The Beginner's Guide to CMMC Compliance with Kitecyber

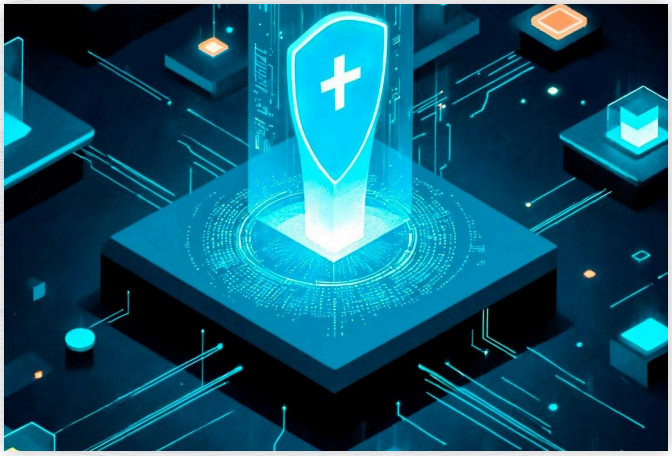
Discover how Kitecyber helps Defense Industrial Base (DIB) contractors map CMMC (Cybersecurity Maturity Model Certification) requirements, protecting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) across endpoints, networks, cloud infrastructure and third-party access.

What is CMMC

CMMC 2.0 is DoD's maturity framework for cybersecurity designed to ensure contractors protect CUI/FCI. It maps controls largely to NIST SP 800-171 (Level 2: 110 controls), with Level 1 (17 basic practices) and Level 3 (higher, for the most sensitive programs). Organisations must identify their required level per contract and implement appropriate policies, technical controls, monitoring, and assessment evidence.

Who must comply

Any organisation (prime or subcontractor) that stores, processes, or transmits CUI or handles FCI for DoD contracts, including cloud providers, vendors and other third parties in the supply chain, must meet the applicable CMMC level and produce assessment evidence.



How Kitecyber helps (summary)

Kitecyber's integrated suite features like **DLP, Data Classification, UEM, UEBA, SWG, ZTNA,** providing technical controls, monitoring, and evidence that accelerate CMMC readiness by:

1. **Discovering & classifying CUI/FCI across endpoints.**
2. **Preventing exfiltration and unauthorized sharing.**
3. **Enforcing device posture and secure configurations.**
4. **Applying least-privilege, identity-bound access.**
5. **Detecting anomalous/insider activity and providing audit logs for assessment.**

CMMC / NIST SP 800-171 Control Families → Kitecyber Mapping Table

This table maps common CUI/FCI control families (NIST 800-171 roots for CMMC Level 2) to Kitecyber products and shows how each feature helps satisfy requirements and evidence auditors expect.

CMMC / NIST Family	Mapped Kitecyber Product(s)	How Kitecyber Helps (controls & evidence)
Access Control (AC)	ZTNA, UEM, DLP	Enforce least-privilege access to CUI systems with identity + device posture (ZTNA + SSO/MFA). UEM ties devices to users and prevents shared accounts. DLP blocks unauthorized access or transfers of CUI and logs access attempts for assessments.
Awareness & Training (AT)	DLP, UEBA, Compliance Workflows	DLP incident summaries + UEBA risk trends provide training data (who misused data and how often). Workflows capture training attestations and track remediation actions.
Audit & Accountability (AU)	DLP, UEBA, SWG, ZTNA (Audit Logs)	Capture detailed, time-stamped logs of data access, transfer, and session activity. UEBA correlates events; exportable logs feed SIEM and assessment packages.
Configuration Management (CM)	UEM, DLP, Compliance Checks	UEM enforces secure baselines, detects configuration drift, and automates patching. DLP flags data exposure caused by misconfiguration; compliance checks provide evidence of baseline enforcement.
Identification & Authentication (IA)	ZTNA, UEM	ZTNA integrates with identity providers for unique IDs and MFA; UEM enforces device authentication and prevents use of unmanaged devices. Logs show authenticated sessions tied to unique users as required.
Incident Response (IR)	DLP, UEBA, Compliance Workflows, Audit Logs	DLP and UEBA detect exfiltration/abuse; automated workflows trigger containment (quarantine/wipe) and record incident timelines, actions and post-incident reports for CMMC evidence.
Maintenance (MA)	UEM, DLP	UEM schedules/automates maintenance (patching, updates) and records evidence; DLP ensures maintenance windows don't expose CUI and logs maintenance-related data events.
Media Protection (MP)	DLP, UEM	Prevents copying of CUI to removable media, enforces encryption of removable storage, and logs or blocks attempts. UEM can enforce USB control and remote wipe for lost media.
Physical Protection (PE)	UEM, DLP (device controls)	While physical controls are mostly procedural, UEM enforces device encryption and remote wipe to mitigate lost/stolen device risk; DLP blocks data persistency to physically removable media.
Personnel Security (PS)	DLP, UEBA, Compliance Workflows	DLP/UEBA help detect insider risk and inappropriate data access; workflows manage onboarding/offboarding to revoke access quickly and document actions.
Risk Assessment (RA)	DLP, Data Classification, UEBA	Data Classification reveals CUI/FCI locations enabling risk scoping; UEBA surfaces high-risk behaviours; together they inform and document risk assessments.
Security Assessment (CA)	DLP, UEM, Audit Logs	Provide objective evidence (policy enforcement reports, device posture, DLP incidents) used in self-assessment packages or by assessors.

System & Communications Protection (SC)	SWG, ZTNA, DLP	SWG inspects web/SaaS uploads and enforces TLS usage; ZTNA segments networks and provides secure tunnels to CUI resources; DLP blocks insecure or unauthorized transmissions.
System & Information Integrity (SI)	UEBA, DLP, UEM	UEBA detects compromise indicators and anomalous processes; UEM enforces AV/EDR posture and patches; DLP prevents and logs suspicious data operations.
Supply Chain / Third-Party Controls	ZTNA, DLP, SWG, UEBA	Enforce just-in-time, least-privilege third-party access (ZTNA); DLP monitors/blocks data shared with vendors; SWG limits vendor internet/app usage; UEBA monitors third-party behaviour for anomalies.

(Mapping aligns CMMC 2.0 expectations to practical technical controls and the kind of evidence auditors/C3PAOs expect.)

Practical outcomes for CMMC readiness

Scope reduction

Data Classification + DLP identify and isolate CUI to minimize systems in-scope.

Prevention of exfiltration

Endpoint + network DLP blocks common leak vectors (email, cloud/SaaS, USB).

Stronger access controls

ZTNA + UEM enforce identity + device checks and MFA for CUI access.

Faster incident response & evidence

UEBA + DLP detect and generate timelines and exportable incident packages for assessors.

Third-party oversight

ZTNA and DLP constrain and monitor vendor access to CUI.

Quick CMMC Implementation Checklist (first 30–90 days)

- Define the required CMMC level for each contract and identify CUI locations.
- Run discovery & classification to map CUI/FCI across endpoints, shares and cloud.
- Deploy UEM baseline encryption, secure configs, disable unmanaged devices, enforce patching.
- Apply DLP rules to block storage/transmission of CUI to unauthorized destinations (SaaS, email, USB).
- Implement ZTNA & SWGI to segment access to CUI systems and secure web/SaaS channels.
- Enable UEBA & logging to detect anomalous behaviour and capture audit trails.
- Create IR workflows linking DLP/UEBA alerts to containment, reporting and evidence packages for assessors.
- Extend controls to vendors enforce access via ZTNA, monitor transfers with DLP, and log third-party sessions.

KITE CYBER

Kitecyber, 691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035
Email: info@kitecyber.com
Website: www.kitecyber.com

LinkedIn Twitter YouTube