MENLO SECURITY

Implementing CMMC 2.0 with Menlo Secure Enterprise Browser Solution

The Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the U.S. Department of Defense (DoD) to enhance the cybersecurity posture of its contractors. These contractors must meet specific cybersecurity standards to protect sensitive unclassified information, particularly Controlled Unclassified Information (CUI), from cyber threats. This document identifies how Menlo Security can help Defense Industrial Base (DIB) partners comply with the DoD Cybersecurity Maturity Model Certification (CMMC) 2.0.

The Menlo Secure Enterprise Browser solution supports the journey to CMMC 2.0 compliance by adopting a zero-trust approach to browser security. Built on a cloud-delivered platform, Menlo isolates browsing activities from endpoints, eliminating web-borne threats before they can infiltrate local devices or networks. Additionally, Menlo Last-Mile Data Protection enhances data integrity and confidentiality by providing protection controls beyond traditional DLP.

TEHCNICAL BRIEF

How Menlo Supports CMMC 2.0 Compliance

CMMC 2.0 includes three levels of cybersecurity maturity:

- **Level 1 (Foundational):** Requires 17 basic practices to safeguard Federal Contract Information (FCI).
- **Level 2 (Advanced):** Aligns with NIST SP 800-171's 110 practices to protect CUI.
- **Level 3 (Expert):** Builds on Level 2 with additional NIST SP 800-172 requirements for proactive threat detection.

The Menlo Secure Enterprise Browser solution helps organizations across all levels by ensuring strict access controls, activity monitoring, and session protection—critical components for securing FCI and CUI.

Granular Access Controls

Access Control

- **Zero Trust Access for CUI and FCI:** Menlo Secure Application Access (SAA) enforces least-privilege access policies. Users must authenticate into the platform via mechanisms such as SAML IDPs, enabling full user attribution for browsing activities (downloads, uploads, web access).
- **Session Monitoring and Logging:** All actions, such as accessing URLs or transferring data, are logged and analyzed in real-time, with detailed logs (username, URL, browser version) exported to SIEM tools for further analysis.

Enhancing Data Security and Integrity

Menlo browser isolation capabilities prevent web-based attacks by securely processing content in a cloud container, keeping threats away from endpoints. Menlo Last-Mile Data Protection goes beyond conventional DLP, offering granular data protection.

Data Security

- **Isolation Technology for Secure Browsing:** Web content is processed remotely in the cloud, isolating malicious code from user endpoints.
- **Advanced DLP Controls:** Menlo enables comprehensive DLP policies, including restricting file downloads/uploads, copy-paste, user input, and more. This ensures that sensitive data is not exposed, shared, or leaked.

Last-Mile Data Protection

Menlo Last-Mile Data Protection provides controls specifically designed to support compliance:

- **Copy/Paste Controls:** Prevents unauthorized sharing by limiting copy-paste actions in browser sessions, including blocking pasting into generative AI websites such as ChatGPT.
- **User-Input Limits:** Restricts input into specific fields on web forms to protect against inadvertent data leaks.

- **Watermarking and Data Redaction:** Ensures that documents accessed or downloaded are traced with visual identifiers, and sensitive data is masked to prevent exposure.

This layered data security approach allows full inspection of sensitive data during all web interactions, from file transfers to form submissions.

Continuous Monitoring and Incident Response

To align with CMMC's requirement for continuous monitoring, Menlo provides centralized visibility and real-time alerts on browsing activities, suspicious behavior, and access attempts.

Browsing Forensics for Session Monitoring and Incident Analysis:

Menlo Browsing Forensics offers in-depth monitoring of all web session activities. It captures a detailed history of user interactions, including visited URLs, file downloads, uploads, and data input. These logs facilitate:

- **Incident Response:** Enabling quick analysis and response to any suspicious or unauthorized behavior.
- **Threat Analysis:** Full integration with SIEM tools for deeper threat detection and behavioral analysis.
- **User Attribution:** Providing full accountability for user actions to ensure compliance and proper auditing of access to CUI or FCI.

Browser Posture Manager (BPM) for Security Posture Compliance:

Menlo Browser Posture Manager (BPM) is designed to maintain secure browsing configurations that align with an organization's security policies and compliance frameworks. BPM verifies that users' browsers meet security policy standards before they can access sensitive data or applications. This includes:

- **Browser Settings and Extensions:** Ensuring that security-critical settings are enabled and compliant, and extensions meet policy requirements
- **Security Baseline Compliance:** Supporting compliance with industry standards (such as the CIS benchmarks), BPM ensures that the browser posture remains compliant even as policies evolve or change.

By maintaining a consistent and compliant security posture, BPM supports secure access while mitigating the risk of browser-based threats and non-compliance due to misconfigurations.

Specific CMMC Practices and Menlo Capabilities

The advantage of providing a secure enterprise browser solution that integrates cloud-based browser isolation with robust DLP capabilities provides for full inspection of potentially sensitive data including file uploads and downloads, POSTs, and GETs. The Menlo Secure Cloud Browser can inspect and block unwanted data exposure based on pre-built or custom DLP dictionaries, including REGEX and string values. Menlo protects against releasing unprotected information to the local browser endpoints and stops it from being leaked

into web applications such as ChatGPT. For instance, the copy and paste controls can prevent pasting into generative AI (GenAI) websites such as ChatGPT and Menlo Browsing Forensics can be used to see the entire history of a web session if an employee went through a GenAI website. This will provide an organization with the ability to identify if and how controlled unclassified information (CUI) was leaked, including user attribution.

The Menlo Secure Enterprise Browser solution does not require organizations to procure additional software or hardware, install or manage any kind of a thick client or agent on the client endpoint.

The paragraphs that follow discuss specific CMMC security requirements and corresponding Menlo Secure Enterprise Browser solution capabilities that help fulfill them.

AC.L2-3.1.1 – Limit System Access to Authorized Users and Devices
Menlo enforces access controls by integrating with SAML-based IDPs (Identity Providers), including common DoD directories such as the Global Federated User Directory (GFUD). Every user must authenticate before gaining access to any web-based resource through the Secure Cloud Browser, ensuring that only authorized users are allowed entry.

AC.L2-3.1.2 – Limit System Access to the Types of Transactions and Functions Authorized Users Can Perform
The Menlo policy engine provides fine-grained access control to web applications, allowing organizations to define, based on least privilege, what data can be viewed, downloaded, or shared by authorized users.

AU.L2-3.3.1 – SYSTEM AUDITING
Menlo Security provides Audit logs containing information pertaining to Admin access to the Menlo admin console. These Audit Logs can be ingested via API into a SIEM tool for additional analysis and alerting. Audit logs contain information about Administrator identity and any changes made by the Administrator. Audit Logs also include failed attempts to access the Menlo Admin console. Access rights to the Menlo console can integrate with SAML based IDP, which can support MFA. Access privileges within the Admin Console can be configured using RBAC roles.

AU.L2-3.3.2 – USER ACCOUNTABILITY
Menlo Security has full user attribution for web browsing traffic crossing the Menlo Secure Cloud Browser. All users must authenticate into the platform, typically via a SAML IDP, such as the GFUD (Global Federated User Directory) used by a majority of the DOD. Once the user has authenticated, full user attribution occurs relative to web events (web browsing, downloads, uploads). Menlo logs all activity and provides those logs in the Menlo Admin console and via Logging API for ingestion into SIEM tools. Web Log events include username, URL, domain, category, timestamp, browser version, region, SRC_IP, DST_IP, Threat type (if applicable), Virus family (if applicable) and more. Logs can be ingested into SIEM and analytic tools for threat analysis, alerting and AI analysis. Menlo also provides scheduled and customized Reporting functionality.

SC.L2-3.13.13 – MOBILE CODE

Mobile code technologies, including Java, JavaScript, ActiveX, and VBScript, can harbor malware. Menlo Security brings mobile code risk under control. The Menlo Secure Cloud Browser first removes 3rd party mobile code from web pages. Then, it offers Adaptive Clientless Rendering (ARC) to display a web page to a user without delivering risky mobile code to the local browser. In a legacy web browsing experience, a user who visits a site such as cnn.com would execute JavaScript code from numerous 3rd party entities. This code represents a risk to the organization if it is executed on the endpoint. Using remote browser isolation capabilities, the Secure Cloud Browser removes this risk by executing the JavaScript in an isolated container in the cloud. The webpage is then rendered down to the endpoint without including any of the original JavaScript or HTML. This process removes thousands of potentially harmful JavaScript and HTML lines for every webpage load. (JavaScript usage varies from site to site) The Menlo Secure Cloud Browser can be utilized on desktop, laptop, and mobile devices. All major browsers (Chrome, MS Edge, Firefox, Safari, Safari OS, and others) are supported.

SC.L2-3.13.15 – COMMUNICATIONS AUTHENTICITY

The Menlo Secure Cloud Browser combined with Menlo HEAT Shield makes session hijacking virtually impossible. Menlo Security stores session cookies in encrypted storage. Additionally, there are two distinct sessions, and simply obtaining local session cookies would not allow a malicious actor to uncover the session cookies between the Cloud Browser and the downstream resource.

SI.L1-3.14.2 – MALICIOUS CODE PROTECTION

The Menlo Secure Cloud Browser can be used in conjunction with other tools to meet this requirement. Menlo does not *detect* malicious code on an endpoint; however, Menlo can dramatically reduce the amount of potentially malicious code that is executed on an endpoint system (ex: laptop) via the web browser, thereby dramatically reducing the attack surface area. From the standpoint of 'Protecting' against malicious code exploits, Menlo reduces the overall exposure to web-borne malicious exploits by removing 3rd party JavaScript and HTML from website rendering. This is the fundamental security concept of Menlo, to dramatically reduce the exposure to potentially malicious code in the web browser, by simply not sending the original web contents to the endpoint in the first place. No "Good or Bad" determination is necessary, as the original code is not sent across Menlo isolation to the trusted network.

Menlo does inspect file downloads from the Internet for malicious content. Any content determined to be malicious would be blocked and not allowed into the trusted network. This inspection extends to password-protect files.

SI.L1-3.14.5 – SYSTEM & FILE SCANNING

Menlo Security inspects file downloads from the Internet for malicious content. Any content determined to be malicious would be blocked and not allowed into the trusted network. Menlo scans files and documents when a file download is initiated.

Additionally, Menlo identifies password-protected files and can prompt the user to enter the password so full inspection can take place. The ability to open and inspect a password-protected file is a feature that is not widely available outside of Menlo.

Downloads inspections include:

- Hash Check
- AV Scan

Menlo provides policy options to restrict users from downloading various file types. This can be used to prevent users from downloading files such as EXE or script files.

Additionally, Menlo Security can also detect and scan when HTML smuggling is attempting to download a malicious file. This is an attack vector that would typically evade network-based sandbox tools and Secure Web Gateways (SWG). As the name suggests, HTML Smuggling can smuggle file contents within HTML that are then compiled locally on the user's browser. Because the malicious file is created after the packets have crossed the wire, they are not seen by network-based tools. In isolation however, this document would be visible as a download at the cloud browser and would be subject to full inspection.

SI.L2-3.14.6 – MONITOR COMMUNICATIONS FOR ATTACKS

The Menlo Secure Cloud Browser can be used in conjunction with other tools to meet this requirement. Menlo Security can detect certain malicious activity and provide threat logs to other internal tools, such as a SIEM which can provide alerting. For example, if a machine is reaching out to a command and control (C&C) network via the web browser, this would get blocked and logged by Menlo as a "Threat".

Additional Threat types include:

- Phishing
- Malware
- Malicious File Download
- C&C Network
- Botnet
- Malvertising
- Spam
- Compromised Host
- Parked Domains
- Flash
- Uncategorized Site
- Vulnerable Service

Simply detecting and mitigating threats are insufficient in today's threat landscape, often leaving endpoints exposed to new 'Zero Day' threats as they emerge. Threats must be separated from endpoints, applications, and networks to eliminate the threat of infection.

Advantages of the Menlo Security Approach to CMMC

- **Integrated Cloud-Based Solution:** Menlo Secure Enterprise Browser solution requires no thick clients or additional hardware, offering seamless cloud-based security.
- **Enhanced Data Inspection:** The Menlo solution ensures all web traffic, data transfer, and file interactions are fully inspected for compliance.
- **Zero Trust Access:** Enforcing a zero-trust model for web traffic limits access to CUI based on policy-driven controls, reducing exposure to threats.
- **Detailed Reporting and Visibility:** Menlo provides detailed logs and custom reporting features, giving visibility into user activities and compliance adherence.
- **Alignment with NIST SP 800-171/172 Standards:** The Menlo capabilities are aligned with NIST standards that underpin CMMC 2.0, making it easier to comply with all maturity levels.

Achieving and maintaining CMMC 2.0 compliance requires robust security practices and controls to manage web-borne threats and ensure data protection. The Menlo Secure Enterprise Browser solution includes the necessary capabilities, including zero-trust access, cloud-based DLP, and continuous monitoring, making it a valuable tool for Defense Industrial Base contractors to secure FCI and CUI effectively.

For more information on how Menlo Security can support your CMMC compliance efforts, visit the Menlo Security website.

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com