BeyondTrust

SOLUTION BRIEF

Identity is the New Perimeter

Mapping BeyondTrust Solutions to the Identity, Credential, and Access Management (ICAM) Architecture

CONTENTS

Introduction

Identity, Credential, and Access Management (ICAM) is the set of tools, policies, and systems that Federal and DoD agencies use to enable the right individual to access the right resource, at the right time, for the right reason in support of critical mission objectives.

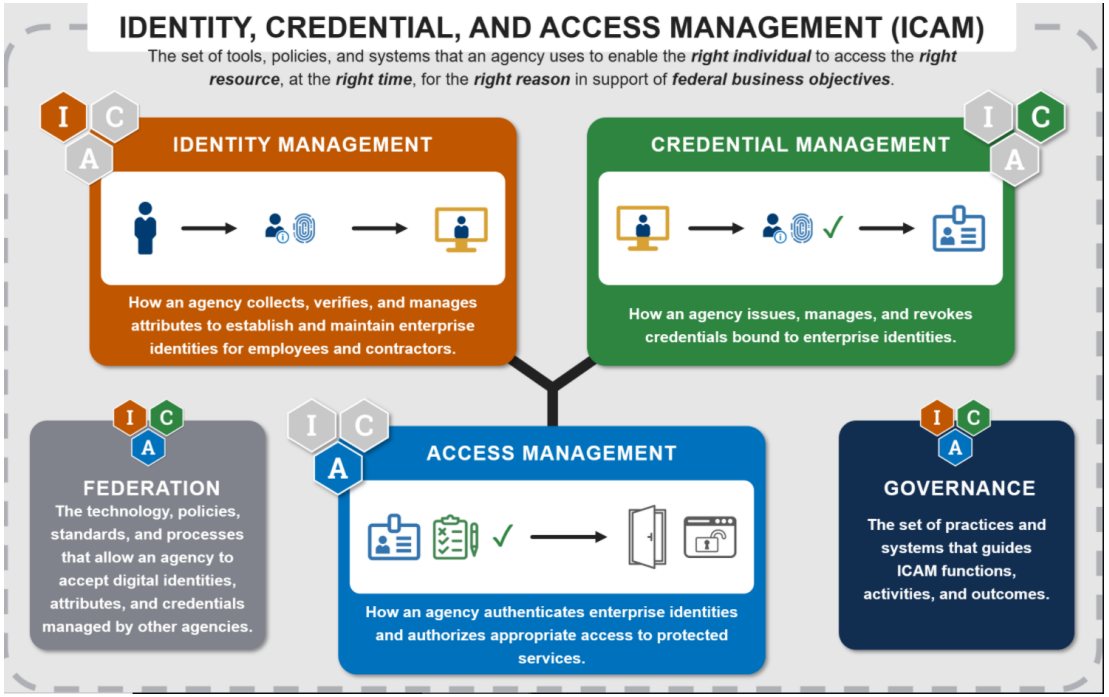
According to OMB Memorandum M-19-17, “To ensure secure and efficient operations, agencies of the Federal Government must be able to identify, credential, monitor, and manage subjects that access Federal resources, including information, information systems, facilities, and secured areas across their respective enterprises. In particular, how agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services, as well as individuals' privacy."

According to the DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, “There are significant advantages to the DoD in providing ICAM services at the DoD enterprise level, including consistency in how services are implemented, improved security, cost savings, and attribution by having a discrete defined digital identity for a single entity.

ICAM is also fundamental for the transformation to a modern data-centric identity-based access management architecture that is required in a future-state Zero Trust (ZT) Architecture. To gain these advantages, DoD enterprise ICAM services must support functionality for both the DoD internal community and DoD mission partners, must provide interfaces that are usable by Component information systems, and must minimize or eliminate gaps in supporting ICAM capabilities.”

BeyondTrust’s Universal Privilege Management solutions secure and protect privileges across passwords, endpoints, access, and identities, giving agencies the visibility and control they need to always verify, apply least privilege, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, supporting an increased focus on ICAM, FICAM and Zero Trust as the perimeter continues to dissolve in the next normal.

The following diagram is a high-level view of the ICAM practice areas and supporting elements:



Source: https://playbooks.idmanagement.gov/arch/intro-arch/

Three Different Types of Management

1. **Identity Management:** how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.
2. **Credential Management:** how an agency issues, manages, and revokes credentials bound to enterprise identities.
3. **Access Management:** how an agency authenticates enterprise identities and authorizes appropriate access to protected services.

Enable ICAM and Zero Trust Security Goals with BeyondTrust

We have a unique set of integrated solutions to address a wide range of architectures, including ICAM, enabling agencies and organizations to achieve Zero Trust security goals:

- (PPM) Privilege Password Management- Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and audit all privileged activities. This solution includes Password Safe (PWS). DevOps Secrets Safe (DSS) - Secure and automate the storage and access of secrets used by applications, tools, and other processes across your development operations environments.

- (SRA) Secure Remote Access - Apply least privilege and robust audit controls to all remote access required by employees, vendors, contractors, and service desks. This solution includes Privileged Remote Access (PRA) and Remote Support (RS).

- (EPM) Endpoint Privilege Management - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

Mapping BeyondTrust Solutions to the ICAM Architecture Chart

Identity Management

FICAM Architecture Service		ICAM Capability	BeyondTrust Responses	Solution
Identity Management	**The set of practices that allow an organization to establish, maintain, and terminate identities.**	**C1.1 Identity Management**		
Identity Proofing	Verifying information to establish the identity of a person or entity	C1.2.1 Internal Credential Management	Password Safe- Encrypted vault (AES-256) that controls privilege session management.	PWS
Creation	Establishing a digital identity composed of attributes that define a person or entity	C1.1.1 Person Entity C1.1.2 NPE	Password Safe- Full Role Based Access Control (RBAC)is supported.	PWS
Maintenance	Maintaining accurate and current attributes within an identity record over its life cycle	C1.1.1 Person Entity C1.1.2 NPE	Password Safe- Full Role Based Access Control (RBAC) is supported.	PWS
Identity Resolution	Finding and connecting disparate identity records for the same person or entity	C2.3 Identity Resolution	Password Safe- Encrypted vault (AES-256) that controls privilege session management.	PWS

Credential Management

FICAM Architecture Service		ICAM Capability	BeyondTrust Responses	Solution
Credential Management	**The set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context.**	**C1.2 Credential Management**		
Sponsorship	Formally establishing that a person or entity requires a credential	C1.2.1 Internal Credential Management	Password Safe- Encrypted vault (AES-256) that controls privilege session management.	PWS
Registration	Collecting the information needed from a person or entity to issue them a credential	C1.1.1 Person Entity C1.1.2 NPE	Privilege management can confirm authentication before providing privilege to a user action.	EPM
Issuance	Transferring a credential to a person or entity	C1.2.1 Internal Credential Management	Password Safe (PWS) introduced Team Passwords that enables organizations to secure shared credentials. Team Passwords enables teams to easily store and manage shared credentials for accounts that are commonly managed within specific teams, while still providing a fully auditable and controlled environment.	PWS
Maintenance	Maintaining a credential over its life cycle	C1.2.1 Internal Credential Management	Passwords are rotated and randomized eliminating the need to maintain a credential over a lifecycle.	PWS
Revocation	Withdrawing a credential from a person or entity	C1.2.1 Internal Credential Management	Quarantine feature when turned on is a measure for when suspicious activity is detected. When turned on the user account can no longer log into the console or API and any active sessions are terminated.	EPM

Access Management

FICAM Architecture Service		ICAM Capability	BeyondTrust Responses	Solution
Access Management	**The set of practices that enables only those permitted the ability to perform an action on a particular resource.**	**C1.3 Access Management**		
Policy Administration	Creating and maintaining the rule sets that govern access to protected resources	C1.3.1 Resource Management	PWS provide JIT RBAC access allowing for a user to access a privileged asset at a specific time for a defined amount of time. Limiting who, when and how long privileged access is granted.	PWS, EPM
Entitlement Management	Establishing and maintaining the authoritative access permissions for a person or entity	C1.3.2 Provisioning	Role Based Access - Group Permissions, Password Safe roles. Password Safe roles- Requestor, approver, requestor approver, information Security Admin, Auditor, No Roles, Credential Manager Recorded Session Reviewer, Active Session Reviewer	PWS, EPM, RS, PRA
Provisioning	Linking and unlinking access permissions for a person or entity to a protected resource	C1.3.2 Provisioning	PWS through our smart rule technology provides adaptive access control. Evaluate JIT context and simplify access requests by considering the day, date, time and location this determines their authorization to access assets.	PWS, EPM, PRA
Authentication	Verifying that a claimed identity is genuine based on valid credentials	C1.3.3 Authentication	The following authentication types can be used, Password Safe authentication, Active Directory, LDAP, Smart Card, RADIUS, third party authentication	PWS, EPM, PRA, RS
Authorization	Granting or denying access requests to protected resources based on a policy determination	C1.3.4 Authorization	Leverage true Role-Based Access Controls with AD and LPAD integration for assigning roles and rights to users.	EPM, PWS

The following tables will map the ICAM Architecture Chart to the BeyondTrust solutions above. The fourth column will show how we respond to each specific control, and the fifth column will contain the relevant solution(s) abbreviation from above.

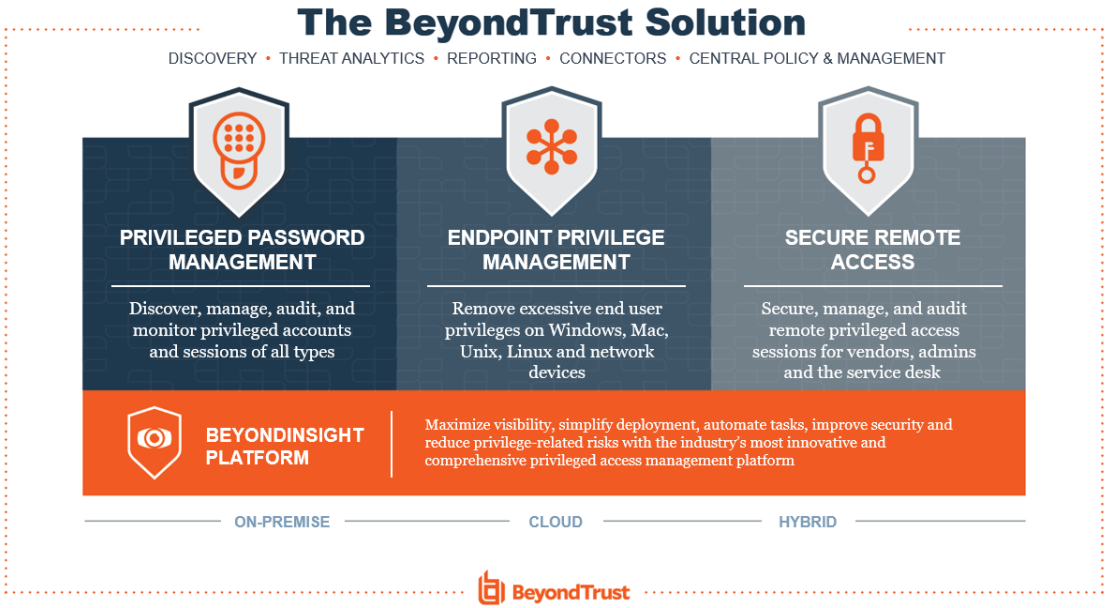
Federation	The ability of one organization to accept another organization's work	C1.1.3 Federated Entity C1.2.2 External Credential Registration C1.3 Access Management		Solution
Attribute Exchange	Discovering and sharing identity attributes between different systems to promote interoperability and simplify the process for establishing an identity	C1.1.3 Federated Entity	Password Safe (PWS) has a robust Discovery engine that discovers and profiles all known and unknown assets, shared accounts, user accounts and Service Accounts. Smart rules quickly identify assets with common traits and automatically place them under PWS management via smart rules. Auto discover SSH keys on host systems.	PWS
Credential Bridging	Transforming a token or credential into an alternative format, potentially containing claims about the client, for acceptance at a relying party	C1.3.3.Authentication	PWS supports SAML and Radius for 2FA and MFA.	PWS, RS, PRA
Credential Translation	Establishing a cross-certified, affiliated relationship to trust credentials at a level of assurance asserted by those credentials	C1.3.3 Authentication	Password Safe / PRA - Local, Domain, SAML, RADIUS and PIC/CAC card authentication are supported.	PWS, PRA
Policy Alignment	Establishing a mutual relationship between parties by deliberately establishing common	C1.1.3 Federated Entity C1.2.2 External Credential Registration	Password Safe / PRA - Full Role Based Access Control is supported.	PWS, PRA

	standards and principles			
Governance	**The set of practices that allow organizations to administer and support the successful execution of the core ICAM services and functions**			
Enterprise Governance	Developing and implementing the policies, rules, and procedures to manage and improve an ICAM program	Section 6	PWS through auto-discovery, smart rules to automatically onboard newly discovered assets and credentials, manage and rotate passwords and monitor and audit sessions would greatly improve the security posture and the ICAM program.	PWS, EPM
Auditing and Reporting	Monitoring, reviewing, and reporting on an ICAM program's conformance with rules, policies, and requirements	C2 Access Accountability for general auditing and reporting N/A for ICAM services as this is a system specific requirement	PWS provides live session management, recorded sessions in real time, build reports for usage, audit, forensics and regulatory compliancy. Audit and log privileged sessions, quickly search session logs, integrate with SailPoint Identity IQ, RDP session audit, real-time activity alerting, command blacklisting and auto log off and disconnect.	PWS
Redress	Fixing problems and vulnerabilities that occur during standard operation of an ICAM program	N/A – System specific requirement	PWS integrates with third party tolls (SIEM), Splunk to get real time notifications and the necessary actions to quickly correct any alerted vulnerabilities.	PWS

Recovery	Preparing the procedures and assets that would be needed to recover from a security or privacy breach and ensure continuity of service	N/A – System specific requirement	Password Safe \ PRA - Full HA architecture of Active/Passive & Active/Active are supported. We can also scale in capacity by additional distributed appliances to avoid service disruption. Multiple forms of MFA/2FA authentication are supported to mitigate security breach. With our appliance-based deployment model for on-prem deployments, all data, logging, encrypted databases are self-contained with no direct access to the underlying operating system being granted be default.	PWS, PRA

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.



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. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace. 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.