workstation-only anti-malware coverage is incomplete — CUI file servers and other back-end systems must also be protected at designated locations.

Assessment Methods

EXAMINE

System and information integrity policy; configuration management policy; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings; scan results from malicious code protection mechanisms; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel installing and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility.

TEST

Organizational processes for employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting malicious code scanning and subsequent actions.

Plain English

What this control is really saying:

Viruses, ransomware, spyware, and trojans enter systems through email, web downloads, removable media, and exploited vulnerabilities. This control requires anti-malware protection at the places where malicious code can enter or execute — endpoints, email gateways, and network boundaries — with definitions kept current to detect the latest threats.

How it is used:

- Endpoint protection software is deployed on all CUI workstations, laptops, and servers — definitions update automatically at least daily.
- The email gateway scans all inbound and outbound attachments and links — malicious content is quarantined and the security team is notified.
- Anti-malware alerts are reviewed within 24 hours — infected endpoints are isolated, investigated, and remediated per the incident response plan.
- The SSP lists all designated locations for malicious code protection and documents the tool deployed at each location.

SI.L2-3.14.2

SYSTEM & INFO INTEGRITY — Malicious Code Protection [CUI Data]

Real World Example

The Scenario

Acme Defense deploys endpoint protection on workstations but not on the CUI file server. Definition updates run weekly — the last update was 47 days ago. An engineer opened an email attachment that triggered a sandbox alert, but the alert was never reviewed.

What the assessor finds

The assessor finds ransomware on the CUI file server — staged for 11 days, not yet triggered. The file server had no anti-malware. The sandbox alert from the engineer's email attachment was the only warning — it was never reviewed.

SPRS Score Impact

3.14.2 carries a point value of 5. Ransomware is the most common and costliest attack against DIB contractors — anti-malware is the first line of defense and its absence or failure to update is among the highest-impact gaps an assessor can find.

What Good Looks Like

Designated locations inventoried in SSP, endpoint protection on all CUI endpoints and servers, definitions updated at least daily, email gateway scanning enabled, alerts reviewed within 24 hours, detections trigger incident response process.

Common Gaps

What assessors actually find in the field:

✗ No endpoint protection

CUI workstations have no anti-malware software — malicious code from email attachments or web downloads executes without detection.

✗ Definitions not updated

Endpoint protection is installed but definitions have not been updated in four months — recently discovered malware families are not detected.

✗ Email gateway not scanning

The email gateway is not configured to scan attachments — malicious files reach user inboxes without inspection.

✗ Servers excluded

Anti-malware is deployed on workstations but not on CUI file servers — malware that reaches the file server is not detected.

✗ Alerts not reviewed

Anti-malware software generates quarantine alerts but nobody reviews them — infections are remediated only when the user notices symptoms.