WHITEPAPER

Addressing NIST SP 800-53 Requirements

Implementing Security Controls for Federal Information Systems with BeyondTrust Privileged Access Management Solutions

BeyondTrust

Contents

Overview of NIST SP 800-53

NIST Special Publication 800-53 provides a catalog of security controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce.

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002 (FISMA) and to help with managing cost effective programs to protect their information systems.

The purpose of the NIST 800-53 is to provide guidelines and best practices for protecting the government's sensitive information and citizens' personal information from cyber-attacks. This special publication is authored by the Joint Task Force.

Meeting NIST requirements sets the baseline for security controls for all agencies and contractors. They are continuously updated to address ever-growing threats and to prevent major cyber security incidents. The NIST 800-53—the special publication for the Security and Privacy Controls for Information Systems and Organizations—is currently in Revision 4.

Meeting NIST SP 800-53 Requirements with BeyondTrust

This white paper explores some of the most important NIST security control families and align BeyondTrust capabilities with the controls directly related to privilege access management. In the pages that follow you will find specific control guidance directly from NIST SP 800-53, and information regarding how BeyondTrust supports each.

Implementing NIST SP 800-53 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.

NIST Control Families Chart

Access Control Family	How We Align
AC-1 ACCESS CONTROL POLICY AND PROCEDURES *An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the access control policy and associated access controls; and reviews and updates the current access control policy organization-defined frequency.*	BeyondTrust Privilege Management solutions provide several methods to support the controlled implementation of policies, along with technology to manage policies as develop through a change control and deployment life cycle.. In addition, BeyondTrust solutions incorporate role-based access control policies to limit and restrict access to only authorized users.
AC-2 ACCOUNT MANAGEMENT *Covers full range of activities related to managing accounts.*	BeyondTrust Privilege Access Management solutions provide discovery technology to aid in the identification of accounts based on assets, applications, and privileges. This information allows for: • Policy and account ownership to be assigned to managers of information system accounts. • Users can be assigned access privileges based on contextual aware policy and just in time privileged access management initiatives. • Accounts that have not been used for a given amount of time can be flagged for mitigation procedures or removal. • Alert on inappropriate account changes and perform backup and restoration on Active Directory accounts.

AC-3 ACCESS ENFORCEMENT *To enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.*	BeyondTrust's Privilege Access Management solutions provide native workflow capabilities and integrations into existing ITSM solutions to ensure proper authorization is granted before a user is provided access. These capabilities include: • Workflows requiring multiple approvals such that two or more individuals must approve user access before granting permissions. • Security-relevant information is logged during all access attempts and can be forwarded to other solutions of authority. • Role-based access control based on IAM integrations, Active Directory, LDAP, on native RBAC models. • Revocation of access authorization based on context or suspicious activity. • Secure remote access internally or externally based on context or just in time requirements. • Access control restrictions to limit lateral movement or attempts to exfiltrate data. • Enforcement of least privilege even when assigned tasks require administrative rights.

AC- 4 INFORMATION FLOW *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.*	BeyondTrust endpoint solutions and password management solutions allow for policies that restrict lateral movement, commands used to make remote connections, and the monitoring and restriction of applications that would violate information flow architectures and policies.
AC-5 SEPARATION OF DUTIES *To document separation of duties of individuals; and define system access authorizations to support separation of duties.*	BeyondTrust's Privileged Access Management solutions provide the ability to enforce policy based on end-user roles and organizational responsibilities. This provides separate, auditable, documented policy sets and individual end user interaction with resources throughout an enterprise.
AC-6 LEAST PRIVILEGE *Covers the concept of least privilege, which allows only authorized accesses for users, and processes acting on behalf of users, that are necessary to accomplish assigned tasks.*	BeyondTrust's Privileged Access Management solutions are designed around the principle of least privilege. They provide the controls required to manage a user's access privileges, allowable application launches, as well as the rights associated with those applications. This includes the capabilities to: • Audit all privileged actions attempted or taken by end users for forensics, certifications, future analysis, or other forms of security and attestation reporting. • Just in time privileged elevation capabilities grant privileges to applications and tasks – not users – without providing administrator credentials.

	• Apply policies across Unix, Linux, Windows, MacOS, and network infrastructure to enforce least privilege on virtually any network connected asset. • Apply least privileged security controls based on the applications reputation including known vulnerabilities, source of application, and attributes like digital signatures.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS AC-8 SYSTEM USE NOTIFICATION AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION AC-10 CONCURRENT SESSION CONTROL AC-11 SESSION LOCK AC-16 SECURITY ATTRIBUTES *These controls collectively encompass the limiting of the number of invalid logon attempts, displaying notifications before granting access, notifying user of date/time of last access, restricting the number of concurrent sessions, locking session after inactivity, and associating security attributes with information.*	BeyondTrust's Privileged Access Management solutions provide advanced capabilities to monitor sessions, login attempts, and session control based on a variety of security attributes. These include: Enforce an authentication failure when a set number of failed attempts have been made for a privileged session. • Provide an account lock mechanism upon consecutive failed attempts. • Initiate a lock out based on a manual action or detected suspicious behavior. • Display and require feedback based messaging to end-users based on end user location, system details or other organizational policies based on the execution of an application. • Limit the maximum [concurrent] privileged or standard user sessions allowed to a managed device. • Terminate a user's session based on idle time or a pre-set length of time a session is active. • Integrate with third party identity governance solutions to apply security attributes to BeyondTrust's authentication model or conte aware policy.
AC-17 REMOTE ACCESS AC-18 WIRELESS ACCESS *Need to establish usage restrictions and authorizations for remote and wireless access*	BeyondTrust Privileged Access Management solutions incorporate role-based access control policies that limit, monitor, and restrict remote and wireless access to only authorized users. This includes the capability to harden end user wireless activity.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS *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.*	BeyondTrust provides Privileged Access Management solutions that can control and monitor the use of external information systems via secure remote access technology. This capability includes: • Secure remote access without the need of a VPN client • Full session monitoring and keystroke logging capabilities • Just in time access to delegated resources • Privileged access management capabilities for credential injection and non-disclosure of credentials to authorized users. • Independence from protocol tunneling and adherence to security best practices for disabling native OS remote access services.
AC-21 INFORMATION SHARING *The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required; and employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.*	BeyondTrust Privileged Access Management solutions are designed around the principle of least privilege. They provide the controls required to 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. This provides advanced controls for information sharing, resource access, and notifications around inappropriate information sharing risks.
	BeyondTrust Privileged Access Management solutions are designed around the principle of least privilege. They provide the controls required

AC-24 ACCESS CONTROL DECISIONS *The information system enforces access control decisions based on organization-defined security attributes that do not include the identity of the user or process acting on behalf of the user.*	that dictate a users' access rights, allowable application launches, and rights associated with those applications based on attribute-based access control. In addition, all actions attempted or taken by end-users can be reported for additional analysis and forensics based on the organization's security attributes.
AC-25 REFERENCE MONITOR *The information system implements a reference monitor for organization-defined access control policies that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.*	BeyondTrust's Privileged Access Management solutions contain tamperproof policy deployment and verification technology to ensure policies cannot be compromised. In addition, policies can be tested and analyzed using native tools to ensure that are being managed and enforced appropriately.

Identification & Authentication Family	How We Align
IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES *The organization develops, documents, and disseminates to organization-defined personnel or roles: an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.*	BeyondTrust allows you to create policies based on product function, user role or asset sensitivity. This control promotes a granular, highly secure environment in support privileged authentication policies and procedures.
IA-2 ACCESS TO PRIVILEGE ACCOUNTS *The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets organization-defined strength of mechanism requirements.*	BeyondTrust Privileged Access Management solutions support multifactor authentication for host, resource, network, and application access when utilizing privileged accounts. The solution is designed to integrate with industry leading multifactor authentication solutions for business continuity within an organization.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION *The information system uniquely identifies and authenticates organization-defined specific and/or types of devices before establishing a (one or more): local; remote; network] connection.*	BeyondTrust products support the use of 2FA, MFA, and PIV Credentials prior to granting authorization/rights to system resources in accordance with established policies.
IA-5 AUTHENTICATOR MANAGEMENT *Covers management of information system authenticators such as passwords and other types of authenticators.*	BeyondTrust Privileged Access Management solutions provide varied and customizable password policies, taking into consideration complexity, lifetime as well as prohibiting re-use of old passwords. In addition, passwords can also be managed long term with restricted access/use to authorized individuals and services.

IA-8 IDENTIFICATION AND AUTHENTICATION (NONORGANIZATIONAL USERS) *The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Non-organizational users include information system users other than organizational users explicitly covered by IA-2.*	BeyondTrust Privileged Access Management solution allow for the use and management of federated and Unfederated accounts. This allows brokered and recorded access to enterprise devices depending on role and governance for nonorganizational users. This identification and authentication model also support one time and just in time access for authorized nonorganizational users.
IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION *The organization identifies and authenticates organization-defined information system services using organization-defined security safeguards. This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services.*	BeyondTrust Privilege Access Management solutions are designed to manage the credentials, certificates, and privileges associated with service-oriented architectures and other designs that require components to authenticate using application to application models.

IA-11 RE-AUTHENTICATION *The organization requires users and devices to re-authenticate when organization-defined circumstances or situations requiring re-authentication.*	BeyondTrust Privilege Access Management solutions allow for policies based on role changes, context, entitlements, time/date, and other factors that can trigger a new challenge and response authentication request. This can apply directly to BeyondTrust software or the resources being used for privileged or remote access.

Audit & Accountability Family	How We Align
Controls related to generating, protecting, and reviewing audit records and ensuring accountability.	
AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES AU-2 AUDIT EVENTS AU-3 CONTENT OF AUDIT RECORDS AU-4 AUDIT STORAGE CAPACITY AU-5 RESPONSE TO AUDIT PROCESSING FAILURES AU-6 AUDIT REVIEW, ANALYSIS, REPORTING AU-7 AUDIT REDUCTION AND REPORT GENERATION AU-8 TIME STAMPS AU-9 PROTECTION OF AUDIT INFORMATION AU-10 NON-REPUDIATION AU-11 AUDIT RECORD RETENTION	BeyondTrust Privileged Access Management solutions help organizations implement automated controls for generating, protecting, and reviewing audit records based on all privileged user, asset, and application activity. This includes: • Verification of audit, accountability, and privileged workflow procedures implemented in the solution. • Detailed audit events for privileged activity and privileged credential usage • Tamper protection to ensure audit records are accurate • Automatic notification and correction of faults when collecting logs or audit data related to the system. • Detailed reporting and indexing of audit data with anomaly and behavioral detection • Time stamp and detailed audit information to perform required analysis for regulatory compliance or determine if there is an indicator of compromise. • Configurable audit log retention parameters to adhere to local, regional, industry, or government regulatory policies.

Security & Assessments Family	How We Align
Includes controls for assessing and authorizing security controls including authorizing connections within and between systems and ensuring on-going assessments.	
CA-1 Security Assessment and Authorization Policy and Procedures CA-2 security Assessment CA-3 SYSTEM INTERCONNECTIONS CA-7 CONTINOUS MONITORING CA-9 security compliance checks	BeyondTrust Privileged Access Management solutions provide the following: • Security control assessment 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. • Reporting and analytics to support full roles-based access to security assessment findings • Provide reports for privileged user access, privilege commands that are executed, as well as vulnerability data. • Perform continuous monitoring based on the organization's defined metrics for vulnerability and privileged access assessments. • Verify application and command relevance before execution on a resource.

Contingency Planning Family	How We Align
Addresses controls needed for contingency planning.	
CP-9 INFORMATION SYSTEM BACKUP CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	BeyondTrust's Privileged Access Management platform offers high availability, full disaster recovery capabilities, and automated backup procedures to ensure contingency planning for privileged accounts can be maintained. These capabilities help ensure privileged credentials are always accessible and available for the requesting systems, even in network outages. Password versioning and reconciliation capabilities further enhance the criticality of being able to access systems with privileged credentials, even if the restoration of a backup from a prior time and date is required. These capabilities also include Break Glass models for unforeseen outages.

System & Communications Family	How We Align
Controls regarding system and communications protection.	
SC-2 APPLICATION PARTITIONING SC-3 SECURITY FUNCTION ISOLATION SC-5 DENIAL OF SERVICE PROTECTION SC-7 BOUNDARY PROTECTION SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY SC-10 NETWORK DISCONNECT SC-11 TRUSTED PATH SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT SC-13 CRYPTOGRAPHIC PROTECTION SC-23 SESSION AUTHENTICITY SC-24 FAIL IN KNOWN STATE SC-25 THIN NODES SC-28 PROTECTION OF INFORMATION AT REST SC-29 HETEROGENEITY SC-30 CONCEALMENT AND MISDIRECTION SC-32 INFORMATION SYSTEM PARTITIONING SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS	BeyondTrust's Privileged Access Management solutions can successfully address a wide-range of the requirements for system and communications protection, including transmission, architecture, cryptographic procedures and functions. This includes: • Separating the password safe database from other components, isolating it and keeping the encryption keys separate. • Allowing an architecture to keep critical components separated and isolated • Enable system components to reside on the internal network, DMZ, or in the cloud helping to ensure security best practices are adhered too • Access Control based on subnet or IP address or other attribute based context • Ensure session authenticity by SSL verification between components and the end user or application. • Optimized using standard ports and protocols • FIPS 140-2 validated cryptography • High availability and disaster recovery architectures are native to the solution. • Common Criteria EAL2 certified • Support for heterogeneous environments including Unix, Linux, Windows, MacOS, infrastructure and next generation technologies • Available as software, virtual or physical appliances, or in the cloud marketplaces for AWS, Azure, and Google. • Hardening of all appliances to DoD Gold Standard STIGs

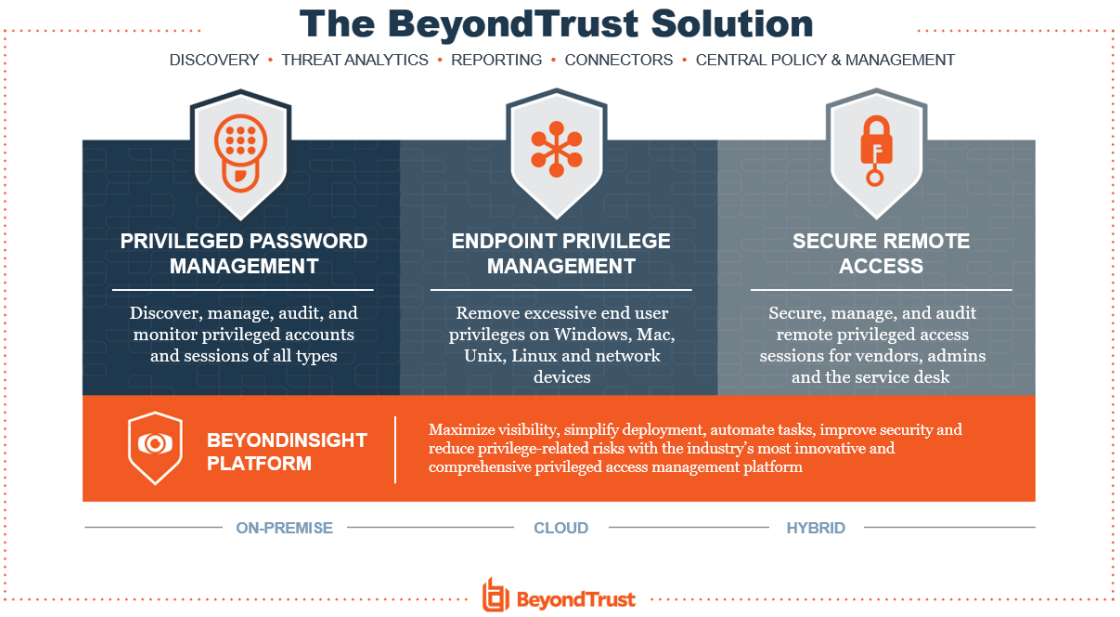
System & Information Integrity Family	How We Align
Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls	
SI-3 MALICIOUS CODE PROTECTION SI-4 INFORMATION SYSTEM MONITORING SI-6 SECURITY FUNCTION VERIFICATION SI-10 INFORMATION INPUT VALIDATION SI-11 ERROR HANDLING SI-12 INFORMATION HANDLING AND RETENTION	BeyondTrust helps organizations meet the requirements for system/information integrity through an internal component check. In case of failure, the system can fail open or closed to isolate a security incident or not disrupt business continuity. All system information in transit is encrypted and verified before logged and inserted into its database. To that end, BeyondTrust's privileged access management platform, when deployed as an appliance, provides: • Native malicious code protection via application control, least privilege, file integrity monitoring, and antivirus • Comprehensive application and operating system monitoring to determine faults and potential indicators of compromise • Automatic diagnostic reporting to determine the solutions health. • Validation of all communications and input to verify integrity of receive information • Automatic error handling and data recovery • Configurable data retention and sanitization policies.

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. In the 2020 Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

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.



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.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

Privilege Management for Windows & Mac

BeyondTrust Privilege Management for Windows & Mac elevates privileges to known good applications that require them, controls application usage, and logs and reports on privileged activities using security tools already in place.

Privilege Management for Unix/Linux Servers

BeyondTrust Privilege Management for Unix & Linux is an enterprise-class, gold-standard privilege management solution that gives you unmatched visibility and control over complex server environments.

Password Safe

BeyondTrust Password Safe unifies privileged password and privileged session management, providing secure discovery, management, auditing, and monitoring for any privileged credential. Password Safe enables organizations to achieve complete control and accountability over privileged accounts.

Privileged Remote Access

BeyondTrust Privileged Remote Access secures, manages, and audits vendor and internal remote privileged access without a VPN. Privileged Remote Access enables security professionals to control, monitor, and manage privileged access to critical systems.

Conclusion

NIST SP 800-53 outlines a “Build It Right” strategy combined with various security controls for continuous monitoring, striving to provide senior leaders of organizations information to support better risk-based decision-making related to their critical missions. We hope this in-depth guide has provided a comprehensive overview of how BeyondTrust solutions map to the fundamentals of the NIST SP 800-53 requirements.

If there is an item/family not covered in this condensed express guide, please don’t hesitate to get in touch - chances are we address them in some way. And for any other queries around meeting NIST compliance, please don’t hesitate to contact us.

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.

V2020_06_ENG