Sophos CMMC Solution Brief

This document outlines how Sophos products contribute to compliance and what configuration responsibilities lie with the customer to ensure protection.

Sophos MDR Complete and Sophos Endpoint form a comprehensive endpoint and managed detection and response solution that supports compliance with many CMMC requirements.

Note: CMMC Level 2 certification also requires full compliance with CMMC Level 1 practices. Therefore, this document includes guidance on how Sophos MDR Complete and Sophos Endpoint support both Level 1 and Level 2 requirements.

Cybersecurity Maturity Model Certification (CMMC)

How Sophos Aligns with CMMC

CMMC Levels

What is the Cybersecurity Maturity Model Certification?

The Cybersecurity Maturity Model Certification (CMMC) is the U.S. Department of Defense's framework for protecting sensitive information across the Defense Industrial Base (DIB). It builds on NIST SP 800-171 federal guidelines and introduces additional practices to address evolving cyber threats.

CMMC introduces scaled assessment requirements based on the sensitivity of the data, utilizing annual self-assessments for foundational levels and requiring independent third-party or government certification assessments for higher tiers.

If your organization handles Federal Contract Information (FCI) or Controlled Unclassified Information (CUI), achieving the appropriate CMMC level is essential to maintaining DoD contracts, and reducing risk in an increasingly complex threat landscape.

CMMC levels

Foundational

- Basic safeguarding of Federal Contract Information (FCI)
- 17 practices
- Annual self-assessment

Advanced

- Protect Controlled Unclassified Information (CUI)
- 110 practices
- Annual self-assessment or Triennial third-party assessment

Expert

- Protect Controlled Unclassified Information (CUI)
- Over 130 practices
- Government-led assessment

CMMC Domains

The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171. These domains and their abbreviations are as follows:

CMMC Domains	
Access Control (AC)	Awareness & Training (AT)
Audit & Accountability (AU)	Configuration Management (CM)
Identification & Authentication (IA)	Incident Response (IR)
Maintenance (MA)	Media Protection (MP)
Personnel Security (PS)	Physical Protection (PE)
Risk Assessment (RA)	Security Assessment (CA)
System and Communications Protection (SC)	System and Information Integrity (SI)

Sophos Control Coverage

This document provides an overview of how Sophos products and services can be leveraged to meet the CMMC requirements. It is crucial to understand that while Sophos offers a robust suite of security solutions, compliance is a shared responsibility that requires ongoing diligence and adaptation to evolving threats and regulations. Organizations mustcontinuously assess their security posture and integrate these solutions effectively to maintain compliance.

Sophos products and services are categorized as Security Protection Assets by the CMMC framework and provide security functions and capabilities to a customer's CMMC assessment scope. Specifically, Sophos helps our customers remain secure and meet CMMC control requirements. Sophos can help:

- **Protect sensitive environments without unnecessary exposure** Sophos solutions are designed to secure endpoints and infrastructure while helping avoid unnecessary expansion of the CUI boundary when configured according to best practices.
- **Focus on security signals, not sensitive content** Sophos analyzes structured telemetry such as events, hashes, and detections, not document contents or business data, supporting a defensible approach to CUI handling.
- **Gain 24/7 threat detection and response** With Sophos MDR and XDR, you get continuous monitoring, expert-led investigations, and rapid response to help reduce risk in CMMC-scoped environments
- **Deploy with control and confidence** Flexible configuration options allow you to align Sophos capabilities with your compliance strategy, risk tolerance, and operational requirements

Access Control (AC)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.1.1	Authorized Access Control	Endpoint Mgmt / XDR / ITDR	Managed endpoints are protected by Sophos Endpoint policies, and Sophos XDR/ITDR monitors for unauthorized device or identity activity. Alerts are reviewed and investigated through Sophos Central.	Authoritative account provisioning and access approval remain in IdP/IAM, HR, and system owner processes. An active access limitation mechanism would need to account for parts d-f.
3.1.2	Transaction & Function Control	Endpoint Mgmt	Sophos Application Control and Device Control restrict user access to unauthorized applications, categories, and peripheral functions on managed endpoints.	Business application authorization logic remains in the underlying applications and IAM platform.
3.1.3	Control CUI Flow	Endpoint Mgmt / XDR	Sophos Web Control, Application Control, and Device Control are configured on managed endpoints to reduce unauthorized movement of CUI via endpoints and common exfiltration paths.	Formal data flow architecture, DLP, segmentation, and egress controls may be needed outside Sophos.
3.1.5	Least Privilege	Endpoint Mgmt / ITDR	Sophos XDR and ITDR are used to detect privilege misuse, suspicious administrative actions, and risky identity conditions that would indicate least-privilege violations.	Least-privilege design and PAM enforcement are usually outside Sophos.
3.1.6	Non-Privileged Account Use	ITDR / XDR	Sophos ITDR and XDR generate detections when privileged accounts are used abnormally or when identity misuse suggests non-privileged users are performing privileged actions.	Endpoint monitoring does not replace account type enforcement in IAM/OS configuration.
3.1.7	Privileged Functions	ITDR / XDR	Privileged account activity is monitored through Sophos ITDR and XDR, and suspicious use of administrative functions is escalated for investigation and response.	Privileged access governance and approvals remain outside Sophos.
3.1.12	Control Remote Access	Endpoint Mgmt / XDR	Sophos monitors remote-access related activity on endpoints and can restrict high-risk remote administration tools via endpoint policies.	VPN/ZTNA service, remote access approval, and gateway controls are separate technologies/processes.

Access Control (AC) continued

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.1.13	Remote Access Confidentiality	Endpoint Mgmt / XDR	Sophos provides visibility into remote-session risks and protected-traffic usage on endpoints; exceptions or suspicious sessions are investigated in XDR.	Encryption of remote sessions is implemented by VPN/ZTNA/ remote-access platforms, not by Sophos alone.
3.1.16	Wireless Access Authorization	Endpoint Mgmt	Managed wireless clients are subject to Sophos endpoint policies and monitoring, supporting enforcement of approved wireless use on corporate devices.	Wireless auth/NAC/WLAN controls must be implemented elsewhere.
3.1.17	Wireless Access Protection	Endpoint Mgmt / XDR	Sophos detects risky activity from wireless-connected endpoints and provides endpoint posture and threat visibility to support wireless protection measures.	WPA2/3, NAC, AP security, and wireless segmentation remain separate controls.
3.1.18	Mobile Device Connection	Endpoint Mgmt	Sophos Device Control restricts or blocks the connection and use of mobile/removable devices on managed endpoints based on policy.	MDM/UEM may still be needed for full mobile device governance.
3.1.20	External Connections	Endpoint Mgmt / XDR	Sophos endpoint policies and XDR detections are used to identify or restrict unapproved external connections initiated from managed endpoints.	Firewall, proxy, NAC, and vendor management processes are typically also required.

Audit and Accountability (AU)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.3.1	System Auditing	Endpoint Mgmt / XDR / ITDR	Sophos Central collects endpoint, threat, and identity telemetry to create audit-relevant security records for investigation and reporting.	Enterprise log retention, immutable storage, and SIEM forwarding may be needed.
3.3.2	User Accountability	XDR / ITDR	Sophos cases and detections correlate user, device, and identity information so security-relevant actions can be traced to accountable entities where telemetry exists.	Full user attribution depends on identity integration and accurate asset ownership data.
3.3.3	Event Review	XDR	Security events generated by Sophos are reviewed as part of daily monitoring and incident triage.	Documented review frequency, roles, and escalation procedures remain organizational responsibilities.
3.3.5	Audit Correlation	XDR	Sophos XDR correlates detections across multiple data sources to support investigation of related security events.	Broader enterprise correlation may still require a SIEM/SOC workflow beyond Sophos.
3.3.6	Reduction & Reporting	XDR / ITDR	Sophos prioritizes detections and findings into dashboards, reports, and cases to reduce raw event volume into actionable information.	Formal reporting cadence and metrics should be defined in procedure.
3.3.8	Audit Protection	Sophos Central	Access to Sophos Central logs and cases is limited by role; audit data is centrally stored within the platform for authorized review.	Long-term log protection, WORM retention, and backup controls are usually outside Sophos.
3.3.9	Audit Management	Sophos Central / XDR	Sophos administrators manage alerting, logging scope, and review workflows within Sophos Central to support audit management.	Enterprise-wide audit settings outside Sophos must be managed separately.

Configuration Management (CM)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.4.2	Security Configuration Enforcement	Endpoint Mgmt	Sophos endpoint protection, web control, device control, and tamper protection policies are centrally managed and enforced on managed endpoints.	OS baselines, GPO/MDM baselines, and vulnerability exceptions are outside Sophos alone.
3.4.6	Least Functionality	Endpoint Mgmt	Sophos Application Control and Device Control are configured to reduce unnecessary functionality and software categories on managed endpoints.	Least-functionality decisions must also be implemented in OS, application, and network configuration.
3.4.8	Application Execution Policy	Endpoint Mgmt	Sophos Application Control blocks or restricts execution of unauthorized applications or software categories on managed endpoints.	Full application allowlisting may need WDAC/AppLocker or equivalent if stricter control is required.

Identification and Authentication (IA)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.5.1	Identification	ITDR	Sophos ITDR monitors identity sources and identity-linked detections to support assurance that security events can be tied to known identities.	Authoritative identity lifecycle is managed by the IdP/IAM platform.
3.5.2	Authentication	ITDR	Sophos ITDR detects suspicious authentication activity and compromised-credential indicators in the enterprise identity environment.	Authentication mechanisms themselves are provided by IdP, OS, VPN, or application platforms.
3.5.3	Multifactor Authentication	ITDR	Sophos ITDR is used to identify MFA gaps, risky sign-ins, and identity posture weaknesses in the connected identity tenant.	MFA enforcement is provided by the IdP/VPN/app, not by Sophos alone.
3.5.5	Identifier Reuse	ITDR	Sophos identity posture findings help identify poor identity hygiene conditions, including lifecycle weaknesses or risky identity configurations.	Identifier lifecycle and reuse prevention belong to IAM governance.

Incident Response (IR)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.6.1	Incident Handling	XDR / MDR	Sophos XDR provides case management, investigation workflows, and response actions to support the organization's incident handling process. Sophos MDR provides 24/7 incident detection, investigation, and response in accordance to defined plans and procedures.	Incident Response Plan with defined roles, thresholds, and playbooks is still needed.
3.6.2	Incident Reporting	XDR / MDR / ITDR / Managed Risk	Sophos detections, alerts, and cases are used to notify responsible personnel and document reportable incidents for escalation. Sophos MDR provides 24/7 incident detection, investigation, and response in accordance to defined plans and procedures.	Regulatory/contractual reporting obligations and notification procedures remain outside the tool.
3.6.3	Incident Response Testing	XDR	Sophos XDR is used during detection validation exercises and tabletops to test monitoring, triage, and response workflows.	Testing frequency and exercise documentation are organizational responsibilities.

Media Protection (MP)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.8.7	Removeable Media	Endpoint Mgmt	Sophos Device Control is configured to block or restrict removable media usage on managed endpoints handling organizational data.	Media handling, labeling, and exceptions procedures remain required.

Risk Assessment (RA)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.11.1	Risk Assessments	Managed Risk / ITDR	Sophos Managed Risk and ITDR findings are reviewed as inputs to periodic cybersecurity risk assessments.	Formal risk methodology, acceptance, and governance are organizational responsibilities.
3.11.2	Vulnerability Scan	Managed Risk	Sophos Managed Risk performs recurring external and internal vulnerability scanning, including authenticated scanning where configured.	Asset inventory completeness and scan authorization must be maintained separately.
3.11.3	Vulnerability Remediation	Managed Risk / Endpoint Mgmt	Managed Risk findings are prioritized for remediation and tracked to closure using re-scans and case workflows.	Patch deployment and exception approval workflows may be handled in separate systems.

System and Communications Protection (SC)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.13.1	Boundary Protection	Endpoint Mgmt / XDR	Sophos endpoint network protections and XDR detections are used to monitor and control malicious or unauthorized communications crossing managed endpoint boundaries.	Boundary firewalls, segmentation, and email/web gateways may be separate products.
3.13.5	Public-Access System Separation	XDR	Sophos detections on internet-facing or publicly reachable assets are reviewed to support separation and monitoring decisions for public-access systems.	Architectural separation of public systems is implemented through network/system design.
3.13.8	Data In Transit	Endpoint Mgmt / XDR	Sophos monitors suspicious network activity and protected-traffic behavior to support data-in-transit safeguards.	TLS/VPN/SSH configuration and key management are separate controls/tools.
3.13.11	CUI Encryption	Endpoint Mgmt	Sophos endpoint posture and policy visibility are used to verify required cryptographic protections are enabled where applicable on managed endpoints.	FIPS-validated crypto selection and configuration must be verified in the actual crypto product.
3.13.16	Data At Rest	Endpoint Mgmt	Sophos endpoint visibility supports verification that endpoint storage protection controls are enabled where applicable.	Disk/database/storage encryption is implemented by the underlying storage/OS/ database platform.

System and Information Integrity (SI)

Control ID	Practice Name	Sophos Product Area	SSP Implementation Statement Recommendations	Control Considerations
3.14.1	Flaw Remediation	Managed Risk / Endpoint Mgmt	Sophos Managed Risk identifies vulnerabilities and exposures, and security personnel use those findings to prioritize flaw remediation.	Patch management tooling and change control remain necessary.
3.14.2	Malicious Code Protection	Endpoint Mgmt	Sophos Endpoint provides real-time anti-malware, exploit prevention, ransomware protection, and behavioral detection on managed endpoints.	AV exclusions, exception handling, and compensating controls must be documented.
3.14.3	Security Alerts & Advisories	Endpoint Mgmt / XDR / MDR / Managed Risk	Sophos generates security alerts and exposure notifications that are reviewed and acted on by security personnel. Sophos MDR monitors threat intelligence feeds and system telemetry, responding to emerging threats and security advisories. Sophos MDR monitors threat intelligence feeds and system telemetry, responding to emerging threats and security advisories.	Alert routing, on-call, and response SLAs remain process responsibilities.
3.14.4	Update Malicious Code Protection	Endpoint Mgmt	Sophos endpoint protections are centrally updated through Sophos Central to maintain current threat-detection capability.	Update approval and outage/ change procedures remain organizational responsibilities.
3.14.5	System & File Scanning	Endpoint Mgmt / Managed Risk	Sophos performs real-time and scheduled malware scanning on endpoints, while Managed Risk performs vulnerability scanning of assets.	Broader vulnerability/ configuration scanning outside Sophos scope may still be needed.
3.14.6	Monitor Communications For Attacks	Endpoint Mgmt / XDR	Sophos monitors endpoint and related communications for attack indicators and generates detections for malicious traffic patterns.	Network IDS/IPS, email security, and firewall controls may also be needed.
3.14.7	Identify Unauthorized Use	XDR / ITDR / Endpoint Mgmt	Sophos XDR, ITDR, and Endpoint detections are used to identify signs of unauthorized endpoint or identity use. Sophos MDR detects misuse, lateral movement, and unapproved access.	Unauthorized use determination still depends on policy, asset ownership, and incident criteria.

Customer Responsibility

This matrix helps customers understand their responsibilities in configuring Sophos tools to address CMMC requirements.

Feature / Scenario	Default Behavior	CUI Risk Level	Customer Action Required	Notes
Automatic File Submission to Sophos	Enabled	High – CUI in malicious files may upload	Disable under General Settings > Malware Sample Submission	Applies when malicious files contain CUI data.
Manual Submission via Threat Graph	Enabled for Admin/Help Desk roles	Medium – File manually uploaded	Restrict roles to essential users; audit regularly	Logged in Central audit logs.
SDU Forensics Collection (-forensics=full)	Manual, local run	High – Memory content may include CUI	Avoid usage unless necessary; do not run on systems with open CUI files	File is saved locally only.
SDU Collection via Central	Enabled	Low – No memory contents	None	Safe to use; used for support diagnostics.
Threat Graph Data Submission	Enabled	Medium – Command lines may have CUI	Avoid including CUI in scripts/ commands; do not disable	Required for full Sophos MDR protection.
Sophos Endpoint Data Submission	Enabled	Medium – Includes command line args	Same as above	Required for exploit protection.
Send logs when endpoint is unhealthy	Enabled	Low – Could include system context	Accept default	Helps Sophos identify product issues.
Live Response (Remote Shell Access)	Disabled by default	Medium – Commands logged in audit	Enable with caution; implement strict access control	Audit logs maintained in Central.
Data Retention Policy	90 days	Low – Metadata, not file content	None	Data aged out automatically.
Intelix Region Configuration	Default region	Low to Medium	Set region via Account Preferences to align with compliance zones	Controls geographic file submission.
Role-Based Access Control (RBAC)	Configurable	Medium – Over-permissioned roles	Enforce least privilege, MFA, role segregation	Essential for strong governance.

Conclusion

Sophos solutions are designed to support CMMC-aligned security architectures. Achieving CMMC certification requires a combination of technology, configuration, and organizational processes. Sophos does not independently establish compliance but provides the tools and expertise to support your journey.

Core Sophos Solutions

- **MDR** – 24/7 managed detection and response
- **Intercept X** – Advanced endpoint protection
- **XDR** – Deep visibility and threat correlation
- **ITDR** - Protect against identity-based attacks
- **Sophos Central** – Unified management and reporting

For questions, please consult your Sophos Solutions Architect or Customer Success Manager.

To learn more visit Sophos.com

SOPHOS