VARONIS

CMMC 2.0

Cybersecurity Maturity Model Certification (CMMC) overview, requirements, & how Varonis fast-tracks certification for Defense Contractors

Contents

Overview

The United States Department of Defense has implemented the Cybersecurity Maturity Model Certification (CMMC) 2.0 to normalize and standardize cybersecurity preparedness across the federal government's defense industrial base (DIB). This whitepaper covers the concept of a maturity model in the context of cybersecurity, key figures of the DIB, the anatomy of current CMMC levels, and how Varonis can fast-track certification.

What is CMMC 2.0?

Cybersecurity Maturity Model Certification 2.0 is a updated and simplified program initiated by the United States Department of Defense (DoD) in order to measure their defense contractors' capabilities, readiness, and sophistication in the area of cybersecurity.

At a high level, the framework is a collection of processes, other frameworks, and inputs from existing cybersecurity standards such as NIST, FAR, and DFARS. (*See Additional Resources* for further detail.)

The primary goal of the certification is to improve the surety and security of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) that is in the possession and use of their federal contractors.

When does CMMC 2.0 take effect?

The CMMC 2.0 program was announced in November, 2021, with phased implementation scheduled to begin in May 2023 from October 2025.

To whom does CMMC apply?

The certification is applicable to both "prime" contractors who engage directly with DoD, and to subcontractors who contract with primes to provide fulfilment and execution of those contracts. Although some level of certification will be a requirement of every contract beginning in 2026, DoD has indicated that they intend to issue contract opportunities at all levels of the maturity model, meaning that there will be some number of requests issued that will require only a low level of certification, and some that will require higher levels of certification.

What to know about the CMMC 2.0 Framework:

The latest CMMC 2.0 model has three levels (replacing the five-tier system in CMMC 1.02). Announced on July 17, 2021, the three CMMC levels are Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert). CMMC assessment requirements vary based on the level of certification needed. Below is an overview provided by the DOD.

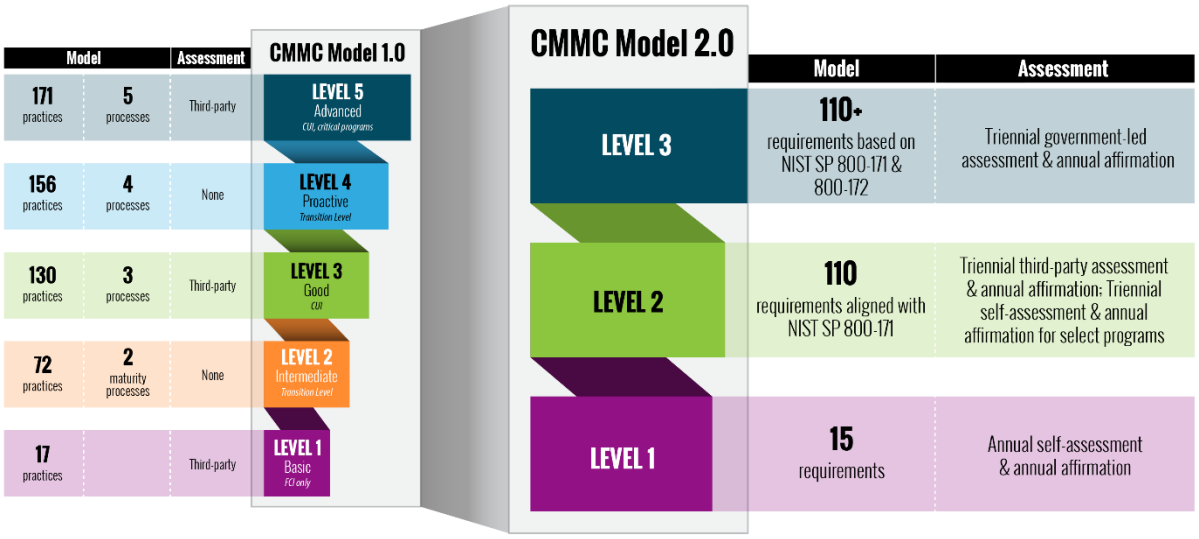

Image provided by the US Department of Defense

CMMC levels are a set of cybersecurity practices, standards, and processes published by the Department of Defense as part of the CMMC program designed to protect national security by aligning how defense contractors and subcontractors handle FCI and CUI. CMMC levels are comprised of practices, composed of domains and capabilities. All CMMC levels have processes, practices, and assessment procedures for DoD contractors.

Level 1: Foundational

Level 1 requires organizations to perform basic cybersecurity practices; however, they may perform these practices in an ad hoc manner without relying on documentation and may reach certification through an annual self-assessment.

Who needs level 1?

DoD contractors and subcontractors that handle Federal Contract Information (FCI), or “Information not intended for public release [that] is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government” will need CMMC level 1 certification.

Level 2: Advanced

Level 2 requires organizations to document their processes to guide their efforts to achieve CMMC Level 2 maturity. This documentation must also allow users to repeat these processes. Organizations must perform their processes as documented to achieve this maturity level.

Level 2 practices are classified as advanced cyber-hygiene practices. CMMC 2.0 Level 2 is equivalent to CMMC 1.02 Level 3, based on NIST SP 800-171.

Assessment requirements for level 2 compliance differ based on whether the CUI data is critical or non-critical to national security. Organizations with prioritized acquisitions that handle data that is critical to national security must pass a higher-level third-party assessment (C3PAOs) every 3 years, while non-prioritized acquisitions with data not critical to national security must conduct an annual self-assessment.

Who needs CMMC level 2?

DoD contractors and subcontractors that handle the same type of controlled unclassified information must meet level 2 compliance. A lower CMMC level may apply to the subcontractor if the prime only flows down select information.

CMMC level 3: Expert

The level 3 CMMC model reduces a system's vulnerability to advanced persistent threats (APTs) by requiring an organization to establish, maintain, and resource a plan to manage the activities needed to implement its cybersecurity practices.

The practices at level 3 qualify as good cyber-hygiene practices and focus on protecting CUI. However, they also encompass all the security requirements that NIST SP 800-171 specifies and the other 20 practices added for CMMC level 2. It's comparable to CMMC 1.02 Level 5.

Who needs CMMC level 3?

CMMC Level 3 applies to companies that handle CUI for DoD programs with the highest priority. The DoD is still developing its specific security requirements; however, it has already been indicated that the requirements of Level 3 will be based on NIST SP 800-171's 110 controls in addition to a subset of NIST SP 800-172 controls.

Know Before: Key CMMC Takeaways

- Applies to DoD prime contractors and subcontractors
- Applies to some new contracts starting in 2020 and applies to all contracts beginning in 2026
- Progressive model covers advancing levels of cybersecurity processes and practices resulting in a certification "Level"
- Contractors must start at Level 1 and certify at each level all the way to the top Level 5
- Varonis is a powerful tool for facilitating all levels of CMMC compliance

How to get certified

DoD has created the CMMC Accreditation Body (AB) which is a non-profit, independent organization to accredit Third Party Assessment Organizations (3PAOs) in addition to individual assessors. Details are forthcoming about the mechanics of certification, but DoD plans to establish a marketplace for 3PAOs to be evaluated and hired by contractors seeking certification.

How Varonis helps fast track CMMC 2.0 compliance

Getting started with CMMC might seem like a daunting task, and the reality is that certification is simply too large of a program to be handled by one person or perhaps even one team within an organization. Nevertheless, certification will be a nonnegotiable requirement of DoD contractors going forward, and Varonis can help federal contractors get started right away.

The best place to start when starting to operationalize CMMC is in Domains. Recall that these are “centers of excellence” with tasks and management that must be performed and continuously optimized for organizations to achieve and advance their levels of certification. Recall also that the primary goal of CMMC is the protection of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

The Varonis Data Security Platform can facilitate, execute and automate a large number of the 170+ Practices and their related Processes within the CMMC model.

How Varonis maps to CMMC 2.0 domains and practices

Here's how Varonis can help organizations achieve data security as expected by the GDPR:

CMMC 2.0	How Varonis helps
Domain – Access Control	**Varonis:**
Practice ○ Authorized Access Control - AC L1-31.1 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). ○ Transaction & Function Control - AC.L1-3.1.2 - Limit information system access to the types of transactions and functions that authorized users are permitted to execute. ○ External Connections – AC.L1-3.1.20 - Verify and control/limit connections to and use of external information systems. ○ Control CUI Flow - AC.L2-3.1.3 - Control the flow of CUI in accordance with approved authorizations. ○ Separation of Duties- AC.L2-3.1.4- Separate the duties of individuals to reduce the risk of malevolent activity without collusion. ○ Least Privilege- AC.L2-3.1.5 - Employ the principle of least privilege, including for specific security functions and privileged accounts. ○ Non-Privileged Account Use -AC.L2-3.1.6- Use non-privileged accounts or roles when accessing nonsecurity functions. ○ Privileged Functions - AC.L2-3.1.7 - Prevent non-privileged users from	○ AC L1-31.1 - A complete permissions map of access controls for users / groups to unstructured data data stores; intelligently makes decisions to remove risky permissions across your cloud collaboration platforms and corporate file systems predictably and at scale. ○ AC.L1-3.1.2 - Identify unusual behavior, unauthorized access of data, and attack patterns on unstructured data and authentication systems. ○ AC.L1-3.1.20 - All service accounts are mapped and controllable through the Varonis Platform, integrates with ServiceNow and other ITSM platforms. ○ AC.L2-3.1.3 - Varonis provides first-party authorization capabilities for data and file shares applies granular policies to label CUI and integrates with EDR and DLP. ○ AC.L2-3.1.4- Varonis enables organization-defined ethical walls to enforce segregation of access. ○ AC.L2-3.1.5 - Varonis DSP establishes least-privilege entitlement model for unstructured data; identify privileged accounts (admins, VIPs) and over-privileged accounts; Automation Engine does it fast. ○ AC.L2-3.1.6- Varonis DSP's ACL discovery and mapping; least-privileged

executing privileged functions and capture the execution of such functions in audit logs. ○ Unsuccessful Logon Attempts - AC.L2-3.1.8- Limit unsuccessful logon attempts. ○ Session Termination - AC.L2-3.1.11 - Terminate (automatically) a user session after a defined condition. ○ Control Remote Access- AC.L2-3.1.12 - Monitor and control remote access sessions. ○ Wireless Access Authorization - AC.L2-3.1.16- Authorize wireless access prior to allowing such connections. ○ Encrypt CUI on Mobile – AC.L2-3.1.19 - Encrypt CUI on mobile devices and mobile computing platforms.	maintenance. Varonis provides entitlement reviews. ○ AC.L2-3.1.7 - Varonis provides complete audit trail and access logs; manages ACLs and entitlement reviews. Incorporates threat models that detect abnormal administrative activity from non-privileged users. ○ AC.L2-3.1.8 - Disable user machines, change passwords, or reduce privileges based on predefined rules and triggers in Varonis. ○ AC.L2-3.1.11- Varonis DSP alerts on built-in threat model triggers in addition to any user-defined rules; automate responses with PowerShell scripting for direct response to alerted threats. ○ AC.L2-3.1.12 - Varonis can monitor VPN sessions of remote users and shut down suspicious behavior. ○ AC.L2-3.1.16 - Specify permitted (whitelist) network connections in Varonis. ○ AC.L2-3.1.19 - Federal Policy Pack identifies CUI; Data Classification Labels automatically adds the appropriated labels and integrates with Microsoft MIP for encryption.
Awareness and Training	**Varonis**
○ Role-Based Training- AT.L2-3.2.2 - Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Professional Services can train teams and optimize their Varonis platform tools for the unique circumstances of any data and networks within supported technology environments.

Audit and Accountability	Varonis
○ System Auditing - AU.L2-3.3.1 - ○ 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. ○ User Accountability - AU.L2-3.3.2 - Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. ○ Event Review - AU.L2-3.3.3 - Review and update logged events. ○ Audit Failure Alerting - AU.L2-3.3.4 - Alert in the event of an audit logging process failure. ○ Audit Correlation - AU.L2-3.3.5 - Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. ○ Reduction & Reporting - AU.L2-3.3.6 - Provide audit record reduction and report generation to support on-demand analysis and reporting. ○ Authoritative Time Source - AU.L2-3.3.7 - Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. ○ Audit Protection - AU.L2-3.3.8 - Protect audit information and audit logging tools from unauthorized access, modification, and deletion. ○ Audit Management - AU.L2-3.3.9 - Limit management of audit logging functionality to a subset of privileged users.	○ AU.L2-3.3.1 - Varonis creates human-readable, enriched audit logs across multiple platforms suitable for long-term retention. ○ AU.L2-3.3.2 - Varonis provides an immutable audit trail of activity linking user accounts, service accounts, admin accounts and VIPs to resolved IP addresses and/or device names. ○ AU.L2-3.3.3 - Varonis provides a full audit trail of all users and objects in the monitored and protected data environments. ○ AU.L2-3.3.4 - Reports and logs on function and health of audit, enrichment and data collection systems; anonymized health monitoring system to ensure audit system stability. ○ AU.L2-3.3.5 - Centralizes audit log review, correlation, alerting/ threat analysis, and reporting of activity on unstructured data into a single platform, simplifying investigations into suspicious activity. ○ AU.L2-3.3.6 - Normalizes audit information from multiple platforms to ensure human-readability, while preserving critical identifying information. ○ AU.L2-3.3.7 - Varonis provides a full audit trail with time stamps that can be correlated to the internal clocks of all systems it monitors. ○ AU.L2-3.3.8 - Varonis offers a granular, role-based system to manage access to Varonis functions, including system management, audit data, alerts, and reporting. ○ AU.L2-3.3.9 - Varonis supports the limiting of management of audit / record retention to privileged user accounts.

Configuration Management	Varonis
○ Security Configuration Enforcement - CM.L2-3.4.2- Establish and enforce security configuration settings for information technology products employed in organizational systems. ○ System Change Management - CM.L2-3.4.3 - Track, review, approve or disapprove, and log changes to organizational systems. ○ Security Impact Analysis - CM.L2-3.4.4 - Analyze the security impact of changes prior to implementation. ○ Access Restrictions for Change - CM.L2-3.4.5 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. ○ User-Installed Software - CM.L2-3.4.9- Control and monitor user-installed software.	○ CM.L2-3.4.2 - Varonis integrates with ITSM including ServiceNow to manage authentication and configuration for numerous services through a single interface. ○ CM.L2-3.4.3 - Varonis logs changes to permissions and group entitlements, and a means to understand their impact with regards to access gained / lost to the unstructured data stores; Varonis empowers data owners with access controls. ○ CM.L2-3.4.4 - Varonis provides previews of impact of potential changes to ACLs and data schemas before committing them. ○ CM.L2-3.4.5 - Varonis provides mapping, an audit trail, and reporting on data systems; Varonis enables approval workflows between data requestors and owners. ○ CM.L2-3.4.9 - Varonis can identify the installation of user software.
Identification & Authentication	**Varonis**
○ Identification - IA.L1-3.5.1- Identify information system users, processes acting on behalf of users, or devices. ○ Authentication - IA.L1-3.5.2- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. ○ Replay-Resistant Authentication - IA.L2-3.5.4- Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	○ IA.L1-3.5.1 - A complete catalog of users, groups, and devices that exist on the network, linked to an activity history; automatic identification of service accounts, admins, executives, and other privileged accounts ○ IA.L1-3.5.2 - Auto-identification of privileged users, service accounts, and individual users to adjust the monitoring of user accounts based on their role, user / device pairings; comparison of current activity to behavioral baselines to verify that users are acting as expected. ○ IA.L2-3.5.4 - Detect replay attacks and analyze Kerberos and NTLM

○ Identifier Handling- IA.L2-3.5.6- Disable identifiers after a defined period of inactivity. ○ Cryptographically-Protected Passwords - IA.L2-3.5.10- Store and transmit only cryptographically-protected passwords. ○	authentications for unusual patterns indicative of potential compromise. Set policies to discontinue access after a set period of time. ○ IA.L2-3.5.6 - Varonis identifies user accounts that have not logged in for a predefined period; identifies user account entitlements to data that have not been used in a predefined period. ○ IA.L2-3.5.10 - Disable user machines, change passwords, or reduce privileges based on predefined rules and triggers in Varonis.
Incident Response	**Varonis**
○ Incident Handling- IR.L2-3.6.1 - Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. ○ Incident Reporting - IR.L2-3.6.2 - Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. ○ Incident Response Testing - IR.L2-3.6.3- Test the organizational incident response capability.	○ IR.L2-3.6.1- Varonis surfaces potential threats based on behavior based threat models, contain threats with automated responses via PowerShell; IRT augments in-house Proactive Incident Response, Forensics Team SOC teams. ○ IR.L2-3.6.2 - Varonis offers robust reporting across the entire span of monitored and protected data environments. ○ IR.L2-3.6.3 - Incident response and forensics team to assist customers with testing incidence response and defense capabilities.
Maintenance	**Varonis**
○ Equipment Sanitization- MA.L2-3.7.3- Ensure equipment removed for off-site maintenance is sanitized of any CUI.	○ Federal Policy Pack identifies CUI; Varonis scrubs any data store of specified data on command. Comprehensive data classification that comes preconfigured to detect PII of many kinds, and is extensible to locate and tag Controlled Unclassified Information (CUI) on equipment in need of repair.

Media Protection	Varonis
○ Media Disposal - MP.L1-3.8.3 - Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. ○ Media Access - MP.L2-3.8.2 - Limit access to CUI on system media to authorized users. ○ Media Markings- MP.L2-3.8.4 - Mark media with necessary CUI markings and distribution limitations. ○ Media Accountability- MP.L2-3.8.5 - Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. ○ Portable Storage Encryption- MP.L2-3.8.6 - Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. ○ Protect Backups - MP.L2-3.8.9- Protect the confidentiality of backup CUI at storage locations.	○ MP.L1-3.8.3 - Varonis comes preconfigured to identify sensitive information of many kinds; + Federal Policy Pack adds policies to locate and quarantine Controlled Unclassified Information (CUI) on unstructured data stores. ○ MP.L2-3.8.2 - Varonis maps the entire data environment; Varonis features automated entitlement reviews and AI-powered recommendations on user-defined schedules. ○ MP.L2-3.8.4 - Comprehensive unstructured data classification that comes preconfigured to detect PII of many kinds, and is extensible to locate Controlled Unclassified Information (CUI) on the network to ensure it is marked appropriately. Files that contain CUI can, via integration with Microsoft Information Protection, be labelled to identify and protect their content. ○ MP.L2-3.8.5 - Varonis+Federal Policy Pack identifies; Data Classification Labels applies persistent labels to data; Varonis control and lock down access to CUI. ○ MP.L2-3.8.6 - Varonis identifies CUI data; Data Classfication Labels applies persistent labels to data and integrates with Microsoft MIP for file encryption. ○ MP.L2-3.8.9 - Varonis monitors and responds to threats on data anywhere in the data estate.
Personnel Security	**Varonis**
○ Personnel Actions - PS.L2-3.9.2 - Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	○ PS.L2-3.9.2 - Identify effective permissions before and after a termination or transfer of a user to ensure that CUI is identified, protectected and

	that unwarranted access to CUI is properly revoked.
Physical Protection	**Varonis**
○ Alternative Work Sites - PE.L2-3.10.6- Enforce safeguarding measures for CUI at alternate work sites.	○ PE.L2-3.10.6 - Varonis covers Microsoft 365 and additional cloud repositories which enables organizations to work from anywhere securely; Varonis enrich the user and entity behavior analytics with network intelligence for greater detail.
Risk Assessment	**Varonis**
○ Risk Assessments - RA.L2-3.11.1- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. ○ Risk Assessments - RA.L2-3.11.2- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. ○ Vulnerability Remediation - RA.L2-3.11.3 - Remediate vulnerabilities in accordance with risk assessments.	○ RA.L2-3.11.1 - Professional Services can optimize and train teams to use the Varonis platform for the unique circumstances of any data and networks within supported technology environments. ○ RA.L2-3.11.2 - Varonis comes loaded with dozens of reports that can be scheduled according to organizational needs; dashboards highlight exploitable configurations in Active Directory. ○ RA.L2-3.11.3 - Varonis maintains a full audit trail for the monitored data environments; Varonis remediates broken ACLs and permissions at scale.
Security Assessment	**Varonis**
○ Security Control Assessment - CA.L2-3.12.1 - Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. ○ Plan of Action - CA.L2-3.12.2 - Develop and implement plans of action	○ CA.L2-3.12.1- Varonis maps the entire data environment for a full view of potential vulnerabilities; Cyber Resiliency Assessment can assess vulnerabilities and exposure. ○ CA.L2-3.12.2 - Varonis maps the entire data environment for a full view, audit

designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. ○ Security Control Monitoring - CA.L2-3.12.3 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. ○ System Security Plan - CA.L2-3.12.4 - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	trail, and reporting of vulnerabilities in data stores. ○ CA.L2-3.12.3 - Varonis features scheduled reporting on all aspects of data risk and security; Varonis surfaces risks and threats in real time. ○ CA.L2-3.12.4 - Varonis maps the entire data environment for a full view of data stores and potential vulnerabilities to document.
System & Communication Protection	**Varonis**
○ Boundary Protection - SC.L1-3.13.1- 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. ○ Role Separation - SC.L2-3.13.3 - Separate user functionality from system management functionality. ○ Shared Resource Control- SC.L2-3.13.4 - Prevent unauthorized and unintended information transfer via shared system resources. ○ Split Tunneling - SC.L2-3.13.7 - Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). ○ Data in Transit - SC.L2-3.13.8 - Implement cryptographic mechanisms to prevent unauthorized disclosure of	○ SC.L1-3.13.1 - Varonis covers the entire data domain with controls on movement within and a full audit trail; Data Classification Labels prevents sensitive data from leaving the network; Varonis detects and prevents unauthorized data exfiltration. ○ SC.L2-3.13.3 - Varonis maintains and manages discrete ACLs for users, groups, services and other roles. ○ SC.L2-3.13.4 - Detect unauthorized data exfiltration and shut down connections and machines; monitor and prevent misuse of data sent through shared links in Microsoft 365. ○ SC.L2-3.13.7 - Varonis can prevent multiple sessons from the same device on the network. ○ SC.L2-3.13.8 - Data Classification Labels integrates with Microsoft Information Protection for data encryption.

CUI during transmission unless otherwise protected by alternative physical safeguards. ○ Connections Termination- SC.L2-3.13.9- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. ○ CUI Encryption - SC.L2-3.13.11 - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. ○ Communications Authenticity - SC.L2-3.13.15 - Protect the authenticity of communications sessions. ○ Data at Rest - SC.L2-3.13.16- Protect the confidentiality of CUI at rest.	○ SC.L2-3.13.9 - Varonis can terminate user sessions based on conditions set by the organization. ○ SC.L2-3.13.11 - Varonis supports FIPS policies enabled on application core components and during data collection of information pertaining to CUI; Data Classification Labels applies labels to data to be encrypted. ○ SC.L2-3.13.15- Identify abnormalities in Kerberos / NTLM authentication exchanges between systems to identify pass-the-ticket, silver ticket, and similar Active Directory attacks. Capability to limit access to CUI to only the people that need to access it ○ SC.L2-3.13.16 - Identify and classify unstructured CUI data at-rest on multiple platforms. Capability to limit access to CUI to only the people that need to access it. Threat models that detect abnormal activity on CUI at rest.
System & Information Integrity	**Varonis**
○ Flaw Remediation - SI.L1-3.14.1 - Identify, report, and correct information and information system flaws in a timely manner. ○ Malicious Code Protection - SI.L1-3.14.2- Provide protection from malicious code at appropriate locations within organizational information systems. ○ Security Alerts & Advisories- SI.L2-3.14.3 -Monitor system security alerts and advisories and take action in response. ○ System & File Scanning- SI.L1-3.14.5 - Perform periodic scans of the information system and real-time scans	○ SI.L1-3.14.1 - Varonis has native reporting via dashboards and PDFs, Automation Engine remediates flaws in ACLs at scale. ○ SI.L1-3.14.2 - Real-time threat detection and analysis that detects both known threats and abnormal behaviors that may indicate insider threats or new malware attacks. ○ SI.L2-3.14.3 - Varonis alerts on built-in threat model triggers in addition to any user-defined rules and abnormalities in learned behavior; automate responses with PowerShell scripting for direct response to alerted threats. ○ SI.L1-3.14.5 - Schedule reporting in Varonis; Real-time threat detection and analysis that detects both known

of files from external sources as files are downloaded, opened, or executed. ○ Monitor Communications for Attacks - SI.L2-3.14.6- Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. ○ Identify Unauthorized Use - SI.L2-3.14.7 - Identify unauthorized use of organizational systems.	threats and abnormal behaviors that may indicate insider threats or new malware attacks w/ data enrichment and additional threat intel from Edge; Varonis identifies information as it is created. ○ SI.L2-3.14.6 - Log, baseline, and alert on users and devices connecting from outside the organization or communicating with devices outside the organization from within to identify unusual behavior consistent with compromise, malicious use, or exfiltration of data. ○ SI.L2-3.14.7 - Audit and track all activity on unstructured data; alert on unusual activity, unexpected first-time access to data.

Conclusion

The Cybersecurity Maturity Model Certification will impact each and every one of the 300,000-plus companies in the United States defense industrial base. Companies that are already familiar with and adhering to NIST, FAR, and DFARS will likely have first-mover advantage in advancing through CMMC, but Varonis can accelerate any company's CMMC with a powerful platform for compliance and security.

Contact the Varonis Federal team for a free Data Risk Assessment, and level up your Cybersecurity Maturity Model Certification.

Schedule a free data risk assessment.

Varonis can help manage your security risk and comply with GDPR by identifying where you have sensitive data, reducing that data's blast radius, and monitoring that data for potential threats. To see where you have GDPR data across your environment, sign up for a free GDPR risk assessment.

Our complimentary assessment run by expert forensics and incident response analysts will help you find and classify regulated data across on-premises and cloud data stores, measure data exposure, and alert on suspicious access to regulated information.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyber threats from both internal and external actors by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, Zero Trust, compliance, data privacy, classification, and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.