CMMC & The Defense Department's Unified Cybersecurity Standards

How BeyondTrust Enables a CMMC Compliant Architecture

BeyondTrust

CONTENTS

Introduction – What is the CMMC?

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. Contractors and their associates must hire a third-party certified auditor to understand if they adequately meet the technical requirements outlined in CMMC.

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:

- **Privileged 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.

For a detailed consultation, contact BeyondTrust.

Domain: Access Control (AC)

C001 ESTABLISH SYSTEM ACCESS REQUIREMENTS	
LEVEL 1	
AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
	Every BeyondTrust solution can assign role-based access dependent on the end user's need and approval chain. Access to managed accounts and managed systems in Password Safe can be segmented as needed via Requestors & Approvers while being defined within access polices. The Secure Remote Access products allow for the same role-based access, allowing you to control access policies for third party vendors. The Endpoint Privilege Management solution allows for granular control on who can access what, but also what can they do within the established privilege session with said privilege credentials. All of this can be on-demand or scheduled as needed.

C002 CONTROL INTERNAL SYSTEM ACCESS	
LEVEL 1	
AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
	Every BeyondTrust solution can assign role-based access dependent on the end user's need and approval chain. Access to managed accounts and managed systems in Password Safe can be segmented as needed via Requestors & Approvers while being defined within access polices. The Secure Remote Access products allow for the same role-based access, allowing you to control access policies for third party vendors. The Endpoint Privilege Management solution allows for granular control on who can access what, but also what can they do within the established privilege session with said privilege credentials. All of this can be on-demand or scheduled as needed.
LEVEL 2	
AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts.	
	Least privilege configuration options can be addressed in the entire solution stack. Remote Support allows for you to start a session in a limited user context and then elevate as needed. EPM for Win/Mac can allow you to auto-elevate approved applications and deny all else based on policy configuration. PMUL and Password Safe can be configured to only allow certain commands to be executed when in a privileged session.
AC.2.008 Use non-privileged accounts or roles when accessing non-security functions.	
	Best Practice Recommendation: Use non-privileged accounts and allow BeyondTrust solutions to provide elevation in the event the non-privileged account is entitled.
AC.2.009 Limit unsuccessful logon attempts.	
	This can be configured within Secure Remote Access and Password Safe.

LEVEL 3	
AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	Every BeyondTrust solution can assign role-based access dependent on the end user's need and approval chain. Access to managed accounts and managed systems in Password Safe can be segmented as needed via Requestors & Approvers while being defined within access polices. The Secure Remote Access products allow for the same role-based access, allowing you to control access policies for third party vendors. The Endpoint Privilege Management solution allows for granular control on who can access what, but also what can they do within the established privilege session with said privilege credentials. All of this can be on-demand or scheduled as needed.
AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
	***Best Practice Recommendation:*** Use non-privileged accounts and allow BeyondTrust solutions to provide elevation when entitled. All activity that takes place within the BeyondTrust solution set is audited and archived for analytics and reporting.
AC.3.019 Terminate (automatically) user sessions after a defined condition.	
	BeyondTrust BeyondInsight has this capability.
LEVEL 4	
AC.4.023 Control information flows between security domains on connected systems.	
	BeyondTrust BeyondInsight has multi-tenancy capability to provide data isolation. Secure Remote Access allows for logical segmentation in which you can configure what security domains are allowed to be administered or accessed by approved members of your organization.

C003 CONTROL INTERNAL SYSTEM ACCESS

LEVEL 2

AC.2.013 Monitor and control remote access sessions.

BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) have this capability.

AC.2.015 Route remote access via managed access control points.

BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) have this capability.

LEVEL 3

AC.3.014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) have this capability.

AC.3.021 Authorize remote execution of privileged commands and remote access to security-relevant information.

BeyondTrust Endpoint Privileged Management allows for granular control of remote commands. This is an Operating System neutral solution as we can address this within MSFT Windows, Mac, Linux and Unix.

LEVEL 4

AC.4.032 Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user & role.

BeyondTrust BeyondInsight, Privileged Remote Access and Remote Support all have this capability

C004 LIMIT DATA ACCESS TO AUTHORIZED USERS AND PROCESSES

LEVEL 1

AC.1.003 Verify and control/limit connections to and use of external information systems.

BeyondTrust BeyondInsight, Password Safe, Privileged Remote Access and Remote Support all have this capability

Domain: Audit & Accountability (AU)

COO7 DEFINE AUDIT REQUIREMENTS	
LEVEL 2	
AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	
	All BeyondTrust solutions have this capability.
LEVEL 3	
AU.3.045 Review and update logged events.	
	All BeyondTrust solutions have this capability.
AU.3.046 Alert in the event of an audit logging process failure.	
	BeyondTrust BeyondInsight and Password Safe have this capability. BeyondInsight alerting can be expanded to include all integrated BeyondTrust solutions.

C008 PERFORM AUDITING

LEVEL 2

AU.2.042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

All BeyondTrust solutions have this capability. BeyondInsight employs an audit history warehousing process that allows for audit data to be retained indefinitely if needed. All BT solutions can also be configured to send qualifying events to an external SEIM or syslog repository as desired whether internal or external, such as the CDM dashboard or both.

AU.2.043 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

All BeyondTrust products work off either system time or, in the case of BeyondInisight, off an identified NTP source. Audit timestamps are based on this time value.

LEVEL 3

AU.3.048 Collect audit information (e.g., logs) into one or more central repositories.

All BeyondTrust solutions have this capability. BeyondInsight employs an audit history warehousing process that allows for audit data to be retained indefinitely if needed. All BT solutions can also be configured to send qualifying events to an external SEIM or syslog repository as desired whether internal or external, such as the CDM dashboard or both.

C009 IDENTIFY AND PROTECT AUDIT INFORMATION

LEVEL 3

AU.3.049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Audit data is safeguarded by BeyondTrust BeyondInsight through maintaining history in the database as well as encrypting the data stored on disk. Limited access due to BeyondTrust BeyondInsight system hardening provides an exceptional layer of security to avoid audit data manipulation. All logs are tamperproof across the BeyondTrust suite.

AU.3.050 Limit management of audit logging functionality to a subset of privileged users.

Roles based administration in all BeyondTrust solutions provide this functionality.

C010 REVIEW AND MANAGE AUDIT LOGS	
LEVEL 2	
AU.2.044 Review audit logs.	
	Role based administration in BeyondTrust BeyondInsight provides this capability.
LEVEL 3	
AU.3.051 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
	Role based administration in BeyondTrust BeyondInsight provides this capability.
AU.3.052 Provide audit record reduction and report generation to support on-demand analysis and reporting.	
	Role based administration in BeyondTrust BeyondInsight and the Analytics and Reporting engine provides this capability. Secure Remote Access sessions can be recorded as well.
LEVEL 4	
AU.4.053 Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.	
	Role based administration in BeyondTrust BeyondInsight provides this capability.
AU.4.054 Review audit information for broad activity in addition to per-machine activity.	
	BeyondTrust BeyondInsight and Analytics and the Reporting engine provides this capability. The integration across the product suite with Beyond Insight allows for the central collection of all events and as mentioned, the Reporting and Analytics capabilities allow for auditors to view the pre-configured reports or build their own as desired within BeyondInsight.

Domain: Configuration Management (CM)

C013 ESTABLISH CONFIGURATION BASELINES	
LEVEL 2	
CM.2.061 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	BeyondTrust BeyondInsight has the capability to discover and maintain current configuration information as it relates to system settings and installed packages. Secure Remote Access collects system information as well that can be viewed real time, as well as, reported against as needed.
CM.2.062 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	
	All BeyondTrust solutions use Roles Based Administration as a basis for providing least privileged access and just-in-time elevation access
CM.2.063 Control and monitor user-installed software.	
	BeyondTrust BeyondInsight has the capability to inventory installed software on a target system. Endpoint Privileged Management has the capability to allow user access and use of installed software on a target system.

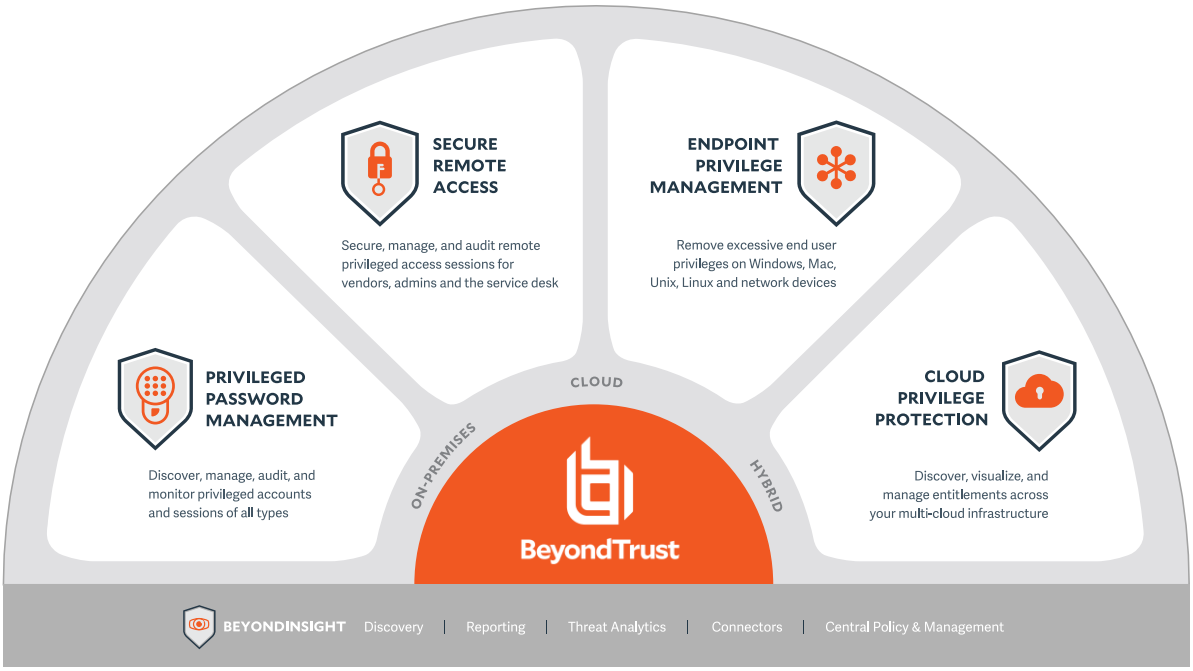
C014 PERFORMANCE AND CHANGE MANAGEMENT
LEVEL 2
CM.2.064 Establish and enforce security configuration settings for information technology products employed in organizational systems.
BeyondTrust BeyondInsight has the capability to inventory installed software on a target system. Endpoint Privileged Management has the capability to allow user access and use of installed software on a target system.
CM.2.065 Track, review, approve, or disapprove, and log changes to organizational systems.
All activities that take place using a BeyondTrust solution are audited and managed.
LEVEL 3
CM.3.067 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
BeyondTrust BeyondInsight has the capability to require approval for many activities including checking out managed privileged account passwords.
CM.3.068 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
BeyondTrust BeyondInsight has the capability to inventory installed software on a target system. Endpoint Privilege Management has the capability to allow user access and use of installed software on a target system.
CM.3.069 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
BeyondTrust Endpoint Privilege Management has the capability to restrict access to targeted applications, libraries and system components.
LEVEL 4
CM.4.073 Employ application whitelisting and an application vetting process for systems identified by the organization.
BeyondTrust Endpoint Privilege Management has the capability to restrict access to targeted applications, libraries and system components.

Domain: ID & Authentication (IA)

C015 GRANT ACCESS TO AUTHENTICATED ENTITIES	
LEVEL 1	
IA.1.076 Identify information system users, processes acting on behalf of users, or devices.	
	All BeyondTrust solutions have this capability.
IA.1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
	All BeyondTrust solutions rely on verification of the identity prior to allowing the attempted action.
LEVEL 2	
IA.2.078 Enforce a minimum password complexity and change of characters when new passwords are created.	
	BeyondTrust BeyondInsight and Password Safe have this capability for managed privileged accounts. Generally, the users' source authentication process would provide this capability. However, passwords on BeyondInsight created identities can be controlled as well. Administrative and customer password complexity to BeyondInsight can be controlled should local accounts be used.
IA.2.079 Prohibit password reuse for a specified number of generations.	
	Standard user access to BeyondTrust solutions rely on an external identity store (i.e., Active Directory or LDAP) for authorization. This service is where password complexity would be maintained. BeyondTrust Password Safe managed account password complexity rules would prevent repeated use of the same complex password.
IA.2.081 Store and transmit only cryptographically-protected passwords.	
	All BeyondTrust solutions have this capability.
LEVEL 3	
IA.3.083 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
	BeyondTrust solutions have the ability to use industry standard protocols such as radius for MFA.

The BeyondTrust Privileged Access Management Platform

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. BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions and is named a Leader in the Gartner Magic Quadrant for Privileged Access Management.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.