Easing the Path to CMMC

Beginning this fall, both large integrators with many Defense contracts under their belt and small businesses vying for their first subcontract will be required to prove that they meet the security requirements specified by the Department of Defense.

This new certification, called the Cybersecurity Maturity Model Certification (CMMC), is an effort to ensure that every organization working in some capacity for the Defense Department has adequate cybersecurity controls in place for the level of controlled unclassified materials it processes. That could be a large prime contractor working on a classified project or a landscaper with access to the schematics of a Naval base.

Of course, those two contractors don't require the same level of security, and the CMMC accounts for that with five levels of maturity. Katie Arrington, special assistant for cyber, Office of the Assistant Secretary of Defense for Acquisition, speaking at an event in March, said the goal is for CMMC to be cost-effective and affordable for even the smallest businesses to implement at the lower CMMC levels.

Preparing for certification

The CMMC consists of five progressively more comprehensive levels, and many companies may be further along in achieving Levels 1 and 2 than they realize. Attaining higher levels, however, may require a more integrated approach to network security—one that benefits from automation and an ongoing infusion of cyber threat intelligence.

The Basics of CMMC

The CMMC, which combines cybersecurity standards and guidance from multiple government regulations, will soon become incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) and used as a requirement for contract award.

The CMMC divides cybersecurity readiness into five levels, each with successively more stringent requirements. Levels 1 and 2 focus on basic and intermediate cyber-hygiene. Level 3 aims to fully protect Controlled Unclassified Information (CUI). Levels 4 and 5 add reducing the risk of Advanced Persistent Threats (APTs).

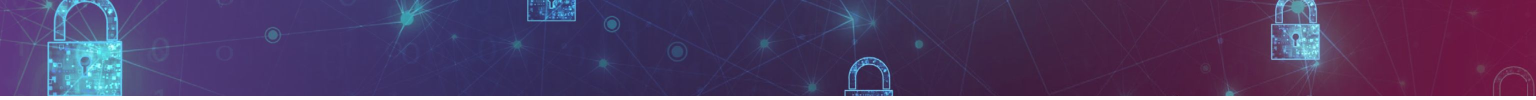
Within each level, the CMMC addresses 17 domains, focusing on such areas as Access Control, Access Management, Configuration Management, Incident Response, Personnel Security, Situational Awareness, Risk Management and System and Information Integrity. Each domain consists of a set of processes, capabilities and practices across the five levels.

"CMMC provides the tools to buy down the risk to make cyber work for you in as secure of an environment as possible," said Kate Arrington, special assistant for cyber, Office of the Assistant Secretary of Defense for Acquisition. "It's the start, but we have a long way to go."

Satisfying these new requirements can be challenging, but the right framework, processes and technology can smooth the path. Fortinet can aide in satisfying these requirements and help to ensure compliance in the CMMC domain.

The first step is assessing your current capabilities compared to the CMMC requirements you need to satisfy. Make a list of all of the security processes and tools you currently use, especially technology and applications that create, process or store sensitive government information. Map all resources to the requirements in CMMC domains and practices. Consider using NIST's Self-Assessment Handbook—NIST Handbook 162; it details certification requirements for NIST SP 800-171 Rev. 1, which corresponds to CMMC Level 3.

The result of this assessment should clearly show the gaps you need to address. You can often resolve those gaps, especially at lower levels, with the right cybersecurity tools. For example, installing a next-generation firewall like the Fortinet FortiGate provides organizations with application control, intrusion prevention, web filtering, SSL inspection and automated threat protection. It significantly improves network visibility, eliminating uncontrolled blind spots. This one product alone addresses more than a dozen controls and several domains,



including access control and incident response, across all levels of the CMMC.

Satisfying requirements at higher levels of the CMMC typically requires more resources and more customization. One option is adding additional security tools to satisfy more requirements. For example, adding products that address access, client, application, cloud, sandbox and other types of security to a next-generation firewall can create a full security fabric that will bring any organization closer to certification.

To attain even higher levels or satisfy more complex requirements require more integration, automation and customization. It might make sense, for example, to implement a series of fully automated solutions supplemented with additional threat intelligence that is customized for a particular set of requirements.

"Professional services and integration with other technologies can help you achieve a Level 4 or 5 status, especially when you incorporate a combination of automation and human intervention and decision-making," said Felipe Fernandez, director of federal systems engineering at Fortinet.

With all of these capabilities in place, it should be much easier to meet CMMC requirements. Take the Incident Response domain, one of CMMC's 17 domains. Capabilities across the five maturity levels in the domain include escalating capabilities around:

- Planning incident response
- Detecting and reporting events
- Developing and implementing a response to a declared event
- Performing post incident reviews
- Testing incident response

With the right combination of automated technologies, threat intelligence and human decision-making, companies should be able track an incident from the time it occurs to closure. Within the Fortinet Security Fabric, that would include the FortiGate firewall, FortiSIEM multivendor incident and event management solution and FortiSOAR security orchestration, automation and response.

This strategy can work for most areas of CMMC. Audit & Accountability is another example. In this case, achieving Level 2 requires little more than creating and retaining a system of logs and records that improves monitoring, analysis and investigation. Achieving Level 3, however, requires the ability to collect audit information into one or more essential repositories, and getting to Level 5 requires being able to automate analysis of audit logs and the identification of non-compliant IT assets. Tools like FortiSIEM and FortiSOAR linked through a unified security platform or fabric can provide the type of automated machine learning required to review logs and act on critical indicators in an automated fashion.

CMMC best practices

When you choose your technology, focus on products that integrate well with those from other vendors, which typically have open and well-documented APIs, work well with your existing systems, and can integrate ongoing threat intelligence data.

And consider implementing a security fabric approach to ensure that your security becomes more integrated and effective, even if you are upgrading your security infrastructure incrementally over time.

"With a security fabric, you'll be getting multiple sources of data, which provide a broader insight into what's normal, and by implication, what's not normal," explained Jim Richberg, former federal executive and field CISO at Fortinet. "If you can add automation, machine learning and other advanced capabilities to that, you'll know what's abnormal but benign, versus what's abnormal and malicious or potentially harmful. The more integrated data you have, the better your insight—and it becomes more actionable."

While it may seem costly to add the capabilities required to meet CMMC requirements, that's not always the case. The goal, Richberg said, is to make sure that everything you add to your environment satisfies multiple requirements. By standardizing on modern, automated cybersecurity tools, especially those that receive continuously updated threat data, you'll get the biggest bang for your buck.

While the requirement won't take effect for several months, Arrington said that contractors should start preparing now. "If you have DFAR 252.204.7012 in your contract and you are self-attesting [that you are secure], you should … have these controls today."