WHITE PAPER

Achieve CMMC Compliance with Tanium

Address certification requirements for continuous visibility, control and compliance.

Tanium supports key technical requirements outlined in CMMC (relative to Tanium products), including:

- 100% of the Risk Assessment family requirements
- Over 75% of the Configuration Management family requirements
- Over 65% of the Incident Response family requirements

Tanium is CMMC Level 2 Certified

Navigating CMMC with confidence

For organizations that process, store, or share Controlled Unclassified Information (CUI) for the Department of War (DoW), achieving Cybersecurity Maturity Model Certification (CMMC) compliance is a strategic imperative, and essential for securing DoW contracts. These organizations need a solution that protects them from cyberattacks and ensures that they are handling sensitive information while meeting specific cybersecurity requirements.

Tanium's Autonomous IT Platform supports many CMMC compliance requirements by providing comprehensive endpoint visibility, automated security controls, and streamlined reporting capabilities to address core compliance requirements with confidence. By consolidating capabilities into a single platform, Tanium simplifies IT security management while cutting costs. The result is improved efficiency without compromising protection.

How does Tanium help achieve CMMC compliance?

The Tanium platform provides an integrated solution that aligns directly with many of CMMC's technical controls while delivering significant operational benefits:

- **Real-time visibility:** Tanium offers continuous monitoring of all endpoints, ensuring that organizations have real-time visibility into their IT environment. This is crucial for maintaining asset management and security controls required by CMMC.
- **Proactive security hygiene:** By continuously assessing and improving the security posture of endpoints, Tanium helps organizations maintain strong security hygiene, which is essential for meeting the CMMC foundational cybersecurity requirements.
- **Autonomous endpoint management:** Tanium automates patch and configuration management, ensuring that all systems are up-to-date and compliant with security policies. This helps meet the configuration management and maintenance requirements of CMMC.
- **Automated incident response:** Tanium provides tools for rapid detection and response to security incidents, helping organizations quickly mitigate threats. This capability supports CMMC incident response and risk management requirements.
- **Continuous compliance reporting:** Tanium generates detailed compliance reports and audit trails automatically, simplifying the process of demonstrating adherence to CMMC standards. This aligns with the audit and accountability requirements.

Mastering CMMC compliance maturity with automation

CMMC's tiered model reflects increasing levels of cybersecurity maturity across organizations supporting the DoW. At Level 1, organizations must demonstrate basic cyber hygiene. At Level 2, the focus shifts to establishing a robust IT management framework. Level 3 raises the bar even further, requiring automated, continuous assessment and enforcement of security controls.

By integrating AI and intelligent automation, Tanium provides the ability to meet these evolving requirements with confidence—delivering broad technical capability, engineered automation, and real-time reporting across the entire endpoint estate.

Tanium directly supports critical Level 3 controls, including:

- Automated detection and remediation of unauthorized or misconfigured systems (CM.L3–3.4.2e)
- Continuous discovery and inventory of system components (CM.L3–3.4.3e)
- Policy enforcement restricting access to only trusted, compliant systems (IA.L3–3.5.3e)
- Advanced analytics to identify and predict risks (RA.L3–3.11.3e)
- Integration of threat intelligence for proactive detection and hunting (SI.L3–3.14.6e)

Additionally, Tanium helps organizations accelerate CMMC readiness and scale compliance efforts with:

- Supplier Performance Risk Scoring System (SPRS) optimization: Monitor compliance posture, identify gaps, and close Plan of Action and Milestones items within required timelines
- Supply chain compliance enforcement: Oversee subcontractor compliance and fulfill critical flow-down requirements
- Assessment readiness enablement: Provide the evidence you need to streamline Certified Third-Party Assessor Organization (C3PAO) and Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessments and stay certification-ready year-round

Secure CUI and maintain DoW engagements with Tanium

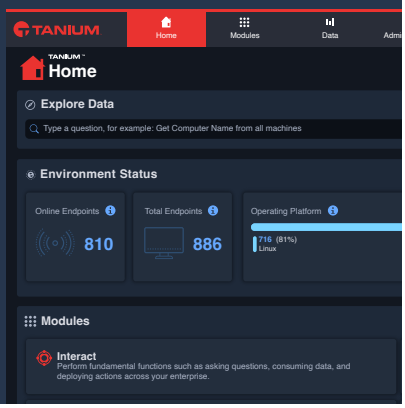
Protecting CUI is not just a compliance checkbox–it's a security imperative at the heart of national defense operations–and the cornerstone of maintaining trust with the DoW. The Tanium platform empowers organizations to achieve CMMC compliance and secure CUI with confidence, enabling organizations to continue vital partnerships, research, and processing data with the DoW while meeting or exceeding CMMC requirements.

By combining real-time visibility, automated management, and proactive risk mitigation, Tanium reduces IT risk, strengthens security resilience, and protects sensitive data. With Tanium, defense contractors and subcontractors can proactively safeguard critical information, accelerate compliance, and sustain long-term mission readiness in an evolving threat landscape.

* Percentages of product coverage is based on current product capabilities relevant to Tanium product offerings and is subject to change as product offerings evolve.

Learn more about how Tanium can help your organization

tanium.com/federal



Tanium is the Autonomous IT company. Driven by AI and real-time endpoint intelligence, Tanium Autonomous IT empowers IT and security teams to make their organizations unstoppable. Many of the world's leading organizations trust Tanium's single, unified platform for endpoint management and security to innovate faster, stay resilient and move business forward with confidence, at scale.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.