SOLUTION BRIEF

A Clear Path to CMMC with Fortinet

How to Meet All Levels of the U.S. Department of Defense's New Security Framework

Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) will regulate how every organization working in some capacity for the U.S. Department of Defense (DoD) maintains adequate cybersecurity controls.

Rather than take a piecemeal approach to implementation, IT teams should invest in tools that satisfy multiple requirements at once, standardizing on modern, automated cybersecurity technology. The Fortinet Security Fabric, spanning security-driven networking, dynamic cloud security, artificial intelligence (AI)-driven security operations, and zero-trust network access, covers multiple requirements at all CMMC levels—all in the same solution set.

Introduction

The Cybersecurity Maturity Model Certification (CMMC) is intended as a comprehensive framework for how cybersecurity solutions are implemented across more than 300,000 companies involved in the U.S. defense industrial base supply chain. CMMC v1.0[1] was released on January 31, 2020, and is the U.S. Department of Defense's (DoD) stepped-up requirement for keeping DoD information accessed by or housed in contractors' technology environments secure.

Previously, contractors supporting DoD had responsibility for assessing and self-certifying their success implementation, monitoring, and maintaining the security of any sensitive DoD information stored or accessible from their IT systems. The big change with CMMC is that the DoD will require third-party-governed assessments of how those contractors comply with best practices intended to protect data from cyber adversaries and prevent successful breaches. Details on how assessments will be conducted are still forthcoming as of July 2020, but all DoD contractors must understand the CMMC's technical requirements and prepare for certification, or risk eligibility to participate in DoD contracts, each of which will be tied to one or more CMMC levels.

Specifically, CMMC includes five certification levels intended to highlight a company's cybersecurity maturity and resilience levels—and therefore, a reflection of how effectively it can protect sensitive government information. Fortinet solutions for government are well-positioned to meet CMMC standards at all levels.

The 5 Levels of CMMC Certification

The CMMC combines cybersecurity standards and guidance culled from multiple government frameworks including but not limited to NIST 800-53 and the NIST Cybersecurity Framework, and will soon become incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) and used as a requirement for contract awards. Version 1.0 of the guidance divides cybersecurity readiness into five levels, each with successively more stringent requirements.

Levels 1 and 2 focus primarily on basic and intermediate cyber hygiene, while Level 3 addresses full protection of controlled unclassified information (CUI). Levels 4 and 5 add requirements for reducing the risk from advanced persistent threats (APT) and automated response capabilities. Each level of CMMC addresses 17 domains, from access control and access management to situational awareness and information integrity. Each of the domains further includes processes, capabilities, and practices reflecting the requirements at each level, 1-5.

Preparing for CMMC

The right framework, processes, and technology investments can smooth the path to CMMC. This is where the Fortinet Security Fabric excels.

Assessing your current capabilities compared to CMMC level requirements you need to satisfy includes:

- Making a list of security processes and tools you currently use that process, access, or store sensitive government information
- Mapping all of those resources to requirements in the CMMC's 17 domains. It's a good practice to use well-known standards tied to the CMMC as guides; NIST's Self-Assessment Handbook[2], for example, details certification requirements for NIST SP 800-171 Rev. 1, which corresponds to CMMC Level 3
- Using the list and map to identify and analyze gaps that need to be addressed for CMMC requirements

Installing a next-generation firewall such as the FortiGate provides organizations with application control, intrusion prevention, web filtering, SSL inspection, and automated threat protection. The FortiGate significantly improves overall network visibility, addressing many controls and domains across all levels of CMMC, including access control and incident response.

CMMC Levels 1-2 (Basic to Intermediate Cyber Hygiene)

Many companies will find that they are further along in meeting CMMC standards than they may have thought, especially at Levels 1 and 2.

Level 1 requirements include antivirus and incident response. Level 2 requirements include awareness and training, risk management, security continuity, and backups.

Installing a next-generation firewall (NGFW) such as the FortiGate provides organizations with application control, intrusion prevention, web filtering, SSL inspection, and automated threat protection. The FortiGate significantly improves overall network visibility, addressing many controls and domains across all levels of CMMC, including access control and incident response.

Fortinet Recommends:

- **FortiGate**—FortiGate enterprise firewalls provide a plethora of functionality from traffic filter to protect an organization from external and insider threats, to VPN remote access, and even switch and wireless controlling. A multifunction network device built on a security platform, FortiGates help mission partners comply with around 50% of all Level 1 through 5 controls and thus is the perfect platform around which to build a CMMC-compliant architecture.

CMMC Level 3 ("Good" Cyber Hygiene)

Level 3 requirements include compliance with NIST SP 800-171, multi-factor authentication, and the ability to manipulate how and where devices connect.

Fortinet Recommends

- **FortiAuthenticator**—FortiAuthenticator provides services that are key in creating effective security policy, strengthening security by ensuring only authorized users at the right time can access CUI data. Most importantly, FortiAuthenticator has the ability to transparently identify network users and enforce identity-driven policy critical to zero-trust security posture as well as integrate two-factor authentication into network systems.
- **FortiNAC**—FortiNAC assists with bring-your-own-device (BYOD) policies and limits where devices can go on the network. FortiNAC also provides automated response to speed the reaction time to suspicious events at the access layer.

CMMC Levels 4-5 (Proactive Cyber Controls and Advanced Cyber Protection)

The higher levels of CMMC require more integration, automation, and customization. Level 4 requirements include network segmentation, detonation chambers, mobile device inclusion, use of DLP technologies, assessment of supply chain risks, and threat hunting. Level 5 requirements include a full-time (24/7) security operations center (SOC), device authentication, cyber maneuver operations, real-time asset tracking, and the ability to provide custom protections.

Fortinet Recommends

- **FortiSIEM**—Powered by enhanced discovery capabilities, FortiSIEM can seamlessly collect a rich variety of performance and availability metrics to help investigators hunt for threats from zero-day malware. FortiSIEM can also alert when the metrics are outside of normal profile and can correlate such violations with security issues to create high-fidelity alerts.
- **FortiSOAR**—FortiSOAR aggregates alerts in one place while enriching them with added context to speed investigations. FortiSOAR streamlines simple SOC tasks like alert ingestion, prioritization based on severity levels, assigning tasks, and subroutines, and automates more complex exchange-to-exchange (E2E) tasks such as triage, enrichment, investigation, and remediation, cohesively centralizing the security processes by automatically correlating alerts from across a security stack into a single incident.

Summary: Best Practices

Implementing a true Security Fabric approach can solve many CMMC requirements at once—and harden your security posture overall.

- The Fortinet Security Fabric enables access to multiple sources of data, powered by automation, machine learning, and a range of advanced capabilities. This helps organizations close gaps in CMMC readiness, improve cyber operations overall (both NOC and SOC), and future-proof teams to prevent new or persistent threats even with a rapidly expanding threat landscape and increasingly onerous compliance requirements.
- Security teams should also focus on solutions that integrate well with those from other vendors, especially those with typically open and well-documented application programming interfaces (APIs).
- Teams should also consider professional services or integration to help with various aspects of CMMC compliance, including implementing a combination of automation and human intervention and decision-making.

> *"While it may seem costly to meet the extensive CMMC requirements, the judicious buyer will recognize that the right product can satisfy multiple requirements across all five levels. Organizations seeking CMMC readiness should invest in modern, automated cybersecurity tools like FortiGate, which receive continuously updated threat data."*
>
> – Jim Richberg, CISO, U.S. Federal Government, Fortinet

[1] Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification Website

[2] Patricia Toth, "NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in

FORTINET

www.fortinet.com

February 9, 2021 11:41 AM

709217-A-0-EN

D:\Fortinet\2020 Old templates\Image Graphics\898628 - Typo in CMMC assets\sb-a-clear-path-to-cmmc-292021\sb-a-clear-path-to-cmmc-292021