Reduce the Complexity and Cost of CMMC Compliance

Gigamon is enabling defense contractors to achieve CMMC compliance today

> Gigamon gave us ease of administration, tremendous cost savings, storage savings and many other enhanced capabilities.
>
> – TIER-ONE DEFENSE PRIME CONTRACTOR

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) SNAPSHOT

+ Effective: November 30, 2020[1]
+ Impacting: 300,000 companies in the defense supply chain
+ Defense contracts will soon contain CMMC requirements
+ Every vendor in the defense supply chain will need to become certified

Gigamon Simplifies and Accelerates CMMC Compliance

Gigamon is uniquely capable of serving as the cornerstone of a DoD contractor's or vendor's certification strategy. By combining pervasive infrastructure visibility with timely and trustworthy threat detection, Gigamon enables DoD partners to meet CMMC requirements faster while reducing ongoing operational cost and complexity.

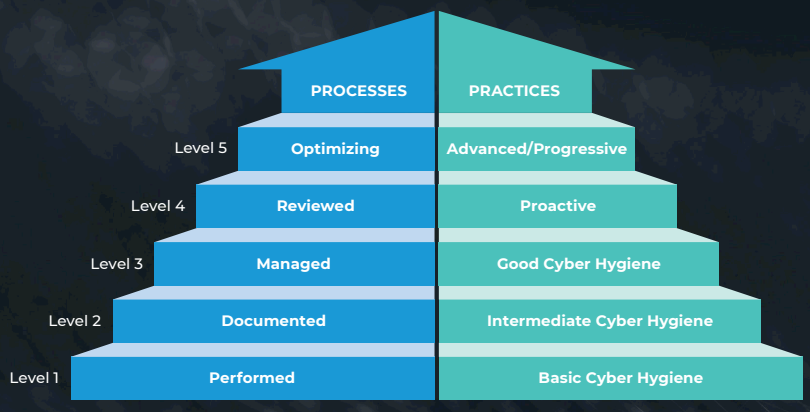
In total, Gigamon solutions address over 35% of the controls across 10 of 17 CMMC domains, including:

+ Access Control (AC)
+ Asset Management (AM)
+ Audit & Accountability (AA)
+ Configuration Management (CM)
+ Incident Response (IR)
+ Risk Management (RM)
+ Security Assessment (SAS)
+ Situational Awareness (SA)
+ System and Communication Protection (SCP)
+ System and Informational Integrity (SII)

The specific CMMC requirements that Gigamon addresses in these areas are listed in Table 1.

CMMC REQUIREMENTS IN BRIEF

CMMC includes 171 practices across five maturity levels. It includes security standards and frameworks drawn from existing requirements such as Federal Acquisition Regulation (FAR) clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems and the security requirements for Controlled Unclassified Information (CUI) specified in NIST SP 800-171. It also includes processes and practices that demonstrate a progression of cybersecurity maturity.



Source: DoD Cybersecurity Maturity Model Certification 1.0 January 2020

Increase Visibility, Reduce Cost with Gigamon

The Gigamon Visibility and Analytics Fabric™, shown in Figure 1, helps DoD contractors, vendors and the DoD itself significantly reduce the cost and complexity of implementing CMMC controls. Lack of infrastructure visibility is one of the most significant obstacles to attaining CMMC. Gigamon creates a single point of visibility for data in transit across enterprise networks, including virtualized networks and cloud instances. It also optimizes the coverage, efficiency, scalability and performance of the cybersecurity tool suite through a variety of powerful capabilities.

Gigamon makes the security tools that DoD contractors and vendors rely on for their CMMC posture more scalable and less expensive to operate by applying traffic reduction techniques such as de-duplication, application filtering, flow mapping and NetFlow to reduce data processing requirements.

A federal government sub-agency confirmed it saved $1,000,000+ using Gigamon solutions while achieving ROI in 6–12 months.

Gigamon also increases security tool effectiveness by enabling centralized traffic decryption and inspection. It is estimated that 50 to 75 percent of malware hides in encrypted traffic. Gigamon centrally decrypts this traffic for inspection, using a FIPS 140-2 Level 2 platform. This offloads CPU-intensive decryption processing from individual tools.

When a tier-one prime contractor needed scalable visibility into SSL/TLS traffic, it found Gigamon to be the "most complete visibility solution" with "protection from blind spots, including within encrypted traffic."

Many DoD partners will need to make network infrastructure and security tool changes in order to attain CMMC. These changes, as well as ongoing maintenance, are greatly simplified through Gigamon capabilities such as inline bypass, tool health checking and failover.

Together, the broad capabilities of the Gigamon Visibility and Analytics Fabric significantly decrease both capital expenses and operational expenses for network and security tools to support any organization's CMMC strategy.

Figure 1. The Gigamon Visibility and Analytics Fabric sits between IT infrastructure and tools. Its capabilities are proven to help contractors of all sizes reduce the complexity and cost of addressing CMMC requirements.

Gigamon Extends Threat Detection and Investigation Across Cloud Operations

Gigamon ThreatINSIGHT™, shown in Figure 2, provides software-as-a-service-based network detection and response (NDR) capabilities to meet CMMC requirements and enhance security posture. ThreatINSIGHT performs discovery and systemic monitoring of user, device and application communications across all IT operations infrastructure. Metadata generated from the communications is analyzed against multiple sources of threat intelligence to provide highly validated threat detections to security operations teams on a 24/7 basis.

Gigamon ThreatINSIGHT directly addresses CMMC controls by providing detection and analytics for all data flows, including TLS encrypted traffic, regardless of network architecture (physical, cloud or hybrid).

Furthermore, through integration with the Zscaler Cloud Security Platform, ThreatINSIGHT enables cloud security at the edge, which is essential for addressing threat vectors introduced in the new work-from-home paradigm.

A government organization reported that it:

+ Accelerated threat prevention, detection and response time
+ Optimized tool utilization by traffic filtering
+ Reduced storage costs with better management of traffic volume
+ Enhanced staff efficiency by reducing manual tasks

...all after using Gigamon solutions.

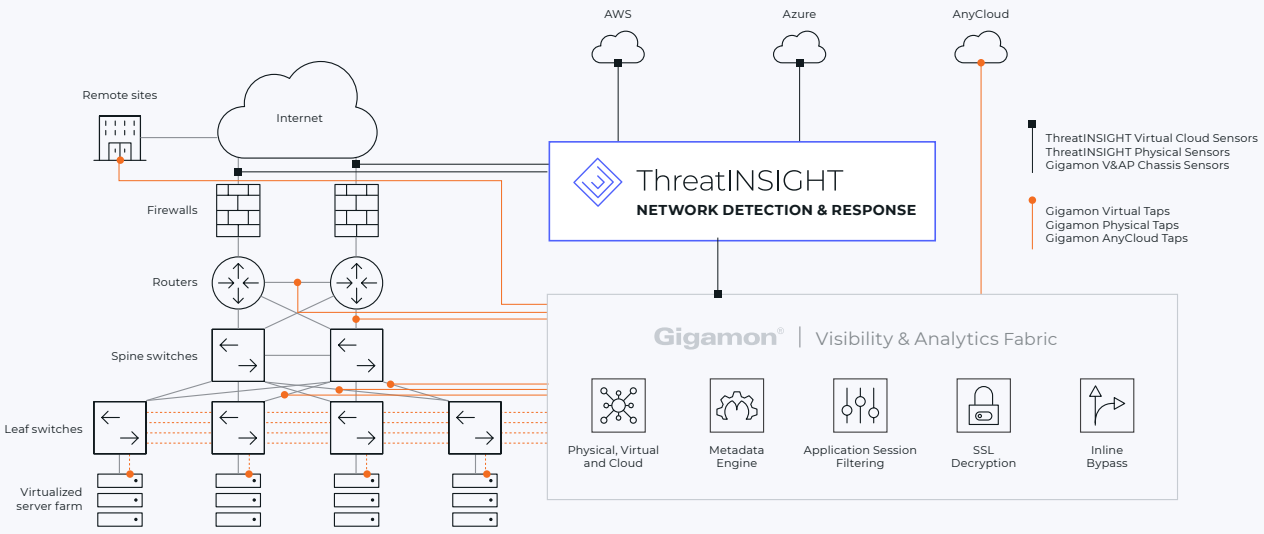


Figure 2. Gigamon ThreatINSIGHT provides network detection and response that directly addresses CMMC controls.

A top 10 systems integrator confirmed the following results with Gigamon solutions:

+ Centralized traffic decryption (FIPS 140-2 Level 2 certified)
+ Maximized network visibility
+ Optimized tool utilization by traffic filtering
+ Lowered escalating tool cost
+ Enhanced staff efficiency by reducing manual tasks

GIGAMON CERTIFICATIONS AND AUTHORITY TO OPERATE (ATO)

+ Department of Defense (DoDIN APL)
+ DISA STIG and IPv6 compliant
+ FIPS 140–2 validated
+ NIAP Common Criteria
+ Trade Agreement Act Compliant (TAA)
+ NEBS 3 compliant

Gigamon is authorized to operate in U.S. Department of Defense's (DoD) Joint Regional Security Stack (JRSS) and many other DoD, intelligence community and civilian agency networks

+ General Services Administration Schedules Program (GSA) Schedule 70
+ NASA's Solutions for Enterprise-Wide Procurement (SEWP)

CAGE: 4XKN9
DUNS: 362737251

A Trusted Partner for CMMC

Gigamon is already trusted by 10 of the top 10 U.S. federal agencies and leading DoD contractors and vendors.

10 out of the top 10 U.S. federal agencies have deployed Gigamon solutions

153 percent ROI improvement of the security stack[2]

50 percent decrease in costs associated with security efforts[2]

58 percent market share in the government sector, nearly four times the nearest competitor[3]

#1 market leader with 38 percent market share, twice the market share of the nearest competitor[3]

[1] Per U.S. Department of Defense interim rule for CMMC, September 2020.

[2] The Total Economic Impact™ of Gigamon, a commissioned study conducted by Forrester Consulting on behalf of Gigamon, April 2016.

[3] Network Monitoring Equipment Annual Market Report: Omdia, June 2020.

TABLE 1. CMMC CONTROLS THAT ARE ADDRESSED BY GIGAMON

Control ID	Description	Maturity Level	Gigamon Visibility & Analytics Fabric Enables or Addresses	Gigamon ThreatINSIGHT Enables or Addresses
AC.1.003	Verify and control/limit connections to and use of external information systems.	1	•	
AC.1.004	Control information posted or processed on publicly accessible information systems.	1	•	
AC.2.013	Monitor and control remote access sessions.	2	•	
AC.2.016	Control the flow of CUI in accordance with approved authorizations.	2	•	
AC.4.023	Control information flows between security domains on connected systems.	4	•	
AM.4.226	Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.	4	•	
AU.2.041	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	2	•	•
AU.2.042	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity.	2	•	•
AU.3.048	Collect audit information (e.g., logs) into one or more central repositories.	3		•
AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious or unusual activity.	3		•
AU.3.052	Provide audit record reduction and report generation to support on-demand analysis and reporting.	3	•	•
AU.4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	5	•	
AU.5.055	Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.	5	•	
CM.2.061	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system.	2	•	
CM.2.063	Control and monitor user-installed software.	2	•	
CM.3.068	Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols and services.	3	•	
IR.2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user response activities.	2		•
IR.2.093	Detect and report events.	2	•	•
IR.2.094	Analyze and triage events to support event resolution and incident declaration.	2		•
IR.2.096	Develop and implement responses to declared incidents according to predefined procedures.	2		•
IR.2.097	Perform root cause analysis on incidents to determine underlying causes.	2	•	•
IR.4.100	Use knowledge of attacker tactics, techniques and procedures in incident response planning and execution.	4		•
IR.4.101	Establish and maintain a security operations center capability that facilitates a 24/7 response capability.	4		•
IR.5.106	In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.	5	•	•
IR.5.108	Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.	5		
RM.2.142	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	2	•	
RM.3.144	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources and risk measurement criteria.	3		•
RM.4.149	Catalog and periodically update threat profiles and adversary TTPs.	4		•
RM.4.150	Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting and response and recovery activities.	4		•

TABLE 1. CMMC CONTROLS THAT ARE ADDRESSED BY GIGAMON (CONTINUED)

Control ID	Description	Maturity Level	Gigamon Visibility & Analytics Fabric Enables or Addresses	Gigamon ThreatINSIGHT Enables or Addresses
RM.4.151	Perform scans for unauthorized ports available across perimeter network boundaries over the organization's internet network boundaries and other organizationally defined boundaries.	4	•	•
RM.5.155	Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.	5	•	
CA.2.158	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	2	•	
CA.2.159	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	2	•	
CA.3.161	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	3	•	
CA.4.164	Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.	4	•	•
SA.3.169	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	3		•
SA.4.171	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track and disrupt threats that evade existing controls.	4		•
SA.4.173	Design network and system security capabilities to leverage, integrate and share indicators of compromise.	4		•
SC.1.175	Monitor, control and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	1	•	•
SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	3	•	
SC.3.180	Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.	3	•	
SC.3.182	Prevent unauthorized and unintended information transfer via shared system resources.	3	•	
SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3	•	
SC.3.189	Control and monitor the use of voice over internet protocol (VoIP) technologies.	3	•	
SC.4.202	Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing internet network boundaries or other organizationally defined boundaries.	4	•	
SC.5.198	Configure monitoring systems to record packets passing through the organization's internet network boundaries and other organizationally defined boundaries.	5	•	
SC.5.208	Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.	5	•	
SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.	1	•	
SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	2	•	•
SI.2.217	Identify unauthorized use of organizational systems.	2	•	
SI.3.220	Utilize sandboxing to detect or block potentially malicious email.	3	•	
SI.4.221	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	4		•
SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	5	•	•