CMMC Overview

Secure Your Data and Simplify CMMC Level 2 and Level 3 Compliance with RackTop

Securing sensitive data and maintaining compliance with the Cybersecurity Maturity Model Certification (CMMC) standards are critical priorities for defense contractors. Mandated by the United States Department of Defense (DoD), CMMC Levels 2 and 3 set rigorous cybersecurity requirements aimed at protecting Controlled Unclassified Information (CUI) from increasingly sophisticated threats.

CMMC Level 3 builds upon the 110 controls of CMMC Level 2 by adding 24 additional, more advanced controls focused on Advanced Persistent Threats (APTs). Level 3 requires rigorous security measures, including advanced access controls, network segmentation, and incident response capabilities, making RackTop's BrickStor Secturity Platform (SP) the ideal solution for your data whether it's on premises or in the cloud.

Achieving and maintaining compliance at these levels is essential, as DoD contracts frequently require certification, directly influencing your organization's ability to compete, operate effectively, and safeguard sensitive data. Non-compliance or breaches in data security can disrupt critical supply chains, result in substantial financial and reputational losses, and threaten future contracting opportunities.

RackTop's BrickStor SP is specifically designed to streamline compliance with both CMMC Level 2 and Level 3. BrickStor goes beyond NIST 800-171 standards, offering advanced data security controls, comprehensive data protection, and advanced threat prevention for unstructured data. BrickStor aligns precisely with required controls, making self-assessments or third-party assessments quick, easy, and efficient, ensuring continuous compliance and robust data security.

Learn How BrickStor SP Addresses Critical CMMC Controls

Access Control (3.1)

3.1.2 – Access Enforcement
BrickStor employs granular access controls down to the file and integrates with centralized identity services (Active Directory/LDAP) + ABAC to provide strict access control enforcement over CUI data.

3.1.4 – Separation of Duties
BrickStor includes features that enable organizations to create a separation of duties, thereby protecting security objects and logs from manipulation or deletion. ImmutaVault™ and Cybersnaps ensure data owners can prevent data from being changed or deleted prematurely.

3.1.5 – Least Privilege
Enabling least privilege policies with BrickStor is easy through its integration with Active Directory and LDAP for system administration and file access. Accounts can be grouped to establish the privileges and permissions afforded to the user.

3.1.6 – Least Privilege – Privileged Accounts
BrickStor's active defense and user behavior auditing capabilities enable organizations to scrutinize the use of privileged accounts and enforce the use of non-privileged accounts when such access is not needed.

3.1.7 – Least Privilege – Privileged Functions
Active defense and user behavior auditing provide alerts on the misuse of privileged accounts, as well as monitoring all privileged account actions.

3.1.8 – Unsuccessful Login Attempts
BrickStor enables organizations to specify behaviors for unsuccessful login attempts.

03.1.9 – System Use Notification
Organizations can display a customized system use notification for administrators.

03.1.11 – Session Termination
Organizations can customize the session termination behavior for administrative and user sessions.

Audit and Accountability (3.3)

3.3.1 – Event Logging
BrickStor logs all file and permission activity through user behavior auditing, while the system audit logs all changes made by system administrators.

3.3.2 – Audit Record Content
The user behavior audit log includes the timestamp, user account, client IP, file operation, and complete file path. Similarly, the system audit log contains the timestamp, admin account, function, settings, and results.

3.3.3 – Audit Record Generation
BrickStor enables auditing on a per-dataset basis with indefinite retention. Logs can be forwarded to a centralized logging facility.

3.3.4 – Response to Audit Logging Process Failures
The health service in BrickStor alerts administrators through emails or webhooks when an audit service fails or if space is filling up for audit logs on each BrickStor deployment.

3.3.5 – Audit Record Review, Analysis, and Reporting
BrickStor features a robust user behavior auditing and analysis interface in its Hub graphical user interface (GUI). The Hub enables authorized users to conduct in-depth analysis of file activity, allowing them to filter by specific users, client IPs, files, operation types, or even off-hours activity.

3.3.6 – Audit Record Reduction and Report Generation
Integrated reporting within the Hub enables administrators to easily generate audit reports and summarize user behavior activity in a meaningful way, highlighting issues, discrepancies, and anomalies.

3.3.7 – Time Stamps
NTP-enabled synchronized timestamps ensure log accuracy and integrity.

3.3.8 – Protection of Audit Information
Immutable, replicated snapshots guard against log tampering or deletion. ImmutaVault's separation of duties provides extra protection for audit and compliance-sensitive information. Vaults can be configured with minimum retention times that cannot be reduced, and the data is isolated to create a virtual airgap within each system.

Identification and Authentication (3.5)

3.5.1 – User Identification and Authentication
BrickStor enforces the use of unique identifiers and accounts. Active defense provides alerts on the use of shared accounts for administrative functions.

3.5.3 – Multi-Factor Authentication
BrickStor supports multi-factor authentication when logging into the Hub.

3.5.4 – Replay-Resistant Authentication
All authentication mechanisms employed by BrickStor are replay-resistant.

3.5.7 – Password Management
BrickStor will connect to centralized authentication and identity providers. However, if an organization chooses to use local accounts, BrickStor will enable the organization to create password rules and policies for local accounts.

3.5.11 – Authentication Feedback
BrickStor does not provide information that would allow unauthorized individuals to compromise authentication mechanisms through failed authentication information.

3.5.12 – Authenticator Management
BrickStor does not deploy with any default authenticators, ensuring that default authentication or generic accounts cannot be exploited through well-known passwords.

Incident Response (3.6)

3.6.1 – Incident Handling
BrickStor includes an incident management workflow in the Hub that can be integrated into the organization's incident management applications and framework. BrickStor's incident management workflow captures a detailed and attributable log of actions and remediations taken in response to the incident. The incident information can be exported as a report in PDF format.

3.6.2 – Incident Monitoring, Reporting, and Response Assistance
BrickStor automatically creates an incident for each event as well as an attributable list of actions. This information can be forwarded in real-time via email and webhooks to other systems. This enables organizations to monitor and document incidents accurately. All information related to each incident can be retained indefinitely and exported into various report formats.

Media Protection (3.8)

3.8.3 – Media Sanitation
Organizations can utilize the Federal Information Processing Standards (FIPS) 140-3 crypto erase functions compliant with NIST media purge standards for reuse and disposal.

3.8.5 – Media Transport Protection
BrickStor utilizes dual-layer FIPS 140-3 encryption for both hard drives and flash drives during physical transport.

3.8.9 – System Backup – Cryptographic Protection
BrickStor utilizes FIPS-validated AES-256 encryption to safeguard snapshots and backup data. Keys can be stored in a protected key manager or an external KMIP-compliant key manager.

System and Communications Protection (3.13)

3.13.8 – Transmission Confidentiality and Integrity
BrickStor employs encryption for data at rest and in transit. Data at rest is encrypted with up to two layers of FIPS 140-3 AES-256 encryption without impacting performance. BrickStor supports Transport Layer Security (TLS) and encrypted protocols for SMB, NFS, and S3, ensuring data in transit remains secure.

3.13.10 – Cryptographic Key Establishment and Management
BrickStor can leverage its internal key manager or an external KMIP-compliant key manager. Organizations can establish key rotation policies for BrickStor to enable the automatic rotation of cryptographic keys in accordance with their policies and regulations.

3.13.11 – Cryptographic Protection
BrickStor utilizes FIPS 140-3 validated cryptographic modules.

System and Information Integrity (3.14)

3.14.3 – Security Alerts, Advisories, and Directives
RackTop distributes timely advisories and updates regarding vulnerabilities that can affect BrickStor users. Advisories provide appropriate workarounds and software updates.

3.14.6 – System Monitoring
BrickStor's active defense capabilities enable organizations to monitor suspicious file activity in real time as well as indicators of attack and lateral movement. BrickStor alerts on probing activity, the attempted or successful use of weak protocols, and shared accounts. The activity is all recorded in audit logs, and organizations can subscribe to alerts.

3.14.8 – Information Management and Retention
BrickStor's data protection policies can be configured by organizations to facilitate the retention and management of data in accordance with policies and regulations. These data protection policies ensure that data is retained for as long as needed and no longer. Organizations can report on the policies and their implementation for each dataset.

Learn more at www.racktopsystems.com/solutions/cmmc-ready/