Need It or Overspend?

A CMMC Level 2 Technology Rubric

CMMC Level 2 assesses the 110 security requirements in NIST SP 800-171 Rev 2. None of them names a product, and no product is "CMMC certified." Many requirements are met with policy, process or settings you already own.

This brief gives you an overview of what you need to spend on and what you can skip.

01

Technologies You Must-have

These nine map directly to Level 2 requirements that apply to nearly every contractor handling CUI. Check what you already own before you buy. Microsoft 365, Windows and your firewall often cover more than you think.

TECHNOLOGY	WHY YOU NEED IT	NIST 800-171 REFS	BUDGET-SMART WAY TO MEET IT
Identity and access management	Unique accounts, least privilege, and limits on who can see CUI	3.1.1, 3.1.2, 3.1.5, 3.5.1, 3.5.2	The directory you likely already have (Entra ID, Active Directory, Google Workspace)
Multi-factor authentication	Required for privileged accounts and for network access to all accounts	3.5.3	Built into most identity platforms; authenticator apps or FIDO keys
FIPS-validated encryption for CUI	CUI must be protected in transit and at rest with FIPS-validated cryptography	3.13.8, 3.13.11, 3.13.16	Encrypted email and file sharing for the people who handle CUI; BitLocker or FileVault in FIPS mode on laptops

TECHNOLOGY	WHY YOU NEED IT	NIST 800-171 REFS	BUDGET-SMART WAY TO MEET IT
FedRAMP Moderate (or equivalent) cloud	Any cloud service that stores or sends CUI must meet FedRAMP Moderate equivalency	DFARS 252.204-7012	Put only CUI in the compliant service. The rest of the business can stay where it is.
Endpoint protection	Malware protection with automatic updates and scanning	3.14.2, 3.14.4, 3.14.5	Microsoft Defender or your existing antivirus, centrally managed
Patching and vulnerability scanning	Scan for vulnerabilities and fix flaws on a schedule	3.11.2, 3.11.3, 3.14.1	Built-in update management plus a scanner; many MSPs include this
Audit logging and review	Log user activity, protect the logs and review them	3.3.1 to 3.3.9	Central log collection with a documented review routine. A full SIEM isn't required for very small orgs 1-3 PCs but beyond that a SIEM should be strongly considered to meet real time event correlation requirements
Firewall and boundary protection	Monitor and control traffic at the network edge; deny by default	3.13.1, 3.13.5, 3.13.6	A business-grade firewall configured deny-by-default
Configuration management	Documented secure baselines and control over what software runs	3.4.1, 3.4.2, 3.4.8	Group Policy, Intune or your MDM; application allow-listing

Several requirements that sound like technology are mostly process: security awareness training (3.2), incident response (3.6), physical protection (3.10), and your System Security Plan (SSP) and Plan of Action and Milestones (POA&M). Low-cost training and a well-kept document set are enough for most small contractors.

02

It depends

These technologies are required only if your environment has the thing that triggers them. If the answer to the trigger question is no, you don't need them.

TECHNOLOGY	TRIGGER QUESTION	NIST 800-171 REFS	IF YES
Secure remote access (VPN or equivalent)	Do people reach CUI systems remotely?	3.1.12 to 3.1.15, 3.13.7	Encrypted, monitored remote access through managed access points
Mobile device management	Do phones or tablets access CUI?	3.1.18, 3.1.19	MDM with device encryption, or keep CUI off mobile entirely
Wireless security	Is there Wi-Fi on the network where CUI lives?	3.1.16, 3.1.17	WPA2/WPA3 Enterprise with authentication; separate guest Wi-Fi
Removable media controls	Does anyone put CUI on USB drives?	3.8.7, 3.8.8	Block USB storage by default, or allow only encrypted, company-owned drives
Encrypted backups	Do you back up systems that hold CUI?	3.8.9	Encrypt backups and protect where they're stored
Managed service provider (MSP/MSSP)	Do you lack staff to run the must-haves?	Scoped as an External Service Provider	Choose one that can show how its services support your SSP
Enclave or segmented environment	Does CUI touch only part of your company?	Scoping decision	Protect only the enclave rather than hardening the whole company

03

Common overspends

These get pitched as "required for CMMC." None is required by a Level 2 requirement. Some are worth buying for other reasons, but not because an assessor demands them.

WHAT GETS PITCHED	WHAT LEVEL 2 ACTUALLY REQUIRES	THE RIGHT-SIZED ALTERNATIVE
Moving the whole company to GCC High	FedRAMP Moderate-equivalent protection for CUI only	Put the people and data that handle CUI in a compliant enclave
Enterprise SIEM with a 24/7 SOC	Logs that are collected, protected and reviewed	Central logging plus a documented weekly review; add managed detection only if you want the coverage
Annual penetration testing	Periodic vulnerability scanning (3.11.2)	A vulnerability scanner run on a schedule
GRC or compliance software platform	An accurate SSP and POA&M	Well-maintained templates. A platform helps at scale, not at 50 people.
DLP, CASB or a zero-trust overhaul	Control of the flow of CUI (3.1.3)	Limit where CUI can go through scoping and access settings you already have
Replacing all hardware	Supported, patched, securely configured systems	Replace only unsupported devices that are in scope
"CMMC-certified" products	Nothing. No product can be CMMC certified.	Ask the vendor which requirements the product helps meet, and how
Protecting everything the same way	Protecting the systems that handle CUI	Scope first, then buy

WORKSHEET

Five questions before you buy anything

1. **Which requirement does this meet?** If the vendor can't name a NIST 800-171 requirement number, be skeptical.
2. **Does it touch CUI or SPD?** If the system is outside your CUI boundary, it doesn't need CMMC-level protection.
3. **Do we already own something that does this?** Check your Microsoft 365 license, operating system features and MSP contract first.
4. **Can we meet it with a policy or a setting instead?** Many requirements are process, not product.
5. **Will we actually run it?** A tool nobody monitors won't pass an assessment. The assessor looks for evidence that it's in use.

Where PreVeil fits

PreVeil's end-to-end encrypted email and file sharing platform meets and supports many of the technology requirements listed above. It protects your CUI in transit and at rest, and helps you create a robust enclave for your environment, which reduces the need to purchase many of these technologies and keep them current.

Prepared for CMMC Summit 2026. This rubric is educational guidance, not legal advice or a substitute for your assessor or RPO. Confirm scope and requirements with them before you make major purchases.