



Predator DNC™ – White Paper CMMC

Technical White Paper

How Predator DNC supports manufacturers with CMMC requirements:

Executive Summary

Manufacturers supporting the U.S. Department of Defense (DoD) must increasingly demonstrate compliance with the Cybersecurity Maturity Model Certification (CMMC) framework. CMMC requires strong access controls, monitoring, secure network configurations, and disciplined protection of sensitive manufacturing data such as Controlled Unclassified Information (CUI).

Predator DNC, a centralized CNC communication and file-transfer platform, supports these requirements by providing controlled, auditable, and secure methods of transmitting CNC programs and related manufacturing files across the shop floor. Predator DNC does not remove FTP entirely — some machines require it — but instead manages and structures its use within a secure, monitored, and properly segmented network, supporting stronger alignment with CMMC expectations.

Predator DNC Overview

Predator DNC is industrial networking software used to transmit CNC programs and machine data to CNC machines, robots, PLCs, CMMs, and other shop-floor devices. It supports Ethernet, wireless, serial (RS-232), and a wide range of machine communication protocols, including FTP where required by OEM specifications.

The primary function of Predator DNC is to centralize the movement of CNC files and add control, visibility, and security to processes that were traditionally manual, inconsistent, or unsecured.

CMMC alignment and supported Controls:

1. Access Control (AC) Centralized, role-based access to CNC files

CMMC requires organizations to enforce strict access policies and identity-based controls for manufacturing data. Predator DNC supports this by:

How It Works:

An operator uses a handheld scanner to read a bar code, QR code, or an RFID tag on a job traveler, part, or fixture. Predator DNC automatically identifies the corresponding CNC program and sends the correct revision to the machine.

Providing centralized permissions that determine who is allowed to send, or receive CNC programs, CNC offsets and other CNC files.

© 1994 – 2025 Predator Software Inc. All rights reserved.

THIS IS A LIVING DOCUMENT. The information contained in this document represents the current view of Predator Software Inc. on the issues discussed as of the date of publication. Because Predator Software Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Predator Software Inc., and Predator Software Inc. cannot guarantee the accuracy of any information presented after the date of publication.

Document Version 12.0.2

Restricting machine access by user, workstation and folder.

Reducing uncontrolled exchanges of sensitive data by replacing ad-hoc processes with governed workflows.

Supporting secure authentication to access Predator DNC.

Even when FTP is used for machine communications, Predator DNC constrains it behind authenticated workflows, preventing uncontrolled direct FTP access from general users.

2. System and Communication (SC) protection with Secure Industrial Networking

CMMC requires protection of data in transit, as well as segmentation of critical equipment. Predator DNC supports secure communication in several ways:

Works Natively within VLANs and Secured Network Segments:

Predator DNC is fully compatible with:

Standard VLANs

Secure VLANs (Locked-down) VLANs

OT/IT network segmentation architectures

Layer – 3 routed networks

Firewalled or access-controlled machine zones

CMMC Benefits include:

Reduced attack surface. Since machines sit in isolated VLANs accessible only through the Predator DNC server with tightly controlled firewall rules

Least privilege networking. Since only necessary ports and protocols are opened to only the required devices.

Improved containment of security incidents. Lateral movement between machines is restricted.

Predator DNC functions cleanly whether the CNC network is flat, partially segmented or fully segmented according to Zero Trust or Defense-in-Depth architectures.

Controlled use of FTP

While Predator DNC supports FTP for CNC machines that require it:

FTP usage occurs within VLAN boundaries, not across open networks.

Firewall rules restrict FTP traffic only between the Predator DNC server and specified machine IPs.

FTP usage is restricted to IP4 addresses, users and passwords for specific CNC machines, robots and CMMs. In addition, specific FTP functions can also be locked down to specific CNC machines, robots and CMMs.

Predator Secure DNC Implementation

Where supported by CNC machines, robots and CMMs, Predator Software also offers Predator Secure DNC which adds authentication and encryption for Ethernet-based communications

3. Audit and Accountability (AU) comprehensive communication logging

CMMC requires continuous monitoring and recording of access and system activity.

Predator DNC provides:

- Full logging of all file transfers per CNC machine, robot or CMM.

- History of uploads and failed communication attempts.

- Logs that can be provided for SIEM or SOC integration.

This creates an audit trail demonstrating controlled access to CUI-bearing CNC, robot and CMM programs which is critical for CMMC Levels 2 and 3.

4. Reducing Risk from legacy processes

Common shop-floor transfer vulnerabilities include:

- Unsecured USB drives.

- Uncontrolled PC to machine, robot or CMM file transfers.

- Open FTP or legacy server use with no or minimal logging

- Untracked program changes/edits on the shop floor

Predator DNC address these risks by:

- Replacing USB based transfers with controlled digital workflows.

- Centralizing file distribution so that any file transfer (even via FTP) is logged

- Preventing direct machine, robot and CMM access from general-purposes PCs

- Ensuring all program movements flow through auditable systems

This aligns directly with CMMC requirements for documented, secure and monitored data flows.

Network security advantages within a CMMC environment

Predator DNC fits naturally into modern CMMC-aligned manufacturing network designs, including:

- Zero Trust OT networks

- Defense-in-Depth network segmentation

- Restricted VLAN architectures

- Firewalled machine/robot/CMM cells

- DMZ-based Predator DNC server placement

- Controlled east-west network traffic

Because Predator DNC relies on predictable, well-defined communication paths, it is ideal for locked-down environments where strict access control and traffic rules are enforced.

Conclusion

Predator DNC supports manufacturers in meeting CMMC requirements by centralizing CNC program access, enforcing role-based controls, supporting secure and segmented network designs, and providing complete auditability of CNC communications. While Predator DNC does not eliminate FTP or other required legacy communication protocols — and often must support it due to shop floor requirements — it transforms FTP and other legacy communications into a controlled, limited, and monitored component of a secure OT/IT communication infrastructure.

By operating effectively within VLANs, secure VLANs, and segmented OT networks, Predator DNC aligns with modern cybersecurity architectures and strengthens a manufacturer's maturity level in preparation for CMMC certification.

Ready to transform your manufacturing operations?

To learn more about how Predator DNC and its integrated solutions can maximize your ROI, improve data security, and prepare your business for the future, contact us at info@predator-software.com or visit our website at www.predator-software.com