SEPIO SYSTEMS

CMMC Compliance

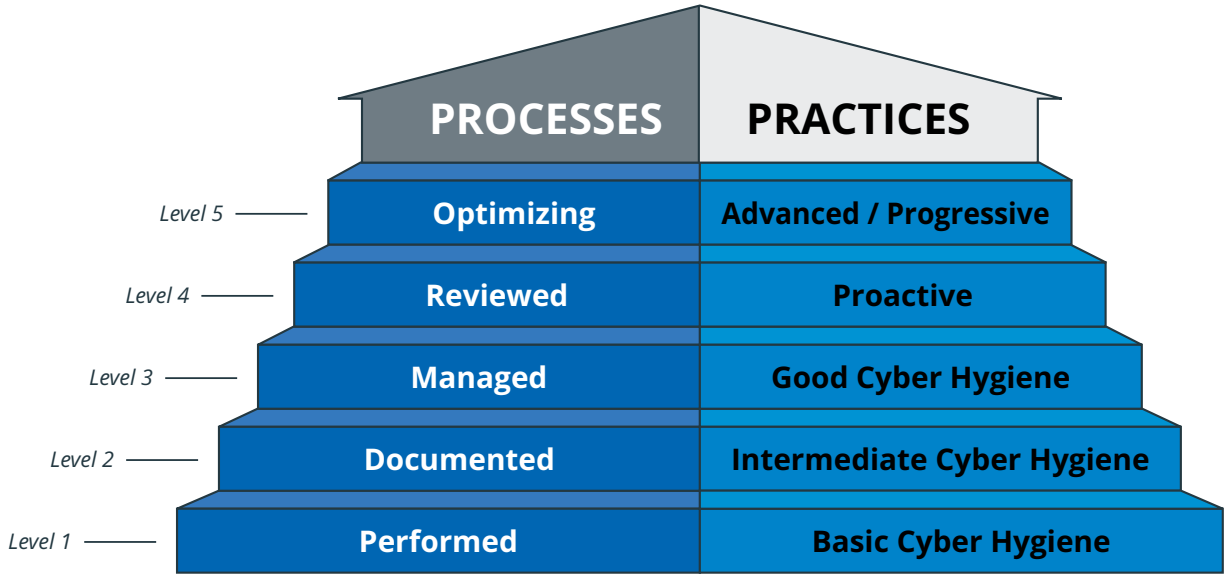
A Sepio Systems white paper

What is CMMC?

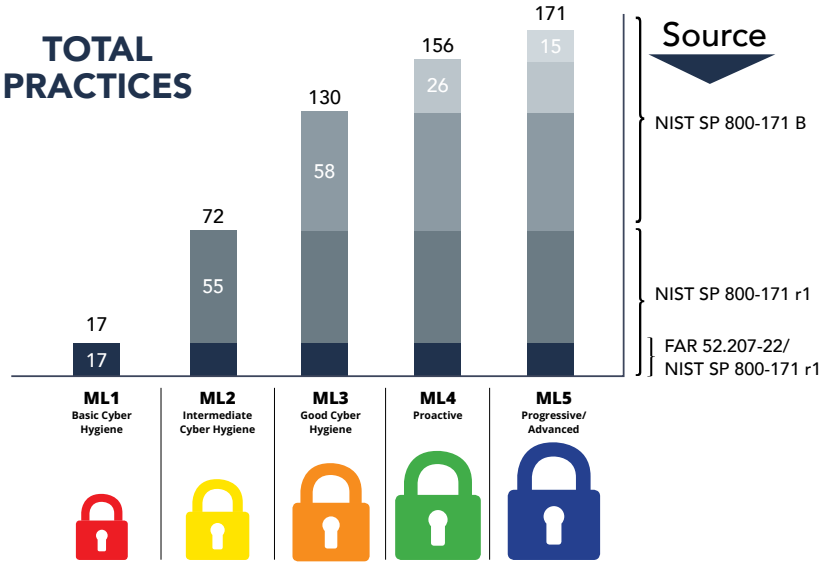
The new Cybersecurity Maturity Model Certification is the US Department of Defense's response to numerous compromises of sensitive defense information sitting on contractors' information systems. The CMMC provides a unified standard for implementing cybersecurity throughout the Defense Industrial Base (DIB) with a framework that better assesses and improves the cybersecurity posture of the DIB. The CMMC incorporates pre-existing legislation such as NIST SP 800-171, 48 CFR 52.204-21 and DFARS clause 252.204-7012.

The CMMC establishes five certification levels demonstrating the maturity and reliability of a company's cybersecurity capabilities to warrant the safeguarding of government information on the contractor's information systems. The purpose of the CMMC is to ensure that sufficient levels of cybersecurity practices and processes are in place to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that sit on the DIB's network.

CMMC Maturity Levels



The CMMC is made up of 17 domains, with 5 processes and 43 capabilities distributed cross those domains, sub sectioned into 171 practices. The CMMC is divided into practices – the technical activities required within any given capability requirement – and processes – which measure the maturity of organization's institutionalization of cybersecurity procedures.



The regulation prior to the CMMC (DFARS clause 252.204-7012) stated that the contractors were responsible for implementing, monitoring and certifying the security of their technology systems and any sensitive DoD information stored on, or transferred by, those systems.

With the CMMC in place, contractors are still tasked with implementing key cybersecurity capabilities, but the DoD is provided with additional security assurance in the form of a third-party assessment. This assessment assures that contractors comply with specific mandatory practices, procedures and capabilities that can adapt to new and evolving cyber threats from adversaries.

The levels of the CMMC are cumulative meaning that as they ascend, compliance with the lower levels is required. Since the CMMC is divided into processes and practices across five levels that are parallel to one another, a contracting organization must meet the requirements for the level they seek in both the practice and process realms. Failure to do so means that the contractor will be certified on the lowest level that they achieve in either process or practice.

An important note is that not all contractors need to achieve a level 5 certificate; it depends on the sensitivity of the DoD information that it will work with, and the range of cyberthreats associated with said information.

CMMC Framework

	Processes	Practices
Level 1	**Performed**	**Basic Cyber Hygiene**
	N/A	L1 focuses on the protection of FCI and consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 ("Basic Safeguarding of Covered Contractor Information Systems").
Level 2	**Documented**	**Intermediate Cyber Hygiene**
	L2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. Documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented.	L2 serves as a progression from L1 to L3. Consists of a subset of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references. Because this is a transitional stage, a subset of the practices reference the protection of CUI.
Level 3	**Managed**	**Good Cyber Hygiene**
	L3 requires that an organization establish, maintain and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training and involvement of relevant stakeholders.	L3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references to mitigate threats. It is noted that DFARS clause 252.204-7012 ("Safeguarding of Covered Defense Information and Cyber Incident Reporting") specifies additional requirements beyond NIST SP 800-171 security requirements such as incident reporting.
Level 4	**Reviewed**	**Proactive**
	L4 requires that an organization review and measure practices for effectiveness. Additionally, organizations at L4 are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis.	L4 focuses on protection of CUI from APTs and encompasses a subset of the enhanced security requirements from Draft NIST SP 800 171B, as well as other cybersecurity best practices. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics techniques and procedures (TTPs) used by APTs.
Level 5	**Optimizing**	**Advanced/Proactive**
	L5 requires organizations to standardize and optimize process implementation across the organization.	L5 focuses on the protection of CUI from APTs. The additional practices increase the depth and sophistication of cybersecurity capabilities.

What is next for DoD contractors?

Contractors need to get familiarized with the CMMC's technical requirements and ready themselves for both certification, and long-term cybersecurity agility. Contractors should evaluate their practices, procedures and gaps, and take action to patch any identified vulnerabilities.

This is where Sepio Systems provides assistance to DoD contractors. Sepio's SaaS can further equip organizations to comply with the CMMC regulation, providing coverage over a realm of practices, up to level 5.

See below for the practices which Sepio can help contractors comply with.

Domain	Capability	Practices
Access Control (AC)	C001: Establish system access requirements.	AC.1.001 AC.2.006
	C002: Control internal system access.	AC.2.011 AC.5.024
	C003: Control remote system access.	AC.4.032
	C004: Limit data access to authorized users and processes.	AC.1.003
Asset Management (AM)	C006: Manage asset inventory.	AM.4.226
Audit & Accountability (AU)	C007: Define audit requirements	AU.2.041 AU.3.045 AU.3.046
	C008: Perform auditing	AU.2.042 AU.3.048 AU.5.055
	C009: Identify and protect audit information	AU.3.049
	C010: Review and manage logs	AU.2.044 AU.3.051 AU.3.052 AU.4.054
Configuration Management (CM)	C013: Establish configuration baselines.	CM.2.061
	C014: Perform configuration and change management.	CM.3.067 CM.3.068
Identification and Authentication (IA)	C015: Grant access to authenticated entities	IA.1.076 IA.1.077

Incident Response (IR)	C016: Plan incident response.	IR.2.092 IR.4.100 IR.5.106
	C018: Develop and implement a response to a declared incident.	IR.3.098 IR.5.102 IR.5.108
Maintenance (MA)	C021: Manage Maintenance	MA.2.111
Media Protection (MP)	C023: Protect and control media	MP.2.121 MP.3.123
Personal Security (PS)	C027: Protect CUI during personnel actions	PS.2.128
Physical Protection (PE)	C028: Limit physical access	PE.1.133 PE.2.135 PE.3.136
Risk Management (RM)	C031: Identify and evaluate risk.	RM.2.142 RM.3.144 RM.4.149 RM.4.150 RM.4.151
	C032: Manage risk.	RM.2.143 RM.3.146 RM.3.147
Situation Awareness (SA)	C037: Implement threat monitoring.	SA.3.169 SA.4.171
Systems and Communications Protection (SC)	C038: Define security requirements for systems and communication.	SC.3.183 SC.3.186 SC.4.197 SC.5.230
	C039: Control communications at system boundaries.	SC.1.175 SC.1.176
	C040: Identify and manage information system flaws.	SI.1.210 SI.4.221
System and Information Integrity (SI)	C041: Identify malicious content.	SI.1.212 SI.5.222
	C042: Perform network and system monitoring	SI.2.216 SI.2.217 SI.5.223

HAC-1 Solution

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment. This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

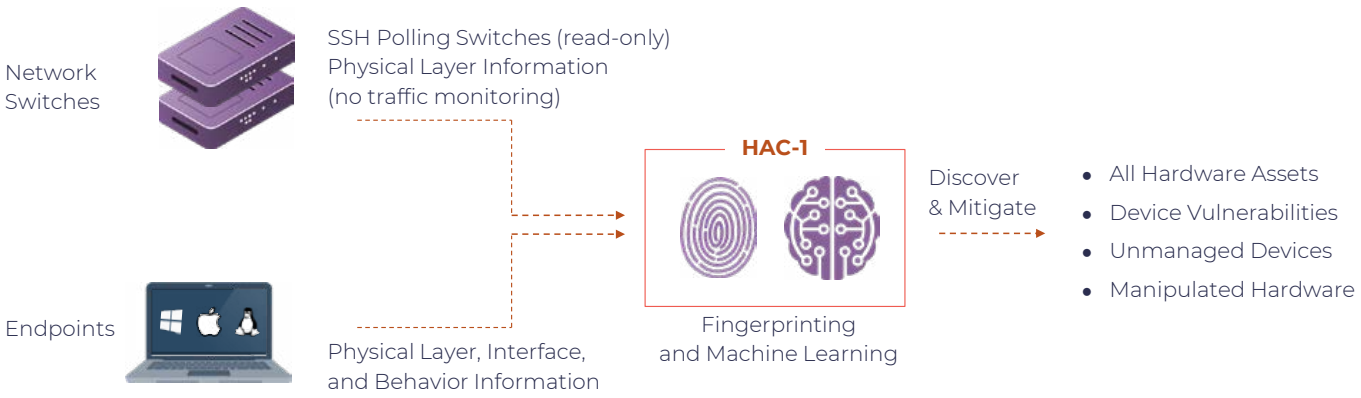
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio Systems is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio Systems calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

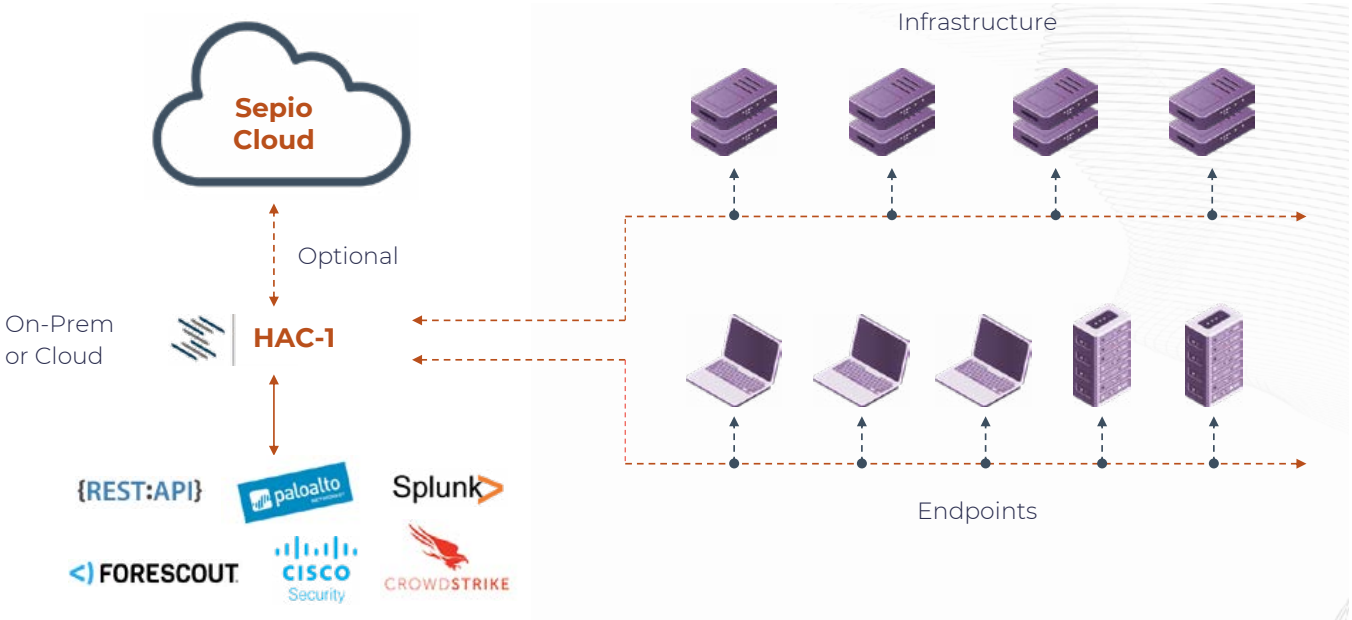
Main Benefits:

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



LEARN MORE

SEPIO SYSTEMS