TRINITY CYBER

Full Content Inspection (FCI) Mapping to CMMC

Solutions Brief

OCTOBER 2025

240.654.1451
info@trinitycyber.com

TRINITY CYBER

Executive Summary

Trinity Cyber's Full Content Inspection (FCI) technology provides excellent coverage for CMMC 2.0 Level 1 requirements related to network security – it excels at boundary protection and malware defense (as reflected by the "Partial" and "Yes" mappings below). Note that many Level 1 controls fall outside Trinity Cyber FCI's scope, including user access management, physical security, media handling, and other procedural controls. Trinity Cyber FCI is a powerful layer in a comprehensive compliance strategy: it significantly bolsters defenses for relevant technical controls, but organizations must implement additional measures (policies, identity management, physical safeguards, etc.) to fully meet all CMMC 2.0 Level 1 requirements.

Compliance Matrix Highlights

CMMC L1 Control	FCI Support?	Mapping & Rationale
AC.L1-3.1.20 – **External Connections** *Verify and control/limit connections to external information systems.*	**Yes**	The inline FCI service monitors all network sessions to external systems and sanitizes malicious traffic. This helps enforce security at external boundaries (e.g., malware protection for harmful connections). Further, FCI helps govern external system use – its Cloud Firewall capability provides policy control such as URL filtering and geo blocking.
SC.L1-3.13.1 – **Boundary Defense** *Monitor, control, and protect communications at external and key internal boundaries.*	**Yes**	This is a core strength of Trinity's FCI. The platform acts as an always-on security checkpoint at the network perimeter, inspecting every session entering or leaving the network. It can actively detect and neutralize threats in real time, in-line with traffic, effectively monitoring and protecting communications at external boundaries far beyond what a standard firewall or IDS provides.

SI.L1-3.14.1 – **Flaw Remediation** *Identify, report, and correct information system flaws in a timely manner.*	**Partial**	FCI mitigates risks from unpatched flaws but doesn't fix them. It detects and blocks exploit attempts for known vulnerabilities (e.g., it stops all exploits of CVEs on CISA's Known Exploited Vulnerability list), effectively providing a "virtual patch" at the network layer. However, Trinity is not a patch management system. The organization must still identify and remediate vulnerabilities in software and systems through regular patching to fully comply.
SI.L1-3.14.2 – **Malicious Code Protection** *Provide protection from malicious code (malware) at appropriate locations.*	**Yes**	FCI offers strong malicious code protection at the network gateway. It fully inspects files and content in transit and surgically removes or neutralizes malware payloads before they reach the internal network. By operating in real time across all sessions, FCI serves as an effective malware filter at the boundary (an appropriate location for such protection), satisfying this control's intent of guarding against viruses, worms, and other malicious code.
SI.L1-3.14.4 – **Malicious Code Updates** *Update malicious code protection mechanisms when new releases are available.*	**Yes**	Yes. Trinity Cyber's platform is fully managed and continuously updated by their Threat Analysis team. Trinity Cyber constantly develops and deploys new detection "formulas" (countermeasures) to address emerging threats, and fine-tune protections based on threat intel and malware analysis. This means the FCI's malware detections are always current, meeting the requirement to update anti-malware mechanisms promptly when new updates or definitions are available.

SI.L1-3.14.5 – **Security Monitoring (Scans)** *Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.*	**Yes**	FCI covers real-time scanning of incoming files, and on-demand internal scans. The service automatically scans all content from external sources in real time as it traverses the network (e.g. as users download files from the internet), thereby meeting the “real-time scan” aspect for files entering the system. As well, FCI can perform periodic at-rest scans of internal systems or files. Organizations should use endpoint anti-virus or similar tools for regular system scans, in addition to Trinity’s always-on network scanning, to fully satisfy this control.