

CMMC & THE DEFENSE DEPARTMENT'S UNIFIED CYBERSECURITY STANDARDS

HOW BEYONDTRUST ENABLES A CMMC COMPLIANT ARCHITECTURE



Discover & Manage Accounts

Ensure all privileged accounts are continuously identified, automatically onboarded, and placed under management.

Control Privileged Access

Limit vendor and insider access via granular, role-based access to specific systems, without sacrificing productivity.

Achieve Compliance

Audit privileged user activity and meet compliance requirements.

The Cybersecurity Maturity Model Certification (CMMC) is a unified framework designed to protect Controlled Unclassified Information (CUI) residing on the Defense Industrial Base (DIB) networks. The framework includes a comprehensive and scalable certification element to enforce cybersecurity requirements for organizations that contract, subcontract or work within the DIB. The certification consists of 5 maturity levels, 17 capability domains, 43 capabilities, and 171 practices.

BeyondTrust and CMMC

BeyondTrust offers a unique set of integrated solutions to address a wide range of architectures, including CMMC, enabling agencies to achieve Zero Trust security goals:

- [Privilege Password Management \(PPM\)](#) - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and audit all privileged activities. This solution includes BeyondTrust Password Safe (PWS).
- [Secure Remote Access \(SRA\)](#) - Apply least privilege and robust audit controls to all remote access required by employees, vendors, contractors, and service desks. This solution includes BeyondTrust Privileged Remote Access (PRA).
- [Endpoint Privilege Management \(EPM\)](#) - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity. This solution includes BeyondTrust Privilege Management for Unix and Linux (PMUL).
- [BeyondInsight \(BI\)](#) - BeyondTrust centralized management, reporting, and threat analytics solution for Privileged Access Management.

The tables on the following pages map our BeyondTrust solutions to the appropriate corresponding domain level, capability, and practice. BeyondTrust enables organizations to meet 11 out of the 17 CMMC Domains. [Please set up a consultation with our team](#) if you'd like to discuss further.



Universal Privilege Management

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

Domain	Capabilities	BT Product(s)
AC – Access Control	- Establish system access requirements - Control internal system access - Control remote system access - Limit data access to authorized users and processes	BeyondInsight Privileged Password Management Secure Remote Access Endpoint Privilege Management Cloud Privilege Protection
AM – Asset Management	- Identify and document assets - Manage asset inventory	BeyondInsight
AU – Audit & Accountability	- Define audit requirements - Perform auditing - Identify and protect audit information - Review and manage audit logs	BeyondInsight Privileged Password Management Secure Remote Access Endpoint Privilege Management Cloud Privilege Protection
AT – Awareness & Training	- Conduct security awareness activities - Conduct training	BeyondInsight Password Safe <i>Session Recording, Reporting and Analytics. We wouldn't be involved in training.</i>
CM – Configuration Management	- Establish configuration baselines - Perform configuration and change management	BeyondInsight Endpoint Privilege Management
IA – Identification & Authentication	- Establish configuration baselines - Perform configuration and change management	BeyondInsight Privileged Password Management Secure Remote Access Endpoint Privilege Management
CA – Security Assessment	- Develop and manage a system security plan - Define and manage controls - Perform code reviews	Endpoint Privilege Management Cloud Privilege Protection <i>Can contribute, but not fully cover. We would not perform code reviews.</i>
MA - Maintenance	Manage maintenance	BeyondInsight
SA – Situational Awareness	Implement threat monitoring	Endpoint Privilege Management Trusted Application Protection
SC – System & Communications Protection	- Define security requirements for systems and communications - Control communication at system boundaries	Endpoint Privilege Management
SI – System & Information Integrity	- Identify and manage information system flaws - Identify malicious content - Perform network and system monitoring - Implement advanced email protections	Endpoint Privilege Management <i>Can contribute, but not fully cover.</i>