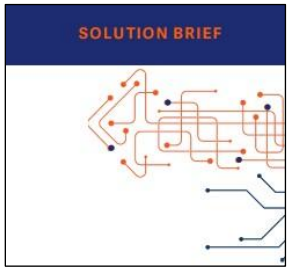

Align CMMC 2.0 Compliance Using BeyondTrust's FedRAMP SaaS Solutions

Thank you for downloading this BeyondTrust Solution Brief. Carahsoft is the Distributor for BeyondTrust solutions available via GSA 2GIT, NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring BeyondTrust's solutions, please check out the following resources and information:

For additional resources:
carah.io/beyondtrustresources

For upcoming events:
carah.io/beyondtrustevents

For additional BeyondTrust solutions:
carah.io/beyondtrustsolutions

For additional Cyber solutions:
carah.io/cybersolutions

To set up a meeting:
beyondtrust@carahsoft.com
(703) 581-6610

To purchase, check out the contract vehicles available for procurement:
carah.io/beyondtrustcontracts

BeyondTrust

SOLUTION BRIEF

Align CMMC 2.0 Compliance Using BeyondTrust's FedRAMP SaaS Solutions

BeyondTrust delivers Privileged Remote Access and Remote Support solutions that are FedRAMP authorized, enabling government contractors to efficiently meet key requirements of CMMC 2.0.

Why CMMC 2.0 Compliance Matters

- DoD Contract Eligibility – Required for handling FCI/CUI under federal contracts
- National Security – Protection capabilities and safeguards for sensitive FCI/CUI information frequently targeted in cyberattacks by threat actors
- Supply Chain Compliance – Applies to primes and subcontractors
- Cyber Maturity – Demonstrates robust cybersecurity posture and provides a framework for continuous improvements in cybersecurity practices

Benefits of Using BeyondTrust

Privileged Remote Access
Enforces least privilege, role-based access control (RBAC), and full session auditing

Remote Support
Provides encrypted, auditable, monitorable remote access across networks and air-gapped environments

Advances Cybersecurity Maturity and Zero Trust Architectures
Implements secure access, enforcing least privilege and enabling ephemeral, just-in-time access controls

FedRAMP Control Inheritance
Accelerates CMMC readiness by inheriting validated NIST 800-53/171 security controls

Continuous Monitoring
Supports incident response capabilities, threat detection and compliance reporting

CMMC 2.0 Mapping: Using BeyondTrust

CMMC Domain	Practice	BeyondTrust Capabilities
Access Control (AC)	AC.L2-3.1.1 / 3.1.5 / 3.1.12	Enforces least privilege, RBAC, and secure remote access
Audit & Accountability (AU)	AU.L2-3.3.1 / 3.3.3	Logs all privileged activity and enables audit review
System & Communications Protection (SC)	SC.L2-3.13.1 / 3.13.8	Encrypts and monitors all remote session traffic
Identification & Authentication (IA)	IA.L2-3.5.2	Supports per-session MFA and identity verification for all access
Incident Response (IR)	IR.L2-3.6.1 / 3.6.2	Enables incident response capabilities, threat detection, logging, and reporting
Risk Management (RM)	RM.L2-3.11.2	Integrates with vulnerability scanning and analytics
Configuration Management (CM)	CM.L2-3.4.6	Enforces minimal access and functionality policies

This document is informational and is intended to provide guidance on how organizations may use BeyondTrust products to meet their own obligations under CMMC 2.0. BeyondTrust is not representing that we are subject to or compliant with CMMC 2.0

To learn more, reach out to us here: https://www.beyondtrust.com/contact