Forescout can help you put CMMC controls into practice

The Forescout platform discovers and assesses every IoT, OT and IT device on your network. Next, it helps you identify, segment and enforce compliance of every connected thing to address these CMMC requirements:

- **Identification & Authentication**: users/devices/applications
- **Configuration Management**: feed device details to real-time CMDB
- **Asset Management**: feed CMDB with accurate data
- **System & Info Integrity**: know who has access to use, change and control data
- **Security Assessment**: define policies & assess by user/role/device category
- **Risk Management**: assess device compliance to quantify risk
- **Access Control**: continuous, policy-based
- **Situational Awareness**: continuous, real-time compliance
- **Media Protection**: detect/block unauthorized digital media
- **System Communications Protection**: segmentation blocks malicious code from spreading across network
- **Incident Response**: accurate log data & third-party orchestration
- **Awareness & Training**: inform users of device noncompliance
- **Maintenance**: prioritize to focus scarce resources
- **Audit & Accountability**: accurate, real-time asset inventory
- **Recovery**: quickly recover to “known good” configuration

CMMC compliance doesn’t require a steep climb. HERE’S HOW FORESCOUT HELPS

- **100% visibility & assessment**
- **NO compliance, NO contracts**

**Implement proven tools**

- **50% of devices on contractors’ networks are unknown***
- **75+ federal government departments/agencies/units supported**
- **10M+ federal endpoints protected**
- **1 source of truth for connected devices**
- **0 agents required**

**Medical Protection**

Failure to meet the appropriate CMMC maturity level will affect your company’s ability to bid on DoD contracts. Other federal agencies are considering adopting versions of these requirements.

**The Cybersecurity Maturity Model Certification (CMMC)** is a unified cybersecurity standard that focuses on the Defense Industrial Base. It applies to every company that does business with the Department of Defense (DoD) and handles controlled unclassified information (CUI). Third-party assessors use the CMMC to determine the cybersecurity maturity of each company’s networks to assess the risk to CUI.

**WHAT are CMMC controls?**

The Enterprise Security Model Certification (CMMC) is a unified cybersecurity standard that focuses on the Defense Industrial Base. It applies to every company that does business with the Department of Defense (DoD) and handles controlled unclassified information (CUI). Third-party assessors use the CMMC to determine the cybersecurity maturity of each company’s networks to assess the risk to CUI.

**WHEN is compliance mandatory?**

Controls to reach maturity levels one through three are already mandatory under NIST SP 800-171. Full CMMC compliance is required by October 1, 2025.

**WHERE can I learn more?**

Watch our webinar: Lessons from the Trenches - CMMC Risk & Reality.

**TAKE THE NEXT STEP**

Need a “cyber Sherpa” to guide you through CMMC compliance and help ensure success? Learn more about how Forescout can help you reach the next level during our Lessons from the Trenches Webinar: CMMC Risk & Reality.