Executive Summary

Organizations pursuing Cybersecurity Maturity Model Certification (CMMC) Level 2 must precisely scope security tooling to avoid unnecessary expansion of the Controlled Unclassified Information (CUI) boundary. Security tools that operate with elevated privileges, particularly Sophos Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Managed Detection and Response (MDR) platforms, and Identity Threat Detection and Response (ITDR) could be misunderstood and incorrectly classified as CUI Assets if configured outside of Sophos' recommendations and end user's risk tolerances.

This Product Applicability Guide evaluates the Sophos security product suite using direct technical input from Sophos Endpoint, Cloud, and XDR architects, including detailed reviews of telemetry schemas, data flows, optional features, and customer-controlled configurations.

This guide concludes that specific Sophos components, when deployed with Sophos and end user defined configurations and exclusions, function as a Security Protection Asset and do not process, store, or transmit CUI. The document also identifies features and services that must be excluded or treated separately in order to maintain defensible CMMC scoping.

---

1. Purpose, Scope, and Methodology

1.1 Purpose

This document is intended to support CMMC scoping decisions, System Security Plan classification language, assessor-facing technical justification, and internal risk and compliance review. It does not assert that Sophos tools independently establish CMMC compliance.

1.2 Methodology

This guide is based on multiple technical interviews with Sophos engineers and architects responsible for endpoint protection, cloud services, XDR and MDR platforms, and backend data pipelines. It incorporates detailed discussions of endpoint telemetry behavior, data schemas, retention models, and optional features that materially affect CMMC scope. All conclusions are limited to behavior explicitly described during those sessions.

---

2. CMMC Scoping Foundations

2.1 Relevant Definitions

Per the CMMC Scoping Guide, a CUI Asset is any asset that processes, stores, or transmits CUI. A Security Protection Asset is an asset that provides security functions and does not process, store, or transmit CUI. Security Protection Data is data generated by security tools for the purpose of maintaining or assessing security posture and does not constitute CUI.

CMMC scoping is determined by data interaction and data semantics, not by privilege level or administrative access.

This document contains confidential and proprietary information of both Client and Coalfire.

© 2026 Coalfire Systems, Inc. All rights reserved. Template only.

2.2 Framing Principle

CUI is implicated only when a product processes, stores, or transmits CUI as information. Elevated access alone does not constitute CUI processing.

---

3. Sophos Product Architecture Overview

Based on the technical interviews, the following Sophos components are relevant in CMMC-scoped environments.

Components evaluated as potential Security Protection Assets include the Sophos EDR, XDR, MDR, and IDTR; Sophos Central as the management plane; and Sophos Taegis ingestion and analytics engine when limited to security event data.

Components explicitly excluded from CUI environments include Sophos Email Security, which scans full email content and attachments; optional Live Terminal functionality that provides interactive shell access; unrestricted log collectors ingesting syslog data (such as net new, unknown files; and Network Detection and Response asset discovery scans unless explicitly disabled.

---

4. Endpoint Telemetry and Data Semantics

4.1 Nature of Endpoint Telemetry

Sophos endpoint agents collect security-relevant event data, including process execution events, file activity metadata, registry changes, network connections, authentication events, and host and user identifiers. These events are recorded locally in endpoint event journals and a subset is streamed to centralized services for detection and correlation.

The agent does not interpret file contents as business or mission information. Telemetry reflects that an event occurred, not the meaning or content of the underlying data.

4.2 Event Journaling and Local Retention

Endpoints maintain local event journals with a default retention target of approximately 90 days, adjustable based on disk allocation. When endpoints are offline or operating in enclave environments, events remain stored locally and are uploaded once connectivity is restored, with timestamps preserved for both event occurrence and upload time.

This design supports incident reconstruction without requiring continuous external connectivity.

---

5. Security Protection Data Versus CUI

5.1 Telemetry Classification

Telemetry transmitted from Sophos endpoints consists of structured security metadata such as operating system version, patch level, installed software identifiers, CVE identifiers, cryptographic hashes, event types, timestamps, and detection

This document contains confidential and proprietary information of both Client and Coalfire.

© 2026 Coalfire Systems, Inc. All rights reserved. Template only.

metadata. Even when derived from systems that process CUI, this data does not include document contents, application payloads, or controlled technical information.

As such, it qualifies as an SPA/Security Protection Data rather than CUI. SPAs that do not process, store, or transmit CUI do NOT require a separate CMMC assessment. [Slide15]

5.2 Hashing, Reputation, and Metadata Considerations

File reputation checks are performed using locally computed hashes. During reputation lookups, additional metadata such as file name, file size, and directory path may be transmitted. If customers embed controlled information in file naming conventions, that risk is introduced by customer practice rather than by the tool itself. This reinforces the importance of data handling policy and hygiene rather than reclassification of the security tool. If an organization cannot guarantee file names will not include CUI, Sophos can work to restrict file names from being collected and sent outside of the CUI boundary.

---

6. Communication and Control Planes

6.1 Agent-Initiated Communication

Endpoint agents communicate with Sophos Central using the Management Communication Service protocol. Endpoints poll or receive queued commands but do not accept arbitrary inbound connections, however this process should be verified by Sophos and end user administrators. There is no SaaS-initiated filesystem browsing, no default interactive remote access, and no unsolicited data extraction when configured according to Sophos' CUI and CMMC standards.

6.2 XDR and Analytics Data Flow

Security events are ingested into the XDR platform, normalized, correlated, and evaluated using detection logic. This processing operates on structured security events and does not reconstruct files, rehydrate user documents, or introduce semantic access to CUI.

---

7. Negative Capability Statements

Based on direct confirmation from Sophos engineers, standard endpoint and XDR configurations do not capture screen images or application payloads, perform keystroke logging, tokenize or index user documents, parse open files for business meaning, expose user sessions outside the Sophos application interface, or allow arbitrary data exfiltration.

User interaction monitoring tools are limited strictly to Sophos product interface interactions and do not monitor customer systems or operating system activity.

---

8. Optional Features Affecting Scope

8.1 Live Terminal

This document contains confidential and proprietary information of both Client and Coalfire.

© 2026 Coalfire Systems, Inc. All rights reserved. Template only.

Live Terminal provides browser-based interactive shell access with file upload and download capability. This feature can process and transmit arbitrary data, introduces potential gaps in session logging, and allows non-deterministic data handling.

In CMMC environments, Live Terminal should be disabled or treated as a cybersecurity risk rather than a Security Protection Asset.

8.2 File Submission and Sample Analysis

Suspicious files may be submitted for sandbox analysis. Automatic submission can be disabled by policy, and manual submission requires administrator action. No human analyst reviews samples by default. In CMMC environments, automatic submission should be disabled and manual submission governed by procedure, including verifying the file and its metadata will not construe CUI.

8.3 Email Security

Sophos Email Security scans full email bodies and attachments and integrates directly with Microsoft 365 and Google Workspace. Because it processes full content, policy must prohibit CUI transmission via email, especially if customers can expect CUI in scanned emails.

---

9. Network Detection, Logs, and Topology Data

9.1 Network Detection and Response

The Network Detection and Response appliance performs local machine-learning-based detection and sends only detection results rather than raw traffic. Asset discovery scans may expose network topology, which may be designated as CUI by the data owner. Asset discovery should be disabled if topology information is treated as CUI.

9.2 Log Collection

Log collectors forward syslog data as provided by the customer. Customers control which logs are forwarded. Logs containing CUI must not be transmitted to external platforms.

---

10. System Security Plan Classification Guidance

Recommended classification for CMMC documentation is as follows.

Sophos endpoint agents configured with the constraints described in this guide should be classified as Security Protection Assets. Telemetry should be classified as Security Protection Data. Email security services and Live Terminal should be disabled, or heavily restricted depending on organizational risk acceptance.

---

11. Final Determination

This document contains confidential and proprietary information of both Client and Coalfire.

© 2026 Coalfire Systems, Inc. All rights reserved. Template only.

Based on direct architectural review and confirmation from Sophos engineering leadership, Sophos endpoint and XDR components can be deployed in CMMC Level 2 environments without expanding the CUI boundary, provided that content-processing features are excluded, telemetry controls are enforced, the configuration follows Sophos' recommendations, and optional high-risk features are disabled.

When deployed under these constraints, the Sophos suite functions as a Security Protection Asset and does not itself process, store, or transmit CUI.

Regulatory Disclaimer

This document is provided for informational purposes only. Regulatory compliance is achieved through governance, policy, and process, not through technology alone.

This document contains confidential and proprietary information of both Client and Coalfire.

© 2026 Coalfire Systems, Inc. All rights reserved. Template only.