RAPID7

SOLUTION BRIEF

ACHIEVING CMMC 2.0 COMPLIANCE WITH COMPREHENSIVE CYBERSECURITY SOLUTIONS

Powered by Rapid7 to Enhance Security, Streamline Processes, and Mitigate Risks for Defense Contractors

In the evolving cybersecurity landscape, protecting sensitive information—particularly within the defense sector—is paramount. The Cybersecurity Maturity Model Certification (CMMC), introduced by the U.S. Department of Defense (DoD), sets stringent standards for contractors and subcontractors handling Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). CMMC aims to protect DoD data against cyber threats through a tiered model of compliance levels.

Achieving CMMC 2.0 compliance involves implementing security controls across systems and networks. Rapid7 simplifies this process by providing the tools necessary to meet CMMC's 2.0 requirements, focusing on access management, incident detection and response, vulnerability management, and risk governance mandate to minimize attack surfaces.

UNDERSTANDING CMMC 2.0 COMPLIANCE

CMMC 2.0 is structured into three maturity levels, each with increasing requirements to protect DoD data:

- **Level 1: Foundational** – Basic security practices to protect Federal Contract Information (FCI).
- **Level 2: Advanced** – Aligned with NIST SP 800-171 to protect Controlled Unclassified Information (CUI).
- **Level 3: Expert** – Based on the advanced practices outlined in NIST SP 800-172, focusing on advanced cyber threat protections.

Each level builds upon the previous one, requiring more advanced practices like continuous monitoring, incident detection, and risk management.

Self-Assessments and Certification

CMMC 2.0 introduces flexibility for compliance assessments:

- Level 1: Organizations can conduct annual self-assessments.
- Level 2: Some organizations handling non-prioritized CUI can also perform self-assessments, while third-party certification is required for prioritized CUI.
- Level 3: Third-party audits are mandatory.

This reduces the burden on organizations and allows smaller contractors to align more easily with compliance requirements.

Flexibility of Plans of Action & Milestones (POA&Ms)

CMMC 2.0 permits organizations to address certain gaps in compliance through approved POA&Ms, providing a structured timeline for remediation. This flexibility ensures that compliance is achievable without delaying operational capabilities.

RAPID7'S SUPPORT FOR CMMC 2.0 COMPLIANCE

Rapid7 helps organizations meet CMMC requirements by integrating critical security practices and providing continuous monitoring and security posture assessment. Rapid7 supports CMMC compliance across these key areas:

Access Management and Identity Protection

- Role-Based Access Control (RBAC): Limits access to resources based on user roles, reducing unauthorized access.
- Multi-Factor Authentication (MFA): Adds an extra layer of security by requiring multiple verification methods.
- Privileged Access Management (PAM): Controls access to critical systems and provides detailed logging and auditing.

These capabilities enforce least-privilege access and robust authentication measures, foundational to Level 1 and Level 2 compliance.

Continuous Monitoring and Incident Detection

- Real-Time Monitoring: Aggregates data across the environment to detect anomalies early and prevent threats from escalating.
- Vulnerability Management: Automated scans help identify and fix system weaknesses before attackers exploit them.
- Incident Response Integration: Automates and integrates with incident response workflows to ensure quick containment and mitigation.

These solutions address the requirements for real-time monitoring and incident management, particularly critical for Levels 2 and 3.

Risk Management and Governance

- Risk Assessment: Continuously evaluates cybersecurity posture, helping prioritize actions based on risk.
- Governance: Ensures consistent security practices across the organization and compliance with internal frameworks.
- Audit and Reporting: Simplifies compliance reporting for CMMC 2.0 audits.

These features support strong risk management practices required for Level 2 and advanced practices for Level 3.

EXPECTED OUTCOMES

Streamlined Compliance

Automation and integration simplify achieving and maintaining compliance.

Improved Security Posture

Continuous monitoring and vulnerability management strengthen security and align with CMMC 2.0 standards.

Faster Incident Detection and Response

Real-time monitoring and automated incident response reduce the impact of security threats.

Comprehensive Risk Management

Continuous risk assessment helps proactively address vulnerabilities.

Simplified Audits

Built-in reporting makes it easier to demonstrate compliance during audits.

THE BOTTOM LINE

As the defense sector faces increasingly sophisticated cybersecurity threats, CMMC 2.0 compliance is crucial for safeguarding sensitive DoD data. Rapid7 equips organizations with the tools to meet CMMC's cybersecurity requirements—from access management and incident detection to continuous monitoring and risk governance.

By adopting Rapid7, organizations can achieve and maintain CMMC 2.0 compliance, strengthen their security posture, and mitigate risks, ensuring they meet the stringent standards set by the DoD.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight