vArmour

CMMC SOLUTION BRIEF

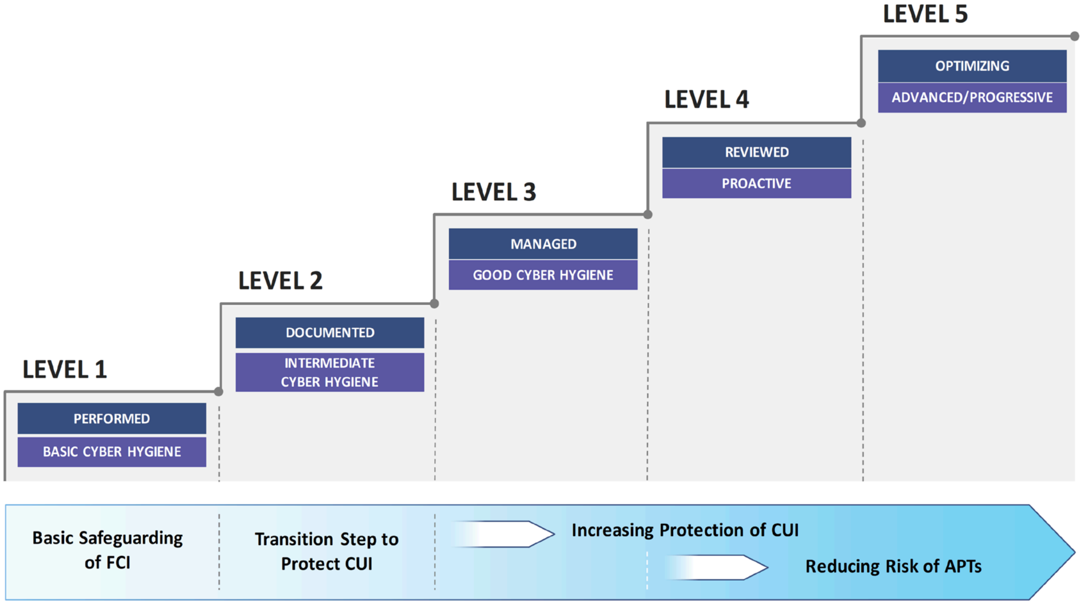
vArmour Accelerates CMMC Framework Adoption

Background

The Department of Defense (DoD) has recently established a new cybersecurity certification framework, called the Cybersecurity Maturity Model Certification ("CMMC"), to protect privileged information within its defense industrial base (DIB) supply chain of over 300,000 companies.

The CMMC framework is intended to ensure that defense contractors adopt cybersecurity compliance through a maturity model. It is not a single cybersecurity requirements document. CMMC draws heavily from existing industry security standards such as NIST, FAR, CIS and DFARS. This model can help companies to better assess and demonstrate their compliance to a set of strong cybersecurity posture and controls. CMMC is a tiered model with five maturity levels for different types of organizations and risk tolerances. What's new is that contractors are required to pass formal third-party CMMC audits and certifications to demonstrate their compliance.

Figure 1. CMMC Levels and Associated Focus



Source: (DoD) https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

vArmour Solutions To Accelerate CMMC Compliance

Given the urgency to prove CMMC compliance, many enterprises must adopt new solutions that can accelerate their cybersecurity maturity. Application Relationship Management (ARM) can help enterprises see, map, and secure their interconnected and dynamic software applications using their existing infrastructure. vArmour solutions enable organizations to visualize applications, application relationships and dependencies, and identities in real-time across the entire enterprise. As a result, enterprises can create, enforce, and validate granular security policies that apply application-centric and operational controls based on a real-time understanding of all interactions or communication among applications, workloads, and identities. This lays a solid foundation for organizations to implement and operate a cybersecurity framework that meets CMMC requirements.

vArmour accelerates time to value beyond existing networking or infrastructure-based approaches by using an agentless solution that does not require new agent or appliance deployments, ensuring you are not limited by implementation complexity or environmental constraints.

Who Should Care About CMMC

Many enterprises, from the largest defense contractors down to small subcontractors, are ill-prepared for CMMC certification. In fact, in a recent survey, nearly one-third of companies analyzed showed evidence indicating they would fail to meet the most basic, Tier 1 CMMC level; and nearly one-half had vulnerabilities that could expose them to breaches. CMMC certification is now a mandatory requirement in many new DoD RFQs that are worth billions of dollars in contract value. Given the timeframe to design, implement, and certify CMMC compliance, companies must act with urgency to avoid being unable to bid on and win new government contracts.

Accelerating CMMC Certification with vArmour

The CMMC framework is organized into a number of security-oriented domains that define required capabilities and processes that must be established. No one vendor delivers solutions across all domains.

With vArmour, enterprises gain unprecedented visibility and insights into all their applications across every environment. Real-time visibility yields better, more actionable insights easily and efficiently compared to those gleaned from abstractions, sampling, or estimates intended to validate policy intent. With greater operational understanding and confidence in observed reality, organizations can make better, faster decisions that significantly improves business performance, resiliency, and customer satisfaction; and significantly reduces risk and adverse compliance or regulatory exposure.

vArmour also automates and simplifies operations, reducing costs by relieving teams of people from tedious manual tasks with software that automates and scales in step with the needs of the business. Organizations can more easily address CMMC regulatory requirements, establish a more comprehensive governance framework, and demonstrate regulatory compliance.

CMMC and Zero Trust: Next Steps

Many enterprises will find that their CMMC and Zero Trust initiatives align closely, because CMMC maturity levels 3 and 4 reflect and require many foundational Zero Trust principles defined in existing security guidelines. Whether your initial driver is CMMC or Zero Trust, however, the journey begins with understanding and visualizing your enterprise environment, because you can't protect what you can't see.

Find out more about vArmour