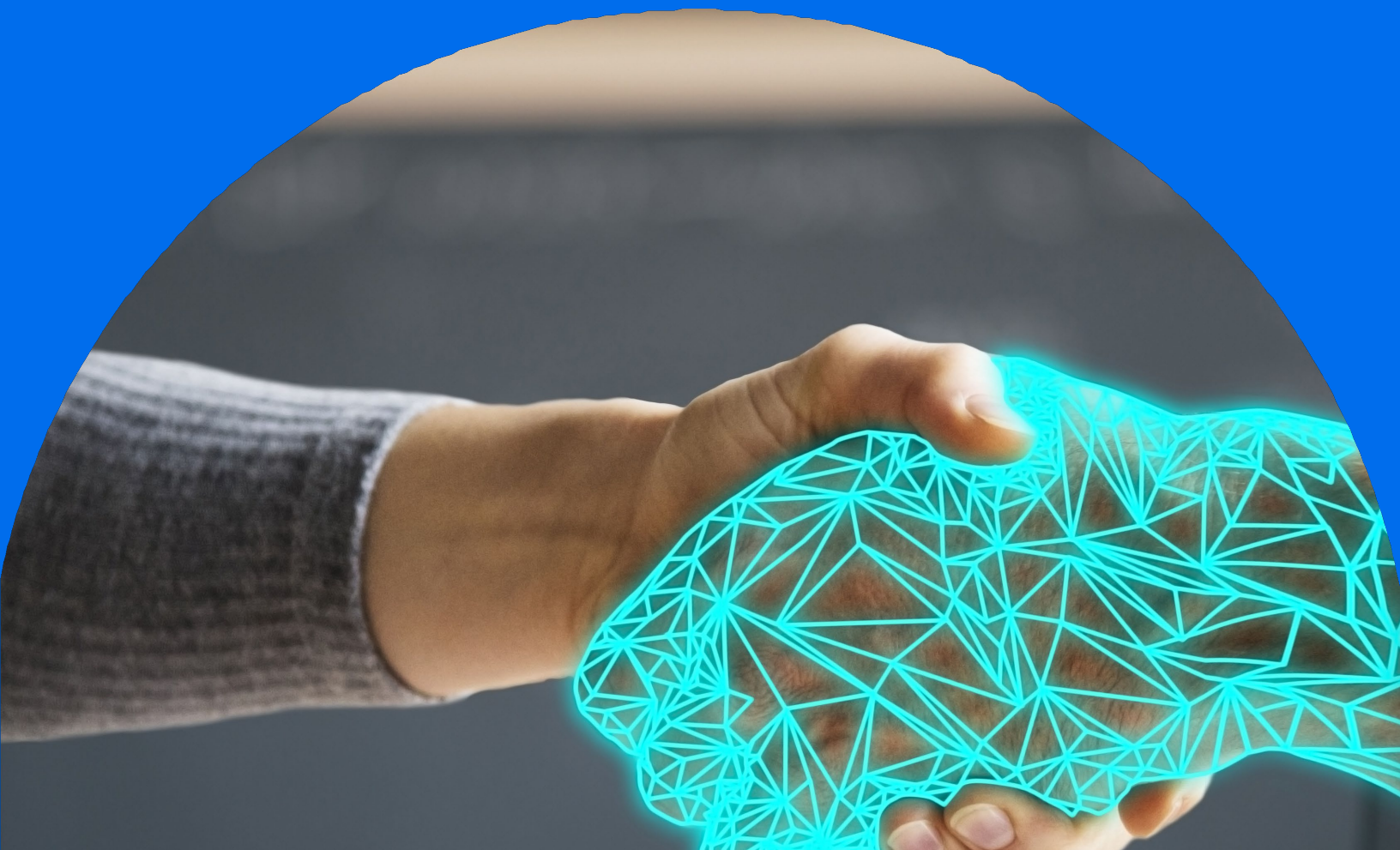


How Actifile Can Help You Achieve CMMC Compliance

May 2023



HOW ACTIFILE CAN HELP YOU ACHIEVE CMMC COMPLIANCE

Studies indicate Cybercrime costs will rise 15 percent per year over the next five years, reaching **\$10.5 trillion annually by 2025**. So it was no surprise when President Biden addressed the issue. Even before he issued the executive order on CyberSecurity, the Department of Defense (DoD) strove to improve the security posture of over 300,000 suppliers and contractors making up the supply chain known as the Defense Industrial Base (DIB). The initiative was driven by the data placing costs of cybercrime at nearly \$109 billion in 2016.

OVER 70,000 DOD CONTRACTORS ARE REQUIRED TO MEET **CMMC** COMPLIANCE BY 2021 .

It wasn't that the DIB was without security. There were existing requirements for creating a System Security Plan (SSP) and Plan of Actions & Milestones (POA&M) mandated by NIST 800-171. These requirements made contractors responsible for the implementation, monitoring, and certification of their IT systems.



On paper, these sounded sufficient, but the actual compliance level across contractors and subcontractors was inconsistent because they were self-managed. Self-management and attestation allowed contractors to push off remediation of missing controls which created a security gap. With this information, the DoD requested that congress enable them to push for more stringent requirements. This resulted in the establishment of the Cyber Security Maturity Model Certification (CMMC).

WHY IS CMMC SO IMPORTANT?

To be effective, the CMMC needed to have some weight behind it. It mandated all contractors doing business with the department of defense to meet CMCC requirements to continue doing business with the DoD. The firm cut-off of 2020 allowed contractors time to implement all required controls and pass the audit for verification. Without this audit validation, they would not be eligible to bid for new contracts.

Unlike with NIST 800-171, meeting the requirements was not simply about having self-determined that the control was in place. Instead, it required an additional step of having an unbiased third-party auditor assess the level of compliance. This eliminated the risk that contractors might misrepresent their current posture and assured the DoD that contractors could prove they are compliant up to the assessed grade.

CONTROL FRAMEWORK

The implementation of CMMC does not mean that the previous NIST 800-171 controls were no longer important. The foundation of CMMC draws on NIST 800-171 revision 2, which is the primary framework referenced for each level. This framework is shorter than NIST 800-53, which is mandated explicitly for government agencies. However, the two frameworks have overlapping controls as NIST 800-171 grew from NIST 800-53 to provide a control framework for the public sector that could integrate with existing government security.

The NIST control frameworks are written broadly and designed to allow organizations to adapt to their environment. Instead of explicitly prescribing a solution, it describes a type of technology such as log monitoring and gives requirements that need to be met for the solution to be sufficient. This allows flexibility in meeting the control and avoids rigidity that could prevent newer technologies from being implemented.



WHAT IS CYBER SECURITY MATURITY MODEL CERTIFICATION (CMMC)?

The Cyber Security Maturity Model Certification or CMMC, as it is commonly referred to, is a regulation intended to help protect the department of the defense supply chain by holding contractors and suppliers to higher security standards. These standards are no longer self-attested but require independent audit review to validate compliance.

"CMMC is not just about security benchmarks, but baking security into every aspect of your processes."

GUY BAVLY, CEO, Actifile

MEETING CMMC

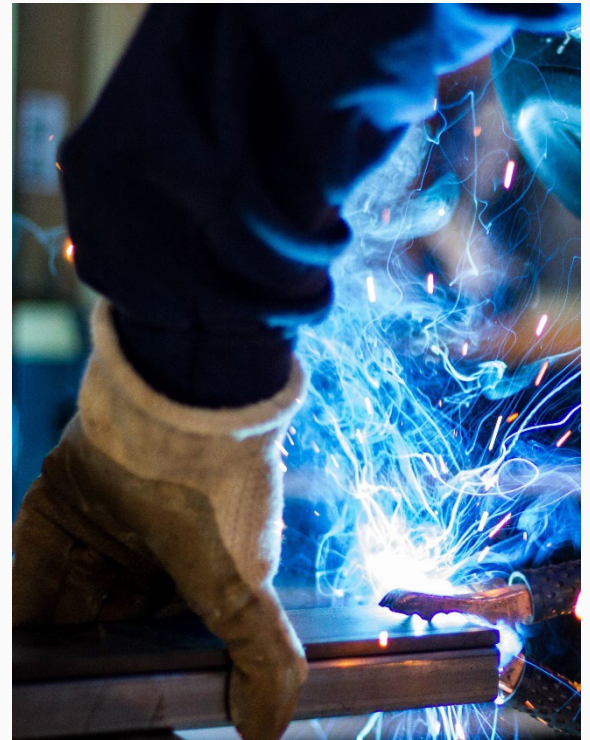
Being able to meet the higher levels of CMMC requires having the right tools and procedures in place. Having the right tools can help meet security controls and the more complex process level requirements. The right solutions can help you automate processes to guarantee that consistent, repeatable actions are taken every time. In addition, some tools will generate in-depth logs of measures taken to prove that you have continually met compliance guidelines. This type of data makes the auditor's job more efficient, allowing them to evaluate your infrastructure quickly without making numerous evidence requests to staff.

To meet CMMC, organizations also need to fully understand where their sensitive data lies, how it is being handled, and by whom. For any software solution to be effective, the organization must know this information.

FIND CUI, FCI AND FOUO DATA

Before you can effectively protect the data, you need to know where it resides. This does not simply mean that you understand where it is stored but also where it might be handled or processed during its lifecycle. This information allows for the creation of targeted controls to protect the data rather than generic, less effective controls.

It is also essential to look beyond where the data is expected to be when hunting for sensitive data. Shadow IT, or the use of unsanctioned technologies is a pervasive issue in IT. Up to 83% of IT professionals report that their employees store data in unsanctioned cloud services. Investigating all of your IT assets, both on-premises and in the cloud is integral to locating all possible places where sensitive data may lurk.



Working manually to locate the different data repositories is a daunting and inefficient task, even in relatively small organizations. Effective use of applications that can automate the investigative process will avoid significant manual efforts, freeing up staff for critical operations. With automated searching, the risk of missing parts of a system or set of assets is also significantly reduced compared to people reviewing.

**MATURING YOUR
SECURITY IS A
PROCESS.
IT TAKES MORE
THAN FLIPPING A
FEW SWITCHES.**

MEETING CMMC

MONITOR AND MANAGE DATA

Once data is located, its usage needs to be monitored to show that it's handled appropriately. One part of the monitoring process is to ensure that only authorized individuals have access to the data. Part of meeting level 2 and beyond of CMMC is implementing the principle of least privilege. This requires that only those who need access to any given data set to complete their job duties are granted access, even if they otherwise would be allowed to see it.

The other monitoring component is to track that the data remains only in appropriate areas. During the course of business, data may be shared or moved to different locations for processing. As long as these locations are within the authorization boundaries, there is no issue. A problem arises when data leaves these trusted areas, especially if it is moved off-site. Effective monitoring solutions should track where sensitive information is at any given time and raise alerts or block its removal when a user attempts to relocate it or copy it elsewhere.

STOP PORTABLE MEDIA ABUSE

One way that data can leave the controlled perimeter is through the use of portable media. This exploitable gap is often overlooked by many solutions that focus on the network-based transference of data. With portable media, bad actors or well-meaning employees can easily copy data and move it outside protected space to wherever they like. Once data is on mobile media, its usage and dissemination become almost impossible to track.

Solutions that can detect the use of portable media and prevent its utilization are essential for protecting data. This type of solution should also generate alerts to IT and security staff about which user was trying to use portable media and what data they were attempting to copy over. This information is needed to verify that no data has been removed, aid the investigation of the incident, and help identify whether the individual was malicious or negligent.

STOP MALWARE FROM ACCESSING CUI

With the increase of ransomware as a viable business threat, organizations need to ensure that CUI data is inaccessible to these types of attacks. Malware attacks often exfiltrate data to the originators, allowing them to request additional ransom in exchange for not disclosing what information they stole. This is frequently done in conjunction with regular ransomware encryption attacks.

By applying encryption to their data, organizations can make it inaccessible to ransomware or malware to steal. Some ransomware can automatically identify interesting information or open up back doors for bad actors to search manually. By using encryption, any data they locate will not be able to be read, and even if they decide to steal it, it will remain protected and useless to them without the decryption keys.

MEETING CMMC

ENCRYPT TO PROTECT DATA

When using encryption to comply with CMMC, it is essential to remember that not all encryption is made equally. Organizations must utilize FIPS 140-2 validated encryption to protect CUI, FCI, and FOUO data. FIPS 140-2 does not simply list different encryption protocols but goes into configuration specifications and appropriate uses for the different types of encryption.

Solutions that already have implemented FIPS 140-2 requirements in their products will save organizations significant amounts of time and effort in meeting CMMC standards. This will allow organizations to start protecting their data with encryption rapidly. However, it takes more than simply performing the encryption but providing evidence that encryption has happened and meets the given standards. Mature products will provide this audit trail which facilitates the validation of these controls by auditors.



DELIVERS ON CMMC

Actifile can help organizations meet many of the control requirements of CMMC. With Actifile, you are able to protect your data throughout its lifecycle and provide the evidence needed to help auditors validate compliance with CMMC.

- Identify CUI, FCI, and FOUO Data - Actifile has pre-built classification policies for CUI and FCI data. It scans through your assets to not only locate where it is but how much is out there. This review also provides validation that the data has not left protected boundaries.
- Provide DLP Controls - Actifile actively reviews all systems and assets in your IT ecosystem to identify Shadow IT applications. It tracks how the CUI is being used and where it resides throughout its lifecycle. Active monitoring identifies and prevents potential exfiltration of CUI.
- Restrict Use of CUI on Portable Media - Actifile's active monitoring can identify when CUI and other sensitive data are moved to portable media. It prevents unintentional movement of this data, but when data must be moved to portable media, it provides FIPS 140-2 encryption using a validated cryptographic module.
- Prevent Malware From Accessing CUI - Actifile uses industry-standard persistent file-level encryption to protect data from being stolen by bad actors. Using Actifile, even if data is stolen by malware and ransomware, it is protected and unreadable without the decryption keys.
- Encrypt Data Using FIPS 140-2 Validated Encryption - Actifile has built-in FIPS 140-2 validated encryption into its solution. With Actifile, you can provide evidence that your data is encrypted in accordance with CMMC.

Schedule a demo to see how Actifile can help your organization meet CMMC.