TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Mapping BeyondTrust Solutions to NIST SP800-171 Requirements

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Contents

NIST Special Publication 800-171 Overview 3
Unified Privileged Access Management to Reduce Risk 4
BeyondTrust Alignment to NIST SP800-171 Requirements 4
3.1 Access Control (AC) 5
3.3 Audit and Accountability (AU) 11
3.4 Configuration Management (CM) 14
3.5 Identification and Authentication (IA) 17
3.6 Incident Response (IR) 19
3.11 Risk Assessment (RA) 20
3.12 Security Assessment and Authorization (CA) 22
3.13 System and Communication Protection Policy and Procedures (SC) 25
3.14 System and Information Integrity (SI) 27
The PowerBroker Privileged Access Management Platform 30
Product Capabilities within the PowerBroker PAM Platform 30
About BeyondTrust 31

TECH TIP:

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "Addressing NIST SP800-53 Requirements with BeyondTrust Solutions".

NIST Special Publication 800-171 Overview

A vast amount of federal information is regularly stored, processed and transmitted by non-federal organizations, like contractors, state and local governments, universities and research organizations. Often, this information is sensitive and if compromised would have a direct negative impact on the functioning of the federal government and an agency's ability to achieve their mission. Therefore, protecting that information both inside and while outside of federal information systems is critically important.

Since the creation of Executive Order 13566, Controlled Unclassified Information (CUI), in late 2010, government cyber incidents have shown no signs of slowing down. We've seen that sophisticated cyber actors are targeting non-federal systems handling government data as a path to high value agency assets. The massive OPM data breach is a good example of this. Thus, there is heightened focus on the security practices of non-government organizations handling CUI. In 2016 we saw updates to FAR clauses, additional NARA regulations and new DoD Cyber incident reporting requirements. Cyber security requirements were even addressed in the 2017 National Defense Authorization Act. Failure to meet these extensive requirements can impact payment for services, or result in damages and civil penalties that can quickly climb into the millions of dollars.

EO13566 mandated the establishment of a government wide CUI program that would create a standardized structured process for the way the executive branch would handle unclassified information that requires protection. NIST SP800-171 was created to provide recommended requirements to secure and protect the confidentiality of CUI when it resides in a non-federal system. The requirements outlined in the special publication are designed to apply only to those non-federal systems that store, process or transmit CUI, or those that provide security for such systems. Agencies use these requirements in contract vehicles and agreements with non-federal organizations to establish requirements for appropriate security measures.

Requirements for protecting CUI have been derived from four key federal standards and guidelines to maintain consistency across agency and non-federal implementation. This insures standardized reliable protection.

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality impact)
- Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; and
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The resulting guidance found in NIST SP800-171 aligns to 14 security requirement families. These requirements matrix directly to specific security controls within NIST SP 800-53 and ISO/IEC 27001. Non-federal organizations are instructed to specify in a system security plan how they will meet these requirements.

Unified Privileged Access Management to Reduce Risk

Controlling and monitoring privileged access is extremely important to mitigating the risks posed by insider threats, preventing data breaches, and meeting compliance requirements. But security and IT leaders, whether in a federal agency or non-federal organization, walk a fine line between protecting the organization's critical data to ensure business continuity, and enabling users and administrators to be productive. Disparate, disjointed tools deployed and managed in silos leave gaps in coverage over privileged access. This legacy model is expensive, difficult to manage, and requires too much time to show any meaningful risk reduction. Organizations need a partner to safeguard the federal information held in their systems.

PowerBroker delivers the complete spectrum of privileged access management solutions. From establishing and enforcing least privilege on endpoints and servers, to securing enterprise credentials, BeyondTrust unifies best-of-breed capabilities into a single, integrated platform that acts as a central policy manager and primary reporting interface. Leveraging vulnerability data from BeyondTrust's Retina and other solutions provides a complete picture of privileged system and asset security – including for network, cloud and virtual assets. This zero-gap coverage reduces risk by ensuring that no assets are left unprotected.

This unified approach enables agencies, and those non-federal organizations storing, processing or transmitting federal information, to take advantage of a modular approach, adding products and capabilities as each access control is implemented.

BeyondTrust Alignment to NIST SP800-171 Requirements

For this brief, we will explore nine (9) of the 14 required security control families in NIST SP800-171 as they map to NIST SP800-53. In the pages that follow you will find specific control guidance directly from NIST SP800-171 and NIST SP800-53, with information regarding how BeyondTrust supports each control directly related to privilege access and vulnerability management. Implementing NIST guidance is designed to be a strategic modular implementation of controls and best practices. The information that follows is organized by control family so that you can easily reference the area of most interest to your organization today, and reference back as you continue to implement other control families.

3.1 Access Control (AC)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Basic Security Requirements		
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems). 3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Account Management AC-2 through AC-2 (K)	*The organization Identifies and selects the following types of information system accounts to support organizational missions/business functions: organization-defined information system account types; assigns account managers for information system accounts; establishes conditions for group and role membership; specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.* *Notifies account managers when accounts are no longer required, authorizes access to the information system based on: a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions.* *Reviews accounts for compliance with account management requirements at the organization-defined frequency; and establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.* • BeyondTrust privileged access management and vulnerability management solutions provide controls to assist with the identification of accounts based on targeted functions. • Group based policy allows delegated rights to be assigned to managers of information system accounts. • Groups of users may be defined to determine rights and roles of access to information systems and accounts. • PowerBroker Password Safe can identify accounts that have not been used for a given amount of time allowing managers the insights required to decide if an account is no longer needed.
	Access Enforcement AC-3	*The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.* • In BeyondTrust least privilege solutions, approval requirements may be implemented to ensure proper authorization is granted before a user is provided access. • To enhance security requirements on selected accounts, rules can be set to require multiple approvals such that two or more individuals must approve user access before granting permissions.

	Remote Access AC-17 AC-17a. AC-17b. AC-17(1) AC-17(2) AC-17(3) AC-17(4)(a) AC-17(9)	*The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorizes remote access to the information system prior to allowing such connections.* • The PowerBroker PAM platform incorporates role-based access control policies that limit and restrict access to only authorized users.
Derived Security Requirements		
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Information Flow AC-4	*The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.* • Both PowerBroker for Unix & Linux and PowerBroker Identity Services allow for targeted policies that regulate which devices can communicate with each other, and assist in specified criteria that establishes what type of data is allowed. • This solution provides a granular policy engine which allows administrators to dissect information transfer between security domains, and based on real-time findings, trigger enforcement of organizational policy.
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Separation of Duties AC-5 AC-5.a AC-5.b AC-5.c	*The organization: separates organization-defined duties of individuals; documents separation of duties of individuals; and defines information system access authorizations to support separation of duties.* • The BeyondTrust PowerBroker PAM platform provides the ability to enforce policy based on end-user roles and duties. This provides separate, auditable, documented policy sets throughout an enterprise.
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. 3.1.6 Use non-privileged accounts or roles when accessing non-security functions.	Least Privilege AC-6 AC-6(1) AC-6(2) AC-6(3) AC-6(4) AC-6(5) AC-6(6) AC-6(7) AC-6(7)(a) AC-6(7)(b) AC-6(8) AC-6(9) AC-6(10)	*The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.* *The organization explicitly authorizes access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.* *The organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.* *The organization authorizes network access to organization-defined privileged commands only for organization-defined compelling operational needs and documents the rationale for such access in the security plan for the information system.*

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.		*The information system provides separate processing domains to enable finer-grained allocation of user privileges.* *The organization restricts privileged accounts on the information system to organization-defined personnel or roles.* *The organization prohibits privileged access to the information system by non-organizational users.* *The organization reviews at the organization-defined frequency the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.* *The information system prevents organization-defined software from executing at higher privilege levels than users executing the software.* *The information system audits the execution of privileged functions.* *The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.* • BeyondTrust privileged access management and vulnerability management solutions are designed around the principle of least privilege. They provide the controls required to dictate a user's access rights, allowable application launches, as well as the rights associated with those applications. In addition, all actions attempted or taken by end-users can be reported for addition analysis and forensics. ○ Patented privilege elevation capabilities grant privileges to applications and tasks – not users – without providing administrator credentials. ○ Apply policies across Windows and Mac endpoints for maximum flexibility. ○ Leverage vulnerability data from Retina and other PowerBroker PAM platform products for a complete picture of privileged application and asset security. ○ Centrally control privileged access management policies and deployment, and report to multiple stakeholders. ○ Reporting is available for all actions attempted or take by users to enable additional analysis and forensics.
3.1.8 Limit unsuccessful logon attempts.	Unsuccessful Login Attempts AC-7 AC-7a. AC-7b.	*The information system enforces a limit of organization-defined number consecutive invalid logon attempts by a user during an organization-defined time period; and* *Automatically locks the account/node for an organization-defined time period; locks the account/node until released by an administrator; delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.*

		• PowerBroker Password Safe and PowerBroker Identity Services enforce an authentication failure when a set number of failed attempts have been made. • BeyondTrust PowerBroker PAM products not only provide a lock out mechanism upon consecutive failed attempts but can initiate a lock out based on a manual action. In both scenarios, the user can remain locked until an authorized administrator unlocks the account.
3.1.9 Provide privacy and security notices consistent with applicable CUI rules	System Use Notification AC-8 AC-8a. AC-8a. 1 AC-8a. 2 AC-8a. 3 AC-8a.4 AC-8b. AC-8c. AC-8c.1 AC-8c.2 AC-8c.3	*The information system displays to users an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that users are accessing a U.S. Government information system; information system usage may be monitored, recorded, and subject to audit; unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and use of the information system indicates consent to monitoring and recording;* *Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and* *for publicly accessible systems displays system use information organization-defined conditions, before granting further access; displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and includes a description of the authorized uses of the system.* • BeyondTrust privileged access management and vulnerability management solutions can provide messaging to end-users. The text and language can be based on end user location, system details or other organizational policies. • Activities occurring on systems and/or by user interaction can be recorded for auditing. This information can be compared to policy violation or applicable federal laws. • Information recorded via these products is accessible to authorized staff only. This information would indicate unauthorized access attempts and be subject to criminal/civil penalties as allowed by law. • Messaging can be displayed to users indicating their actions will be recorded, and can be set to remain on screen until the end user acknowledges the message, or for the full duration on certain recorded events. • The BeyondTrust IT Risk Management Platform, PowerBroker Password Safe, PowerBroker for Unix & Linux, and PowerBroker Auditor allow for messaging to show data related to the system and/or desired use prior to granted additional access [rights].

		• Messaging provided by the products related to recording of actions/screens remain in compliance with the respective privacy laws of a given region/organizational policy. • Messaging to end-users can be developed to include the intended/authorized use cases as it pertains to the respective product, prior to granting access rights.
3.1.11 Terminate (automatically) a user session after a defined condition	Session Termination AC-12	*The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect.* • PowerBroker Password Safe and PowerBroker for Unix & Linux can automatically terminate a user's session based on idle time or a pre-set length of time a session is active.
3.1.12 Monitor and control remote access sessions 3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. 3.1.14 Route remote access via managed access control points 3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information	Remote Access AC-17 AC-17a. AC-17b. AC-17(1) AC-17(2) AC-17(3) AC-17(4)(a)	*The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorizes remote access to the information system prior to allowing such connections.* *The information system monitors and controls remote access methods.* *The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.* *The information system routes all remote accesses through organization-defined number managed network access control points.* *The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for organization-defined needs* • The PowerBroker PAM platform incorporates role-based access control policies that limit and restrict access to only authorized users. • Help implement cryptographic mechanisms to protect the confidentiality and integrity of remote access solutions, and force information system routes for all remote accesses through managed network access control points.

3.1.20 Verify and control/limit connections to and use of external systems	Use of External Information Systems AC-20 AC-20a. AC-20b. AC-20(1) AC-20(1)(a) AC-20(1)(b)	*The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:* *access the information system from external information systems; and process, store, or transmit organization-controlled information using external information systems.* *The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization verifies the implementation of required security controls on the external system as specified in the organizations information security policy and security plan; or retains approved information system connection or processing agreements with the organizational entity hosting the external information system.* • BeyondTrust privileged access management and vulnerability management solutions are designed around the principle of least privilege. They provide the controls required to dictate a user's access rights, allowable application launches as well as the rights associated with those applications. In addition, all actions attempted or taken by end-users can be reported for addition analysis and forensics.
3.1.22 Control CUI posted or processed on publicly accessible systems.	Publicly Accessible Content AC-22 AC-22a.	The organization designates individuals authorized to post information onto a publicly accessible information system; • BeyondTrust privileged access management and vulnerability management solutions are designed around the principle of least privilege. They provide the controls required that dictate a users' access rights, allowable application launches, and rights associated with those applications. In addition, all actions attempted or taken by end-users can be reported for additional analysis and forensics.

3.3 Audit and Accountability (AU)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Basic Security Requirements		
3.3.1 Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate system activity. 3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	Audit Events AU-2 AU-2(3)	*The organization reviews and updates the audited events as defined by agency policy. The set of audited events should be reviewed at regular intervals to ensure that the current set is appropriate.* • Audit policies within the PowerBroker PAM platform are designed to be easy to configure and change. • Updating policies is normal and expected behavior for all BeyondTrust customers.
	Content of Audit Records AU-3 AU-3(1)	*The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. It generates audit records containing the agency defined additional information.* • BeyondTrust audit records contain the standard who, what, where and when; along with many other relevant tracking details specific to the platform or product that is generating the audit event. • Session recording is offered on systems that make sense, and detailed time line audit trails are provided everywhere else.
	Audit Review, Analysis and Reporting AU-6 AU-6(1) AU-6(3)	*The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.* • The BeyondTrust IT Risk Management Platform acts as a security information and event management platform for BeyondTrust privileged access management and vulnerability management solutions which provides centralized logging with audit and reporting capabilities. • BeyondTrust has its own vulnerability scanner fully integrated into the BeyondTrust Platform, which can also consume data from other scanner tools. This information can be used in reporting and decision making in the PowerBroker PAM solutions. • The BeyondTrust IT Risk Management Platform PowerBroker PAM products use RBAC to provide access to the system, and controls what can be viewed and/or configured by the accessing user. • PowerBroker for Unix &Linux can read data from almost any source that is accessible by the host system and include it within any audit records it generates. • Dynamically adjust audit capabilities based on external settings and information is provided by most BeyondTrust solutions.

	Audit Generation AU-12	*The information system compiles audit records from organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.* • In the PowerBroker PAM platform, all actions performed by a user/administrator are logged and time-stamped. Reports can be generated to view a complete audit-trail.
Derived Security Requirements		
3.3.3 Review and update audited events	Audit Events AU-2 AU-2(3)	*The organization reviews and updates the audited events as defined by agency policy. The set of audited events should be reviewed at regular intervals to ensure that the current set is appropriate.* • Audit policies within the PowerBroker PAM platform are designed to be easy to configure and change. • Updating policies is normal and expected behavior for all BeyondTrust customers.
3.3.4 Alert in the event of an audit process failure	Response to Audit Processing Failures AU-5	*The information system provides a warning to personnel, roles and locations defined by the organization within a time period specified by organizational policy. when allocated audit record storage volume reaches repository maximum audit record storage capacity as defined by organizational policy.* • The network traffic caused by BeyondTrust PAM and VM solutions can be controlled in many ways, including a wide variety of configuration controls for how the data is transmitted, as well as what is audited and when. • PowerBroker for Unix & Linux and PowerBroker Auditor will continue to operate with failover capability and/or limited capability with store/forward options in most cases.
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious or unusual activity.	Audit Review, Analysis and Reporting AU-6(3)	*The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.* *The information system provides the capability to centrally review and analyze audit records from multiple components within the system.* • The BeyondTrust IT Risk Management Platform: ○ Acts as a security information and event management platform for BeyondTrust privileged access management and vulnerability management solutions which provides centralized logging with audit and reporting capabilities. ○ Offers an advanced threat analytics feature that analyzes and pinpoints anomalies within the data collected from BeyondTrust privileged access management and vulnerability management solutions as well as third party feeds. These clusters can help identify patterns indicating malicious activity.

3.3.6 Provide audit reduction and reporting generation to support on-demand analysis and reporting.	Audit Reduction and Report Generation AU-7	*The information system provides an audit reduction and report generation capability that provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records.* • The BeyondTrust IT Risk Management Platform offers an advanced threat analytics feature that analyzes and pinpoints anomalies within the data collected from BeyondTrust privileged access management and vulnerability management solutions as well as third party feeds. These clusters can help identify patterns indicating malicious activity • The BeyondTrust IT Risk Management Platform includes a reporting feature that allows for quicker and easier ways to summarize audit data, targeting the most meaningful information quickly and easily based on internal and external filters. • Filtering within BeyondTrust solutions reports, along with smart grouping (intelligent and dynamic grouping) of assets, simplifies the source of report data selection. • The BeyondTrust IT Risk Management Platform provides run time filtering capabilities which will vary by report, but in every case, allows for very granular reporting and easy selection of data based on filters that make sense for the given report.
3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Time Stamps and Synchronization with the information system AU-8 AU-8(1)	*Time stamps generated by the information system include date and time. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.* • Base timestamps are included on all audit records generated by all BeyondTrust privileged access management and vulnerability management solutions. Many also allow for alternative date/time event determination where appropriate.
3.3.8 Protect audit information & audit tools from unauthorized access, modification and deletion. 3.3.9 Limit mgmt of audit functionality to a subset of privileged users.	Protection of Audit Information AU-9 AU-9(4)	*The information system protects audit information and audit tools from unauthorized access, modification, and deletion.* *The organization authorizes access to management of audit functionality to only an organization-defined subset of privileged users.* • Access to audit information can be granularly configured to prevent unauthorized access. This role based delegation ensures that users do not perform unauthorized actions within BeyondTrust privileged access management and vulnerability management solutions. • BeyondTrust privileged access management and vulnerability management solutions are protected by granular administrative delegation controls. Privileged access can be set to ensure changes are made only to authorized sets of resources, with a full audit trail of activity. • Privileged users can be limited to read-only roles. These roles can be defined at a granular level based on a user's responsibilities.

3.4 Configuration Management (CM)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Basic Security Requirements		
3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware and documentation) throughout the respective system development life cycles 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizations systems	Baseline Configuration, Reviews and Updates CM-2	*The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.* • Retina, the BeyondTrust vulnerability management solution, can scan and report against configuration compliance benchmarks. This can help validate changes have been applied to systems.
	Configuration Settings CM-6 CM-6(a) CM-6(d)	*Establishes and documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements; monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.* • Retina, the BeyondTrust vulnerability management solution, can scan and report on configuration compliance. • PowerBroker solutions can be configured to monitor, log or alert when certain system changes occur.
	Information System Component Inventory CM-8 CM-8a. CM-8a.1 CM-8a.2 CM-8a.3 CM-8b.	*Develops and documents an inventory of information system components that:* *accurately reflects the current information system; includes all components within the authorization boundary of the information system; is at the level of granularity deemed necessary for tracking and reporting; and reviews and updates the information system component inventory organization-defined frequency.* • Retina, the BeyondTrust vulnerability management solution, can scan and enumerate attributes about a system (i.e. Software, software version, machine name, and more). This information can be used for tracking and reporting.
	Updates During Installations/Removals CM-8(1)	*The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.* • Retina, the BeyondTrust vulnerability management solution, can scan and enumerate attributes about a system (i.e. Software,

		software version, machine name, and more). This information can be used for tracking and reporting.
Derived Security Requirements		
3.4.3 Track, review, approve/disapprove, and audit changes to organizational systems	Configuration Change Control CM-3 CM-3a. CM-3f.	*The organization determines the types of changes to the information system that are configuration-controlled; audits and reviews activities associated with configuration-controlled changes to the information system* • Retina, the BeyondTrust vulnerability management solution, can be utilized to scan systems before they depart to ensure they are hardened correctly.
3.4.4 Analyze the security impact of changes prior to implementation	Security Impact Analysis CM-4	*The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.* • Retina, the BeyondTrust vulnerability management solution, can scan and report on configuration compliance. This can help verify that configuration changes have been applied.
3.4.5 Define, document, approve and enforce physical and logical access restrictions associated with changes to organizational systems	Access Restrictions for Change CM-5	*The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.* • The PowerBroker PAM platform can limit the access/privilege of a user until approvals are received. • Retina, the BeyondTrust vulnerability management solution. can scan and report on configuration compliance. Delta reports can be used to quickly identify system changes. • The PowerBroker PAM platform can be configured to allow/block the execution/installation of applications based on their signature.
3.4.7 Restrict, disable and prevent the use of nonessential functions, ports, protocols and services 3.4.8 Apply deny-by-exception (blacklist) policy to prevent use of unauthorized software or	Prevent Program Execution CM-7(2) CM-7(4) CM-7(4)(a) CM-7(4)(b) CM-7(4)(c) CM-7(5) CM-7(5)(a) CM-7(5)(b) CM-7(5)(c)	*The information system prevents program execution in accordance with one or more organization-defined policies regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.* *The organization identifies organization-defined software programs not authorized to execute on the information system; employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and reviews and updates the list of unauthorized software programs at the organization-defined frequency.* *The organization identifies organization-defined software programs authorized to execute on the information system; employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and reviews and updates the list of authorized software programs at the organization-defined frequency.*

deny-all, permit-by-exception (whitelisting)policy to allow the execution of authorized software		• Retina, the BeyondTrust vulnerability management solution, supports the review process by identifying all ports, protocols and services. While we do not disable these services, this solution can verify that they are disabled. • PowerBroker solutions can be configured to block unauthorized applications. • PowerBroker for Unix & Linux, PowerBroker for Windows and PowerBroker for Mac can employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system • BeyondTrust privileged access management and vulnerability management solutions can assist in identification of applications for the review process.
3.4.9 Control and monitor user installed software	Configuration Management Plan CM-11 CM-11a. CM-11b. CM-11c.	*The organization establishes organization-defined policies governing the installation of software by users; enforces software installation policies through organization-defined methods; and monitors policy compliance at the organization-defined frequency.* • PowerBroker for Unix & Linux, PowerBroker for Windows and PowerBroker for Mac can report on which applications are being executed, and where dictated by policy can deny the execution of these applications. • BeyondTrust privileged access management and vulnerability management solutions can help identify open source applications. PowerBroker can deny the execution of these applications. • The PowerBroker PAM platform can control which users have the rights to install software via organization-defined policies. These polices can be reviewed at organizational defined intervals. • BeyondTrust privileged access management and vulnerability management solutions can alert when unauthorized applications are detected or executed.

3.5 Identification and Authentication (IA)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Basic Security Requirements		
3.5.1 Identify system users, processes acting on behalf of users, or devices 3.5.2 Authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational systems.	Access to Privileged Accounts IA-2	*The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).* • BeyondTrust privileged access management and vulnerability management solutions associate a user with the actions taken by him/her. This user can be uniquely identified and reported on for further analysis and/or forensics.
Derived Security Requirements		
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts and for network access to non-privileged accounts. 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts	Access to Privileged Accounts IA-2 IA-2(1) IA-2(2) IA-2(3) IA-2(8) IA-2(9)	*The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).* *The information system implements multifactor authentication for network access to privileged accounts.* *The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.* *The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.* • BeyondTrust privileged access management and vulnerability management solutions associate a user with the actions taken by him/her. This user can be uniquely identified and reported on for further analysis and/or forensics.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created. 3.5.8 Prohibit password reuse for a specified number of generations 3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password 3.5.10 Store and transmit only cryptographically-protected passwords	Password Based Authentication IA-5(1) IA-5(1)(a) IA-5(1)(b) IA-5(1)(c) IA-5(1)(d) IA-5(1)(e) IA-5(1)(f)	*The information system, for password-based authentication enforces minimum password complexity of organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type; enforces at least the organization-defined number of changed characters when new passwords are created; stores and transmits only cryptographically-protected passwords; enforces password minimum and maximum lifetime restrictions of organization-defined numbers for lifetime minimum/ lifetime maximum; prohibits password reuse for organization-defined number generations; and allows the use of a temporary password for system logons with an immediate change to a permanent password.* • BeyondTrust PowerBroker Password Safe provides varied password policies, taking into consideration complexity, lifetime as well as prohibiting re-use of old passwords. • Passwords can also be managed long term with restricted access/use to authorized individuals and services.

3.6 Incident Response (IR)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Basic Security Requirements		
3.6.1 Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities. 3.6.2 Track, document, and report incidents to appropriate organizational officials and/or authorities	Incident Response Assistance IR-7	*The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.* • BeyondTrust privileged access management and vulnerability management solutions support systems such as syslog, Simple Network Management Protocol (SNMP) and email alerting when certain events are reported. • The BeyondTrust support center can help with the configuration and interpretation of events & alerts generated by BeyondTrust products.

3.11 Risk Assessment (RA)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Basic Security Requirements		
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI.	Risk Assessment RA-3 RA-3a.	*The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits* • The BeyondTrust IT Risk Management Platform will perform vulnerability and access scans across an environment and help tie risk scores to the various items found.
Derived Security Requirements		
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	Vulnerability Scanning RA-5 RA-5b. RA-5b.1 RA-5b.2 RA-5b.3 RA-5c. RA-5d. RA-5e.	*The organization scans for vulnerabilities in the information system and hosted applications at the organization-defined frequency and/or randomly in accordance with organization-defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported; employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact; analyzes vulnerability scan reports and results from security control assessments; remediates legitimate vulnerabilities within organization-defined response times in accordance with an organizational assessment of risk; and shares information obtained from the vulnerability scanning process and security control assessments with organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).*

		• The BeyondTrust IT Risk Management Platform ○ includes an enterprise-class network security scanner. Scans can be performed on a scheduled basis and ad hoc. Organizations can perform both credentialed and non-credentialed scans to retrieve asset information. ○ will process all information discovered by the security scanner and will enumerate software, platform, and configurations, and compare the findings against known vulnerabilities and best practices. The platform will process all information discovered by the security scanner and provide a vulnerability impact report. ○ incorporates pivot grid technology to allow for analysis of scan results and comparison security assessments. ○ can be used to remediate vulnerabilities. ○ utilizes role-based access control when disseminating reporting and analytic information. ○ is configured to receive regular updates as new vulnerabilities are discovered. ○ allows for granular configuration when determining what system information is discovered during network security scans. ○ allows for both credentialed and non-credentialed scans of information systems. PowerBroker Password Safe integrates directly with the scanner allowing for automatic password retrieval and rotation when performing credentialed scans. ○ includes numerous reporting options allowing for the comparison of collected vulnerability data between defined dates or against an initial baseline. These also include identification of vulnerabilities that have been previously exploited in the wild ○ includes a built-in threat management feature, which allows correlation of user activity with vulnerability data, to determine where an attack originated, and its history within the protected environment. • The BeyondTrust Retina network security scanner incorporates a very broad and deep array of vulnerabilities and target assets definitions.

3.12 Security Assessment and Authorization (CA)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application 3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems 3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. 3.12.4 Develop, document and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships	Security Assessments CA-2 CA-2a. CA-2a.3 CA-2b. CA-2c. CA-2d.	*The organization Develops a security assessment plan that describes the scope of the assessment including Security controls and control enhancements under assessment; Assessment procedures to be used to determine security control effectiveness; and Assessment environment, assessment team, and assessment roles and responsibilities; Assesses the security controls in the information system and its environment of operation at an organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; Produces a security assessment report that documents the results of the assessment; and Provides the results of the security control assessment to organization-defined individuals or roles.* • BeyondTrust privileged access management and vulnerability management solutions ○ Control and audit across supported platforms and information systems. ○ Provide a detailed audit trail as well as an executive style report to assist in assessing security controls effectiveness. ○ Provide detailed asset information to assist in the security assessment. ○ Include a comprehensive audit and reporting console to help organizations determine what controls have been implemented. Reports can be run ad hoc or subscribed to be received on a regular basis. ○ Reporting and analytics console supports full roles-based access controls to support an organization's defined roles or individuals. ○ Return valuable information that is used for assessment. The solution allows for role-based access control when viewing such assessment data to support a clear separation of duties. ○ Provide reports for privileged user access, privilege commands that are executed, as well as vulnerability data.

with or connections to other systems	Plan of Action and Milestones CA-5 CA-5a. CA-5b.	*The organization develops a plan of action and milestones for the information system to document the organizations planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and updates existing plan of action and milestones at organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.* • The BeyondTrust IT Risk Management platform, Retina and PowerBroker Password Safe provide remediation information. This information is organized based on organizational priorities and can be used to track remediation progress and milestones.
	Continuous Monitoring CA-7 CA-7a. CA-7b. CA-7c. CA-7d. CA-7e. CA-7f. CA-7g.	*The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:* *Establishment of organization-defined metrics] to be monitored;* *Establishment of organization-defined frequencies for monitoring and organization-defined frequencies for assessments supporting such monitoring;* *Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; correlation and analysis of security-related information generated by assessments and monitoring; response actions to address results of the analysis of security-related information; and* *reporting the security status of organization and the information system to organization-defined personnel or roles, at an organization-defined frequency.* • BeyondTrust privileged access management and vulnerability management solutions provide a mechanism to perform continuous monitoring based on the organization's defined metrics. Many commonly used metrics are predefined within the solution. These continuous monitoring mechanisms can be tailored to meet an organizations frequency requirements. • The PowerBroker PAM platform provides privileged command execution and file integrity monitoring. This information can be presented for both scheduled reports and alerting, insuring compliance.

		• BeyondTrust privileged access management and vulnerability management solutions provide a security dashboard view to gain insight into an organizations security status based on defined metrics. • The BeyondTrust IT Risk Management Platform offers an advanced threat analytics feature that analyzes and pinpoints anomalies within the data collected from BeyondTrust privileged access management and vulnerability management solutions as well as third party feeds. These clusters can help identify patterns indicating malicious activity • The BeyondTrust IT Risk Management Platform includes a reporting feature that allows for quicker and easier ways to summarize audit data, targeting the most meaningful information quickly and easily based on internal and external filters. • BeyondTrust privileged access management and vulnerability management solutions have the capability to perform limited actions based on the security-related information gathered. • The BeyondTrust risk management platform can assist in providing the security status of the organization. Access to the platform and reports is based on RBAC. • Roles-based access control features allow the system to be used for both internal and independent types of assessments. • Features within the BeyondTrust IT Risk Management platform allow for the discovery of and reporting on security related trends within an organization. This information can be distributed directly from the tool or sent to external systems.

3.13 System and Communication Protection Policy and Procedures (SC)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

Derived Security Requirements		
3.12.3 Separate user functionality from system management functionality	Application Partitioning/Interfaces for Non-Privileged Users SC-2	*The information system separates user functionality (including user interface services) from information system management functionality.* • BeyondTrust privileged access management and vulnerability management solutions support implementation of granular, targeted policies to allow or prohibit information system use and administration. Any allowed or prohibited access can be audited and/or alerted on for further analysis.
3.12.4 Prevent unauthorized unintended information transfer via shared system resources.	Information in Shared Resources SC-4w	*The information system prevents unauthorized and unintended information transfer via shared system resources*. • PowerBroker PAM Platform solutions include measures, (e.g. SSL Certificates, RBAC) to help prevent unauthorized access to shared system resources. • Both PowerBroker for Unix & Linux and Integration Services allow for targeted policies that regulate which devices can communicate with each other, and assist in specified criteria that establishes what type of data is allowed. • This solution provides a granular policy engine which allows administrators to dissect information transfer between security domains, and based on real-time finding trigger enforcement of organizational policy.
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards	Transmission Confidentiality and Integrity SC-8 SC-8(1)	*The information system protects the (one or more): confidentiality; integrity of transmitted information.* *The information system implements cryptographic mechanisms to (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by organization-defined alternative physical safeguards].* • BeyondTrust privileged access management and vulnerability management solutions: ○ Allow you to create policies based on product function, user role or asset sensitivity. This control promotes a granular, highly secure environment.

		○ Provide various cryptographic solutions for communications. This includes SSL, Hash Values/Checksums on installers, and data encryption.
3.13.11 Employ FIPS validated cryptography when used to protect the confidentiality of CUI.	Cryptographic Protection SC-13	*The information system implements organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.* • BeyondTrust privileged access management and vulnerability management solutions provide various cryptographic solutions for communications. This includes SSL, Hash Values/Checksums on installers, and data encryption.
3.13.15 Protect the authenticity of communication sessions	Session Authenticity SC-23	*The information system protects the authenticity of communications sessions.* *The information system invalidates session identifiers upon user logout or other session termination.* • PowerBroker Password Safe provides secure end-to-end session communication between targeted systems. It utilizes one-time use session IDs to connect targeted systems. This model prevents unauthorized or repetitive use of granted access.

3.14 System and Information Integrity (SI)

For a deeper examination of specific capabilities as they align to specific NIST SP800-53.r4 controls please reference our technical guide "*Addressing NIST SP800-53 Requirements with BeyondTrust Solutions*".

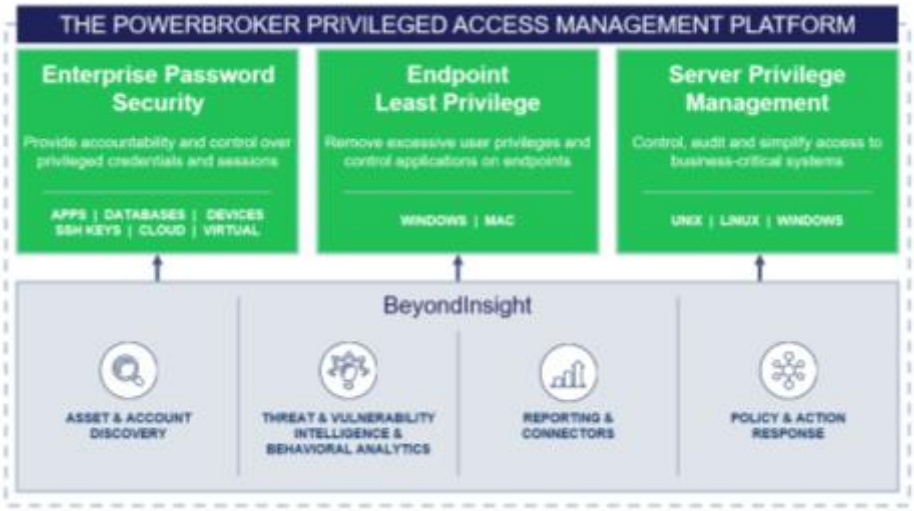
Basic Security Requirement		
3.14.1 Identify, report, and correct information and system flaws in a timely manner. 3.14.2 Provide protection from malicious code at appropriate locations within organizational systems 3.14.3 Monitor system security alerts and advisories and take appropriate actions in response	Flaw Remediation SI-2 SI-2a. SI-2b. SI-2c. SI-2d.	*The organization identifies, reports, and corrects information system flaws;* *tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; installs security-relevant software and firmware updates within the organization-defined time period of the release of the updates; and incorporates flaw remediation into the organizational configuration management process.* • The BeyondTrust IT Risk Management platform can assist with the identification, reporting and remediation of flaws in information systems. • The BeyondTrust IT Risk Management platform provides many vulnerability trending reports that assist in measuring time between identification and remediation.
	Malicious Code Protection SI-3 SI-3a. SI-3c. SI-3c.2	*The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; configures malicious code protection mechanisms to (one or more): block malicious code; quarantine malicious code; send alert to administrator; or other organization-defined action in response to malicious code detection* • PowerBroker for Windows, together with The BeyondTrust IT Risk Management Platform, evaluates all recorded application data for the presence of known malicious code. This information is used in real-time, at application launch to deny/quarantine and report on further attempts to execute this software throughout the enterprise.

	Security Alerts, Advisories and Directives SI-5 SI-5a. SI-5b. SI-5c. SI-5d.	*The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis; Generates internal security alerts, advisories, and directives as deemed necessary;* *disseminates security alerts, advisories, and directives to: (one or more): organization-defined personnel or roles; organization-defined elements within the organization; organization-defined external organizations; and implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.* • The BeyondTrust IT Risk Management platform, Retina and PowerBroker for Windows products provide automated emails and alerts can be generated based on various usage conditions including usage and access control changes. Alerts can also be generated based on found security flaws.
Derived Security Requirements		
3.14.4 Update malicious code protection mechanisms when new releases are available 3.14.15 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened or executed.	Malicious Code Protection SI-3 SI-3a. SI-3c. SI-3c.2	*The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; configures malicious code protection mechanisms to (one or more): block malicious code; quarantine malicious code; send alert to administrator; or other organization-defined action in response to malicious code detection* • PowerBroker for Windows, together with The BeyondTrust IT Risk Management Platform, evaluates all recorded application data for the presence of known malicious code. This information is used in real-time, at application launch to deny/quarantine and report on further attempts to execute this software throughout the enterprise.

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. 3.14.7 Identify unauthorized use of organizational systems.	Information System Monitoring SI-4c. SI-4c.1 SI-4c.2 SI-4d. SI-4g.	*Deploys monitoring devices strategically within the information system to collect organization-determined essential information; and at ad hoc locations within the system to track specific types of transactions of interest to the organization* *Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; provides organization-defined information system monitoring information to organization-defined personnel or roles, (one or more): as needed; at the organization-defined frequency.* • BeyondTrust privileged access management and vulnerability management solutions: ○ can collect, store and report on many attributes about information systems. This information is protected via RBAC. ○ allow RBAC controls to be implemented by roles based on group membership, and or individual.

The PowerBroker Privileged Access Management Platform

The PowerBroker Privileged Access Management Platform is an integrated solution to provide control and visibility over all privileged accounts and users. By uniting best of breed capabilities that many alternative providers offer as disjointed tools, the PowerBroker platform simplifies deployments, reduces costs, improves system security and closes gaps to reduce privileged risks.



PRODUCT CAPABILITIES WITHIN THE POWERBROKER PAM PLATFORM

The PowerBroker platform includes the following individual best-of-breed products that are fully integrated into the platform itself. For how these products help to achieve NIST requirements, please reference the detailed charts earlier in this document.

PowerBroker Password Safe	PowerBroker Password Safe is an automated password and privileged session management solution offering secure access control, auditing, alerting and recording for any privileged account – from local or domain shared administrator, to a user's personal admin account (in the case of dual accounts), to service, operating system, network device, database (A2DB) and application (A2A) accounts – even to SSH keys, cloud, and social media accounts. Password Safe offers multiple deployment options, broad and adaptive device support, with session monitoring, application password management and SSH key management included natively.
PowerBroker for Windows	PowerBroker for Windows (PBW) is a privilege management solution that mitigates the risks of cyber-attacks as a result of users having excessive rights. By removing admin rights, protecting the integrity of critical files, and monitoring user behavior, PBW protects organizations without impacting end-user productivity.
PowerBroker for Mac	PowerBroker for Mac reduces the risk of privilege misuse by enabling standard users on Mac OS to perform administrative tasks successfully without entering elevated credentials.

PowerBroker for Unix & Linux	PowerBroker for Unix & Linux is a least privilege solution that enables IT organizations to eliminate the sharing of credentials by delegating Unix and Linux privileges and elevating rights to run specific Unix and Linux commands without providing full root access.
PowerBroker for Sudo	PowerBroker for Sudo provides centralized policy, logging, and version control with change management for multiple sudoers' files. The solution simplifies policy management, improves log security and reliability, and increases visibility into entitlements. This makes it easier for you to securely manage on low-priority servers or in areas where completely replacing sudo is not feasible.
PowerBroker Identity Services	PowerBroker Identity Services centralizes authentication for Unix, Linux, and Mac environments by extending Active Directory's Kerberos authentication and single sign-on capabilities to these platforms. By extending Group Policy to non-Windows platforms, PowerBroker provides centralized configuration management, reducing the risk and complexity of managing a heterogeneous environment.
Retina CS	Retina CS is a vulnerability management software solution designed from the ground up to provide organizations with context-aware vulnerability assessment and risk analysis for making better privileged access management decisions.
Platform Capabilities	The PowerBroker platform is built on the shared capabilities found in BeyondInsight, our IT risk management platform. Common components centralized for all products in BeyondInsight include asset and account discovery, threat, vulnerability and behavioral analytics, reporting and connectors to third-party systems, and central management and policy.

About BeyondTrust

BeyondTrust® is a global security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: privileged access management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.