SOLUTION BRIEF

How the Nozomi Networks Platform Supports CMMC 2.0 Compliance

Many organizations have no visibility into OT/IoT systems and are unable to manage their risks. Nozomi Networks is the leader in OT/IoT security and visibility.

If your Cybersecurity Maturity Model Certification (CMMC) relevant environment includes OT and IoT devices (specialized assets1), our platform provides the protocol mastery, monitoring techniques, and threat and anomaly detection capabilities that IT-centric security tools don't have.

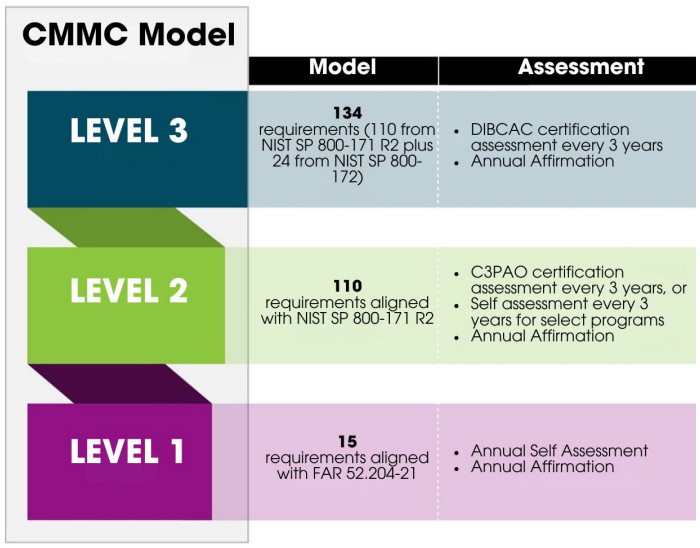
It helps you determine your CMMC 2.0 relevant environment, automatically collect required data for certification, and meet key Level 1, 2 and 3 requirements within 11 of the 14 domains.

Overview of CMMC 2.0

The CMMC program is designed to ensure that sensitive information shared by the U.S. Department of Defense (DoD) with DIB prime and subcontractors through acquisition programs is handled securely during contract performance. Such information is labelled Federal Contract Information (FCI) or Controlled Unclassified information (CUI).

CMMC 2.0 has a maximum of 134 requirements across 14 domains and offers three levels of maturity depending on the type of sensitive unclassified information to be handled per the contract. Level 1 requirements are aligned with FAR 52.204-2. Level 2 is aligned with NIST SP 800-171, and Level 3 includes an additional 24 requirements from SP 800-172.

Before award, contracts are assigned one of the three CMMC levels, based on the type and sensitivity of controlled unclassified information to be handled. If you plan to bid (or be a sub-supplier in a bid) on a DoD contact after October 1, 2025, you must have achieved the required CMMC level specified in the contract to be eligible to bid.



Source: U.S. DoD CIO

As of October 2025 Nozomi Networks has achieved In Process designation at the Moderate impact level under the Federal Risk and Authorization Management Program (FedRAMP®) for its Vantage for Government platform.

How the Nozomi Networks Platform Supports CMMC 2.0 Compliance

CMMC 2.0 requires DoD contractors to safeguard all assets in their relevant environments, including specialized assets such as OT and IoT devices. These assets often operate on proprietary or legacy protocols, lack built-in security controls, and cannot be scanned or patched by traditional IT security tools without risking operational disruption.

For contractors whose relevant environments include OT and IoT assets, this creates a significant compliance challenge. CMMC practices — from asset identification to continuous monitoring and incident response — still apply, but most IT-centric solutions were never designed to address these unique systems. For starters, IT security tools can't read OT and IoT protocols, so they can't understand asset behavior and can't detect threats and anomalies. The Nozomi Networks platform fills this gap.

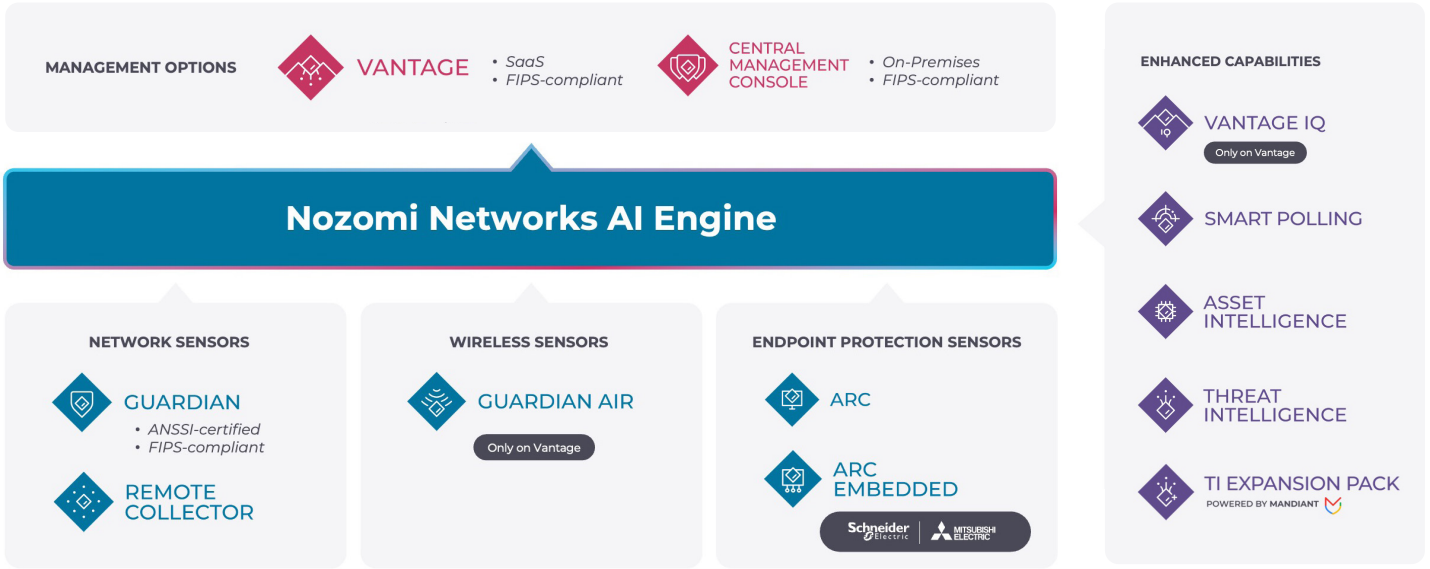
Platform Overview

Purpose built for complex industrial and critical infrastructure environments, the Nozomi Networks platform combines visibility from the endpoint to the air with continuous monitoring and AI-powered analysis to minimize cyber risk and maximize operational resilience. It helps you:

- **See** all OT, IoT and IT devices on your network and understand their behavior.
- **Detect** and prioritize cyber threats, vulnerabilities and anomalies based on their risk .
- **Respond** faster to critical breaches and process control issues with guided remediations.

The Nozomi Networks platform continuously monitors the operational environment to detect vulnerabilities, configuration weaknesses, indicators of compromise (IOCs) and anomalous behavior across OT, IoT and connected systems. AI-enriched asset profiles provide real-time awareness of system flaws and known vulnerabilities.

Our OT/IoT-focused threat intelligence feed helps ensure sensors can detect emerging malware and IOCs, while multi-factor risk scoring prioritizes remediation efforts based on threat exposure and operational criticality. Threat intelligence, anomaly detection and behavioral analytics work together to identify potential compromises early.



Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com