# Splunk for Cybersecurity Maturity Model Certification (CMMC) Solution

## Supporting the Cybersecurity Mission

In 2018, the Department of Defense (DoD) revised its cybersecurity strategy when it updated the National Defense Strategy. This called for cybersecurity as a fourth qualification for the award of DoD acquisitions, in addition to the preexisting pillars of cost, schedule and performance. This strategy implied that existing cybersecurity requirements established by the DoD Federal Acquisition Regulation Supplement (DFARS) had not gone far enough to meet the nation's cyber mission. To address this gap, the Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD A&S) worked with stakeholders from industry, the DoD, University Affiliated Research Centers, and Federally Funded Research and Development Centers to develop the Cybersecurity Maturity Model Certification (CMMC).

The CMMC builds on DFARS both in technical requirements and by establishing "trust, but verify" relationships with DoD contractors. To accomplish this, the CMMC institutes a requirement for recurring audits for all DoD contractors. The recurring audit benefits the national cyber mission but creates new challenges for DoD contractors. Rather than establishing compliance with a single event as with the DFARS, DoD contractors must regularly demonstrate compliance and cybersecurity disposition to qualify for new contract opportunities.

## Historical Challenges

To meet the CMMC's new, ongoing requirements for demonstrating cybersecurity and compliance, DoD contractors need to overcome four common challenges associated with cybersecurity and continuous monitoring.

### Slow, Complex Implementation

DoD contractors must quickly deploy and adopt technologies for continuous monitoring and execution of cybersecurity practices defined by the CMMC. This achievement requires a robust platform that can be rapidly adapted to address unique use case requirements. The timelines for initial certification and execution do not allow for long-running waterfall projects, with discrete phases for planning, data modeling and other activities. To achieve certification, DoD contractors must apply proven enterprise-grade technology that can be iteratively tailored and extended to address the unique demands of the CMMC criteria.

### Siloed Sensors and Data Sources

In addition to mastering implementation complexities, DoD contractors must overcome siloed tools and data sources to establish repeatable, integrated processes that streamline monitoring, execution and audit preparation. Systems integrators often maintain diverse corporate networks that include everything from laptops and networking appliances to industrial control systems. These networks not only contain diverse tooling, but often span distributed physical environments, including regional offices, data centers, public clouds and industrial facilities. DoD contractors require an integrated approach to monitoring their environments and readily furnishing artifacts associated with them.

### High Volume and Velocity Data

Given the comprehensive nature of the CMMC, DoD contractors must collect and monitor data from vast collections of sensors and applications. This machine data is generated at a high volume and velocity while spanning an unlimited number of digital formats. To complicate matters, accessing data from each of these various sensors and applications requires business processes, controls and even analyst training. Corporate business units may produce gigabytes-to-terabytes of new data every day, often with exponential growth in the volume and velocity of data over time. Contractors require a platform that can scale to meet these growth and diversity challenges.

### Rigidity as a Limiting Factor to Growth

As organizations make strategic decisions to meet the demands of the Cybersecurity Maturity Model Certification, they must ensure that their selected approach does not inhibit their growth. Today's networks are dynamic ecosystems that continuously evolve with the needs of the business. Compounding this challenge, the CMMC has multiple levels of maturity, applied based on the expected handling of controlled unclassified information (CUI). Though organizations will achieve an initial Cybersecurity Maturity Model Certification level, business needs may warrant adopting additional cyber security practices to elevate their maturity level and qualify for new contract opportunities. DoD contractors require a robust capability that will remain extensible and able to accommodate the various levels of the CMMC as relevant to their business and future contract bids.

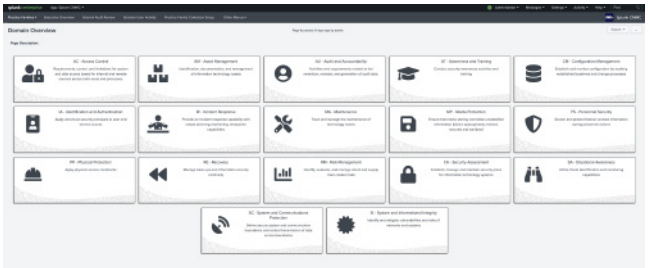
## Splunk's Approach

Splunk® provides an open, data-to-everything platform with more than 19,000 customers across commercial and public sector entities. Splunk's customers include all four branches of US Armed Forces, DoD agencies and defense contractors. With Splunk, organizations can overcome the aforementioned historical challenges. Splunk has

developed the Splunk for CMMC solution to address the requirements of DoD's new Cybersecurity Maturity Model. This solution is tailored to align with the domains, capabilities, and the 170+ practices defined across CMMC's five maturity levels.

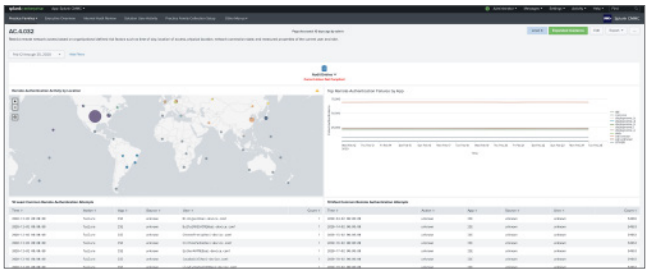
## Rapid Operationalization

With Splunk, organizations can leverage their data to rapidly gain visibility into the use cases and workflows required by the CMMC. Splunk provides a single environment to **Investigate -> Monitor -> Analyze -> and Act** on your data. Splunk's ability to ingest virtually any form of data enables the iterative implementation of workflows and analytics that flexibly align to the CMMC-mandated cybersecurity practices — across the range of CMMC L1 to L5.



## A Single Pane View Into Your Data

As the Data-to-Everything platform, Splunk provides a lynchpin capability for integrating siloed data sources and sensors. Splunk software is vendor and location-agnostic, meaning that Splunk offers organizations a single pane of glass window into their enterprise across tools, sensors, geographies, and even cloud or hosting providers. Splunk's Common Information Model (CIM) streamlines data normalization and allows for standardized analytics across multiple data sources. By establishing this single pane, Splunk enables organizations to break down silos and gain visibility across their data for CMMC, continuous cybersecurity monitoring, and beyond — unlocking the full value of their data.



## Designed for Scale On-Premise or in the Cloud

Splunk Enterprise on-prem or the FedRAMP Authorized Splunk Cloud SaaS offering rise to enterprise data demands with the ability to easily process multiple terabytes of new data per day, processing and surfacing tens of thousands of events per second. Splunk also scales horizontally to address the growth and dynamic needs of organizations. These capabilities, coupled with assurances like built-in high-availability and disaster recovering mean that Splunk is prepared to meet the big-data challenge.

## Robust and Responsive to your Mission

The **Splunk for CMMC** solution not only provides a tailored approach designed to scale and adapt to the needs of any environment, but is also designed to allow organizations to mature and adopt enhanced capabilities as their missions require. Built on Splunk Enterprise, the solution is designed to surface data from other Splunk capabilities that can be used to address CMMC practices. Splunk Enterprise Security, Splunk Phantom and Splunk UBA are all capabilities that automate, streamline and enable practices required by the CMMC.

## So What Are You Waiting For?

Cybersecurity is critical to both the National Defense Strategy and the intellectual property of your organization. Start taking steps towards your successful Cybersecurity Maturity Model Certification today.

### Solution Impact

- Continuously monitor your environment to achieve and maintain security and compliance requirements.
- Accelerate the adoption and achievement of CMMC-required practices.
- Capture organizational efficiency by applying a consistent enterprise data environment.
- Reduce complexity with audit information, traceability and activity in one environment.
- Save time with automated data collection and furnishing of requirements to address audits.
- Chart a path towards achieving more advanced levels of Maturity Certification.

Splunk can help your organization meet the Cybersecurity Maturity Model Certification. Whether you've been using Splunk Enterprise for years or you are evaluating Splunk for the first time, **contact us to learn more**.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com



20-13209-PUBSEC-CybersecurityMaturityModelCertification(CMMC)Solution-101-TB