CMMC COMPLIANCE AND THE FUTUREX ADVANTAGE

Your path to scalable CMMC confidence

DIGITAL RESILIENCE

What is CMMC (Cybersecurity Maturity Model Certification)?

The CMMC is the U.S. Department of Defense's (DoD) mandatory framework that sets the cybersecurity standards contractors and their partners must meet to handle government data across the Defense Industrial Base (DIB).

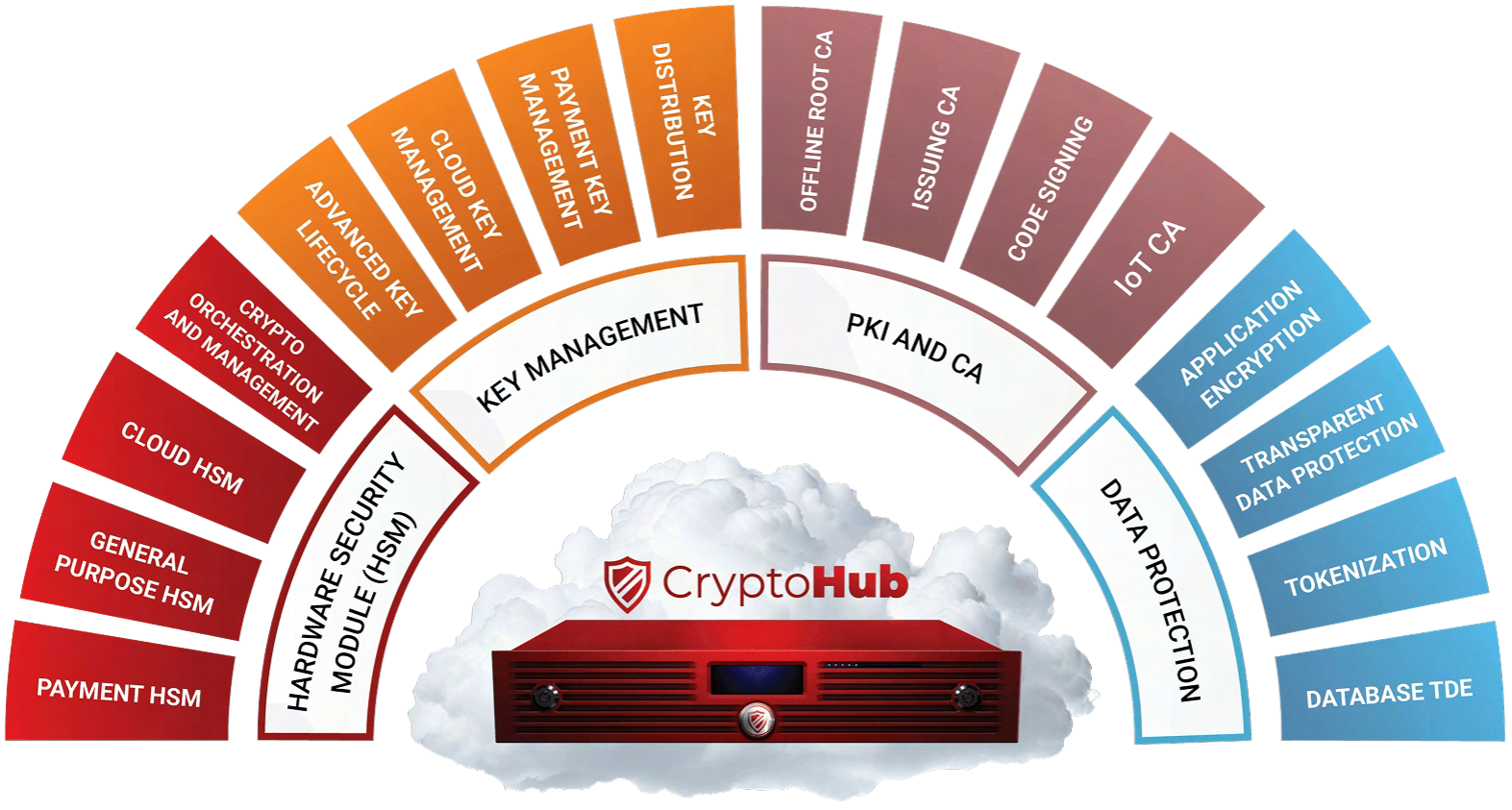
CryptoHub's added value to solve CMMC challenges

The CryptoHub platform scales to protect all workloads and environments. It supports ongoing compliance, auditing, incident response, and key management, strengthening cybersecurity resilience as a versatile, scalable cryptographic foundation for broad, continuous CMMC compliance.

CMMC Control	Requirement	CryptoHub Implementation	How Futurex CryptoHub Provides a Solution
RA.L3-3.11.2	Vulnerability scanning and remediation.	Integration with security tools and platforms.	Monitors encryption keys and cryptographic settings for vulnerabilities, enabling quick remediation.
IR.L2-3.6.1/3.6.2	Incident response and reporting.	Real-time audit logs and alerts.	Detects and alerts on unauthorized key access or crypto operations, facilitating rapid incident response.
CM.L3-3.4.1	Configuration management.	Policy enforcement and key lifecycle management.	Controls and audits changes to cryptographic configurations securely and transparently.
MP.L3-3.8.5	Media access controls and protection.	Restricted key access for media decryption.	Ensures only authorized users can decrypt CUI on removable or portable media.
AC.L3-3.1.17	Remote access protection.	Secure key handling with IdP integration.	Enforces strong authentication and authorization for cryptographic operations on remote devices.
PE.L3-3.7.5	Physical protection of equipment.	FIPS 140-3 Level 3* validated HSM hardware.	Provides tamper-resistant, physically secure cryptographic key storage.
SI.L3-3.14.1	System and communications protection.	Hardened cryptographic services across environments.	Ensures data integrity and secure communications using robust cryptography aligned with NIST standards.
SC.L3-3.13.11	Cryptographic protection for mobile devices	Key management for mobile and endpoint encryption.	Supports secure encryption and key control for mobile devices accessing or storing CUI.
AU.L3-3.3.4	Audit record retention and protection.	Immutable, secure audit logs.	Maintains long-term protected audit trails for cryptographic activities useful for regulation and forensic reviews.

* Pending

CryptoHub: The Multi-Purpose Unified Platform



1. **Enterprise-wide encryption and key management:** CryptoHub centrally manages encryption keys and enforces cryptographic controls across cloud apps, file shares, email, databases, and on-premises systems, delivering consistent end-to-end protection of CUI and FCI in transit, at rest, and in backups. It also supports application-layer encryption and tokenization to secure sensitive data throughout its lifecycle.
2. **Hybrid and multi-cloud compliance:** CryptoHub supports secure key management across AWS, Azure, private clouds, SaaS, and legacy applications, enabling Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) models. This flexibility ensures compliance control regardless of where the data resides.
3. **Scalable audit readiness and automated compliance reporting:** Automated collection and retention of cryptographic logs streamline CMMC audits, whilst continuous monitoring and real-time alerts enable proactive incident response and ongoing compliance validation.
4. **Flexible deployment models:** CryptoHub can be deployed on-premises, in the cloud, or hybrid environments, adapting to evolving DoD and CMMC demands.
5. **Data sovereignty and residency controls:** The platform enforces geographic key storage restrictions to comply with ITAR, EAR, CMMC, and regional data protection laws.
6. **Integration with security ecosystems:** CryptoHub integrates seamlessly with access management, SIEM, endpoint protection, and DLP tools, forming a core component of comprehensive CMMC/DFARS security and compliance frameworks.

Spotlight on how Google Workspace CSE addresses CMMC compliance

The CMMC mandates standardized data protection controls, especially for cloud platforms like Google Workspace handling CUI. Rooted in NIST SP 800-171, these controls apply at Levels 2 and 3 whenever Google Workspace stores, processes, or transmits CUI for Defense contracts.

Key CMMC requirements emphasize encryption, access control, auditability, and secure configuration, all of which must be properly configured and enforced on Google Workspace to protect DoD data..

CMMC Control	Requirement	Google Workspace Implementation	How Futurex CryptoHub Provides a Solution
SC.L2-3.13.8	Encrypt CUI in transit	TLS 1.2+, MTA-STS, context-aware access	Acts as the external key service for CSE ensuring data is encrypted before leaving the client's browser, protecting CUI end-to-end in transit.
SC.L2-3.13.16	Encrypt CUI at rest	AES encryption at rest, CSE for files	Provides FIPS 140-3 Level 3* validated HSM-based key management that controls keys used by CSE, securing CUI at rest across all Google Workspace assets.
MP.L2-3.8.9	Encrypt CUI in backups/storage	Cloud backup encryption	Ensures keys used to encrypt CUI backups remain under customer control through CryptoHub; the same encryption keys protect backup data managed securely via CryptoHub.
SC.L2-3.13.10	Cryptographic key mngmt	CSE + third-party key manager	Full lifecycle key management (generation, rotation, revocation), BYOK support, and secure storage of encryption keys in validated CryptoHub HSMs, empowering customers with exclusive key access.
AC.L2-3.1.5 / 3.1.2	Restrict access to CUI	MFA, RBAC, DLP	Integrates with enterprise identity providers to enforce strong access control policies, enabling CryptoHub to restrict key usage only to authorized users based on business need-to-know.
AU.L2-3.3.x series	Logging and reporting for CUI access	Workspace logging, Access Transparency	Maintains immutable audit logs for all key activities and cryptographic operations, providing evidence and transparency necessary for CMMC assessments and incident response.
MP.L2-3.8.x series	Prevent unauthorized data transfer/sharing	DLP, sharing controls	In combination with Google Workspace DLP, CryptoHub's key control ensures data remains protected by encryption keys that unauthorized entities cannot use, preventing unauthorized disclosure.

Request a Futurex Briefing

Try CSE Free for 30 Days

* Pending

FUTUREX

FUTUREX.COM

For over 40 years, Futurex has been an award-winning leader and innovator in the encryption market, delivering uncompromising enterprise-grade data security solutions. Over 15,000 organizations worldwide trust Futurex to provide groundbreaking hardware security modules, key management servers, and cloud HSM solutions.

Futurex is headquartered outside of San Antonio, Texas, with regional offices worldwide and over a dozen data centers across five continents and delivers unmatched support for its clients' mission-critical data encryption and key management requirements.

864 Old Boerne Road,
Bulverde, Texas 78163