BeyondTrust

WHITEPAPER

MAPPING BEYONDTRUST CAPABILITIES TO PCI DSS 3.2

CONTENTS

PCI DSS 3.2 - Overview

This guide has been prepared so that IT and security administrators can quickly understand how BeyondTrust Privileged Access Management (PAM) solutions map into requirements set forth in the Payment Card Industry Data Security Standard (PCI DSS) version 3.2. This guide is primarily intended to be used for those who must comply with merchant processing specifications but applies to most service providers as well.

What is the Payment Card Industry Data Security Standard (PCI DSS)?

Initially developed in 2004, and currently on version 3.2, the Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for every organization that accepts credit cards such as Visa, MasterCard, American Express, and others. The PCI standard:

- Was created to increase controls around cardholder data to reduce credit card fraud
- Has become a de facto standard for protecting access to personally identifiable information (PII), especially in the retail industry
- Is mandated by the card issuers; and
- Is administered by the Payment Card Industry Security Standards Council (PCI SSC)

No single software product can ensure or implement “PCI compliance” for any enterprise. Nor is any software product in itself, “PCI compliant.” Compliance to the PCI Data Security Standard (DSS) requires a combination of business practices, personnel management, physical restrictions, and software tools.

However, specific provisions contained in the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures Version 3.2 document of the PCI Security align to a number of capabilities in the BeyondTrust solution portfolio.

PCI Data Security Standard – High Level Overview

Source
www.pcisecuritystandards.org

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Challenges for IT Organizations in Meeting PCI Requirements

Organizations that must comply with the merchant requirements under PCI face several challenges when working to prove their compliance with PCI DSS.

Fines And Penalties: Compliance Is Mandatory

There are three levels of PCI compliance that an organization may be subject to, depending on the number of transactions that the organization processes, or if they are subject to the "merchant" or the "service provider" compliance definitions. If an organization is at the highest level of compliance (Tier 1), assessments are conducted annually by a Qualified Security Assessor (QSA) who creates a Report on Compliance (ROC). Any other levels of compliance (Tiers 2-3), may self-assess against the controls and may not directly involve a QSA. If an organization has been breached and was not in compliance with PCI, the card issuers can impose significant financial penalties on the merchant.

Complexity, Time, And Resource Constraints: PCI Distracts From Core Operations

Merchants and service providers subject to PCI DSS should work to continually improve processes to ensure ongoing compliance and security, rather than treating compliance as a point-in-time project. Naturally, this can create a tremendous resource drain on IT teams.

How BeyondTrust Solutions Can Help

As they can be used as fundamental technologies to achieve compliance, this white paper explains how to map BeyondTrust solutions to PCI DSS requirements to maintain security and more easily demonstrate and maintain compliance. BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges.

Each PCI DSS requirement is outlined in the following sections and are mapped to these BeyondTrust solutions:

- (PPM) Privileged Password Management - Enable automated discovery and onboarding of all privileged accounts, secure access to privileged credentials and secrets, and auditing of all privileged activities.
- (SRA) Secure Remote Access - Apply least privilege and robust audit controls to all remote access required by employees, vendors, and service desks.
- (EPM) Endpoint Privilege Management - Combine privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity.

The tables on the following page highlight the primary applicable PCI DSS requirements that are addressed by capabilities within BeyondTrust solutions. This is not an exhaustive list but includes the most relevant features for supporting PCI DSS compliance.

Note: BeyondTrust solutions are not directly subject to the PCI DSS requirements. If BeyondTrust solutions are used by an organization that is subject to the PCI DSS, it is up to a PCI Qualified Security Assessor (QSA) and the organization to determine the scope for their compliance assessment.

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources to assist organizations with their PCI DSS assessments and validations.

Mapping BeyondTrust Solutions To PCI DSS 3.2 Requirements

Requirement 1. Install And Maintain A Firewall Configuration To Protect Cardholder Data

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
1.1	Establish and implement firewall and router configuration standards that include the following:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.	BeyondTrust supports controlling, monitoring, recording, and notification based on the use of managed accounts and/or connections of managed accounts while providing a detailed audit trail of events and configurations changes that occurred through recorded sessions, keystroke logging, and prevention of execution. The implementation of ACLs will be required in order to enforce these capabilities.	●	●	
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.	BeyondTrust supports the enforcement of adaptive controls over privileged accounts with access by enabling approval(s) flow prior to usage. In addition, BeyondTrust can control, monitor, record, and notify based on the use of managed accounts and/or connections of managed accounts while providing a detailed audit trail of events and configurations changes that occurred through recorded sessions, keystroke logging, and prevention of execution. The implementation of ACLs will be required in order to enforce these capabilities.	●	●	
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Network diagrams describe how networks are configured and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.	BeyondTrust supports network scanning to identity systems and assets.	●	●	

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Using a firewall on every Internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.	BeyondTrust supports controlling, monitoring, recording, and notifications based on the use of managed accounts and/or connections of managed accounts while providing a detailed audit trail of events and configurations changes that occurred through recorded sessions, keystroke logging, and prevention of execution on firewalls and routers.	●	●	
1.1.6	Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	1.1.6b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. *Note- BeyondTrust solutions apply to 1.1.6b, requirements listed above*	BeyondTrust supports minimizing the impact of services, protocols and ports by restricting, limiting, or preventing applications, executables, and execution.	●	●	●
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. *Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable to unauthorized access by malicious individuals or software. For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity's network.	BeyondTrust supports controlling, monitoring, recording, and notifications based on the use of managed accounts and/or connections of managed accounts while providing a detailed audit trail of events and configurations changes that occurred through recorded sessions, keystroke logging, and prevention of execution.	●	●	
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).	BeyondTrust supports outbound traffic flow which is restricted only to BeyondTrust for communication. The configuration is unique to the entity organization utilizing TLS encryption with an X.509 certificate. Communication can only occur with BeyondTrust as a result.		●	

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	If cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. Securing system components that store cardholder data in an internal network zone that is segregated from the DMZ and other untrusted networks by a firewall can prevent unauthorized network traffic from reaching the system component. *Note: This requirement is not intended to apply to temporary storage of cardholder data in volatile memory.*	BeyondTrust supports configurations that can leverage segregated, segmented, and untrusted networks.	●	●	
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: ▪ Specific configuration settings are defined. ▪ Personal firewall (or equivalent functionality) is actively running. ▪ Personal firewall is not alterable by users of the portable computing devices.	Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is re-connected to the network. The specific firewall configuration settings are determined by the organization. *Note: This requirement applies to employee-owned and company-owned portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to an organization's CDE could result in access being granted to attackers and other malicious users.*	BeyondTrust supports the ability to limit, prevent, deny, and notify on commands and executables used including the ability to disable a firewall.	●		●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.	BeyondTrust supports controlling, monitoring, recording, and notifications based on the use of managed accounts and/or connections of managed accounts while providing a detailed audit trail of events and configurations changes that occurred through recorded sessions, keystroke logging, and prevention of execution.	●	●	

Requirement 2. Do Not Use Vendor-Supplied Defaults For System Passwords And Other Security Parameters

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.	BeyondTrust supports the scanning, discovery, onboarding, and management of default credentials.	●	●	
2.1.1.b	Interview personnel and examine policies and procedures to verify: ▪Default SNMP community strings are required to be changed upon installation. ▪Default passwords/passphrases on access points are required to be changed upon installation.	If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. In addition, the key-exchange protocol for older versions of 802.11x encryption (Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.	BeyondTrust supports scanning, discovery, onboarding, and management of wireless devices and access point credentials.	●	●	
2.1.1.c	Examine vendor documentation and login to wireless devices, with system administrator help, to verify: ▪Default SNMP community strings are not used. ▪Default passwords/passphrases on access points are not used.					

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.					
2.2.a	Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses. Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov, www.sans.org, and www.cisecurity.org, www.iso.org, and product vendors. System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.	BeyondTrust supports industry-standard hardening requirements.	●	●	
2.2.c	Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.		BeyondTrust supports scanning and enumeration of system services, ports, protocols, and software to determine configuration.	●		
2.2.d	Verify that system configuration standards include the following procedures for all types of system components: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure • Configuring system security parameters to prevent misuse • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		BeyondTrust supports scanning, discovery, onboarding, and management of assets, their default account and passwords in order to ensure default passwords are rotated automatically according to policy. In addition, BeyondTrust can prevent the use of application functionality, scripts, and executables that are not approved.	●	●	●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*	If server functions that need different security levels are located on the same server, the security level of the functions with higher security needs would be reduced due to the presence of the lower-security functions. Additionally, the server functions with a lower security level may introduce security weaknesses to other functions on the same server. By considering the security needs of different server functions as part of the system configuration standards and related processes, organizations can ensure that functions requiring different security levels don't co-exist on the same server.	BeyondTrust supports appliance-based solutions and logical asset grouping configurations based on attributes. BeyondTrust can scan and enumerate services, ports, protocols, and software on assets which can be used to determine what is approved or not approved for use.	●	●	
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	As stated in Requirement 1.1.6, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. Including this requirement as part of an organization's configuration standards and related processes ensures that only the necessary services and protocols are enabled.	BeyondTrust support appliance-based solutions leveraging only needed services, ports, protocols, and software. BeyondTrust can scan and enumerate services, ports, protocols, and software which can be used to determine what is approved or not approved for use.	●	●	
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network.	BeyondTrust supports the scanning and enumeration of systems in order to identify services, ports, protocols, and software on assets which can used to validate configurations. In addition, BeyondTrust can discovery, onboard, and enforce password management of accounts based on policy.	●		

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
2.2.4	Configure system security parameters to prevent misuse.	System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.	Beyondtrust supports numerous security parameter configuration options, some of which are wizard driven. Organizations can configure based upon specific security requirements and use cases. In addition, BeyondTrust supports the scanning and enumeration of system services, ports, protocols, and software which can be used to identify installed, drivers, features, roles, sub systems, file systems and web services.	●	●	
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. By removing unnecessary functionality, organizations can focus on securing the functions that are required and reduce the risk that unknown functions will be exploited. Including this in server-hardening standards and processes addresses the specific security implications associated with unnecessary functions (for example, by removing/disabling FTP or the web server if the server will not be performing those functions).	BeyondTrust supports the scanning and enumeration of system services, ports, protocols, and software which can be used to identify installed, drivers, features, roles, sub systems, file systems and web services.	●		
2.3 Encrypt all non-console administrative access using strong cryptography. Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:						
2.3.a	Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.	If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's IDs	BeyondTrust supports encrypted administrative web access.	●	●	●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
2.3.b	Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.	and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. To be considered “strong cryptography,” industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography” in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.) *Note: SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect, defined in Appx A2*	BeyondTrust supports appliance-based solutions which are configured with only essential services, protocols, and ports enabled for functionality.	●	●	●
2.3.c	Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.		BeyondTrust supports encrypted administrative web access.	●	●	●
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization’s configuration standards.	BeyondTrust supports the scanning and enumeration of system services, ports, protocols, and software which can be used to determine installed components for validation and inventory.	●		●

Requirement 3. Protect Stored Cardholder Data

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage.	A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. Understanding where cardholder data is located is necessary so it can be properly retained or disposed of when no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained. Identifying and deleting stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated or manual or a combination of both. For example, a programmatic procedure (automatic or manual) to locate and remove data and/or a manual review of data storage areas could be performed. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. Remember, if you don't need it, don't store it!	BeyondTrust supports the ability to configure retention period on recorded sessions.	●	●	
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions.	BeyondTrust supports the ability to configure retention periods for recorded sessions and mask authentication password fields	●	●	

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
	It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. For non-issuing entities, retaining sensitive authentication data post-authorization is not permitted.				
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	If full track data is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions.	BeyondTrust supports the ability to prevent cardholder data from being keystroke logged and file integrity to prevent unauthorized changes.			●
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	The purpose of the card validation code is to protect ""card-not-present"" transactions—Internet or mail order/telephone order (MO/TO) transactions—where the consumer and the card are not present. If this data is stolen, malicious individuals can execute fraudulent Internet and MO/TO transactions.	Beyondtrust supports the ability to configure masked fields.	●		

Requirement 4: Encrypt Transmission Of Cardholder Data Across Open, Public Networks

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) • General Packet Radio Service (GPRS) • Satellite communications	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted. Note that some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods). Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection. Generally, the web page URL should begin with "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser. Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a “security seal,” "secure site seal," or “secure trust seal”)—which may provide the ability to click on the seal to reveal information about the website.	BeyondTrust supports encrypted connections to remote devices and certificate-based communication with management consoles. BeyondTrust does not process, store or communicate any card holder data.	●	●	●

		Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.) Note: SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2.				

Requirement 5: Protect All Systems Against Malware And Regularly Update Anti-Virus Software Or Programs

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. Without an anti-virus solution that is updated regularly, these new forms of malicious software can attack systems, disable a network, or lead to compromise of data.	BeyondTrust supports the scanning and identification if anti-virus is present. BeyondTrust supports the prevention of executables from running.	●		●
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	It is important to protect against ALL types and forms of malicious software.	BeyondTrust supports the scanning and identification of assets to determine if anti-virus is present and its current state. BeyondTrust supports the enforcement of enabled anti-virus.	●		●
5.2.a	Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.	Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.	BeyondTrust supports detection of anti-virus definitions age.	●		●
5.2.b	Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: • Configured to perform automatic updates, and • Configured to perform periodic scans.					
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Anti-virus that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software.	BeyondTrust supports the enforcement anti-virus privileged access by limiting, preventing, and/or denying anti-virus application access to inappropriate users.			●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
	Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active—for example, disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after it is re-enabled.				

Requirement 6: Develop And Maintain Secure Systems And Applications

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
6.4.2	Separation of duties between development/test and production environments	Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know. The intent of this requirement is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment and have a separate account with user-level access to the production environment.	BeyondTrust supports user-based policies which can be leveraged for separation of duty requirements.			●

Requirement 7: Restrict Access To Cardholder Data By Business Need To Know

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.	BeyondTrust supports granular roles-based access, user-based policies, adaptive workflow with Just-In-Time capabilities to include the ability to deny access.	●	●	●
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly.				
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.				
7.1.3	Assign access based on individual personnel's job classification and function.	Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.				
7.1.4	Require documented approval by authorized parties specifying required privileges.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.				

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access. Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.	BeyondTrust supports granular roles-based access, user-based policies, adaptive workflow with Just-In-Time capabilities to include the ability to deny access.	●	●	●
7.2.1	Coverage of all system components.					
7.2.2	Assignment of privileges to individuals based on job classification and function.					
7.2.3	Default "deny-all" setting.					

Requirement 8: Identify And Authenticate Access To System Components

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.	BeyondTrust supports unique ID's for authentication. Beyondtrust support integration with enterprise authentication services and local authentication which can be used to control adds, deletions, and modifications. BeyondTrust supports revocation of user access. BeyondTrust supports authentication lockouts. BeyondTrust supports inactivity timeouts. *Applicable to 8.1.1 – 8.1.8 sub-requirements*	●	●	
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Note that a digital certificate is a valid option for "something you have" as long as it is unique for a particular user. Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.	BeyondTrust supports enterprise authentication services including various Radius, Multi-Factor, SAML, and SmartCard authentication methods.	●	●	●
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored and use this data to gain unauthorized access.	BeyondTrust supports encrypted authentication and communication transmission.	●	●	●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
8.2.3	Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/ passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use “equivalent strength” to evaluate their alternative. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.) Note: Testing Procedure 8.2.3.b is an additional procedure that only applies if the entity being assessed is a service provider.	BeyondTrust supports local and enterprise authentication services that adhere to minimum passwords length, complexity, change intervals, and history enforcement. NOTE: Not all functionality is available with local authentication.	●	●	●
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.	BeyondTrust supports enterprise authentication services including various Radius, Multi-Factor, SAML, and SmartCard authentication methods. *Applicable to 8.3.1 – 8.3.2 sub-requirements*	●	●	●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
8.4	Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	Communicating password/authentication policies and procedures to all users helps those users understand and abide by the policies. For example, guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don't contain dictionary words, and that don't contain information about the user (such as the user ID, names of family members, date of birth, etc.). Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files and being alert for malicious individuals who may attempt to exploit their passwords (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem"). Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.	BeyondTrust supports encrypted authentication, communication, transmission, and data at rest.	●	●	●
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.	BeyondTrust supports the enforcement of unique ID's for authentication. *Also Applicable to 8.5.1*	●	●	●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism.	BeyondTrust supports unique IDs for authentication and generation of random passwords.	●	●	

Requirement 9: Restrict Physical Access To Cardholder Data

Not applicable to BeyondTrust solutions

Requirement 10: Track And Monitor All Access To Network Resources And Cardholder Data

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
10.1	Implement audit trails to link all access to system components to each individual user.	It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.	BeyondTrust supports the capturing of audit events relevant but not limited to authentication, access, changes, policies, enforcement, elevation, and security. These can be integrated with a SIEM for centralized collection and forwarding of audit events.	●	●	●
10.2	Implement automated audit trails for all system components to reconstruct the following events:	Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities	Beyondtrust supports the capturing of audit events relevant but not limited to authentication, access, changes, policies, enforcement, elevation, and security. These can be integrated with a SIEM for centralized collection and forwarding of audit events. *Also Applicable to 10.2.1 – 10.2.7*	●	●	●
10.3	Record at least the following audit trail entries for all system components for each event:	By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.	BeyondTrust supports the capturing audit events relevant but not limited to authentication, access, changes, policies, enforcement, elevation, and security. *Also Applicable to 10.3.1 – 10.3.6*	●	●	●
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.	BeyondTrust supports the configuration of Network Time Protocol for time synchronization. *Also Applicable to 10.4.1 – 10.4.3*	●	●	●

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
10.5	Secure audit trails so they cannot be altered.	Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.	Beyondtrust supports the preservation of audit logs and inability to edit audit trails. In addition, BeyondTrust supports the ability to integrate with SIEM systems for centralized forwarding and collection of audit events. *Also Applicable to 10.5.1 – 10.5.5*	●	●	●
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.	BeyondTrust supports audit logs and integration with SIEM for centralized logging and forwarding of events. *Also Applicable to 10.6.1 – 10.6.3*	●	●	●
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.	BeyondTrust supports retention configuration of audit logs.	●	●	●

Requirement 11: Regularly Test Security Systems And Processes

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	Implementation and/or exploitation of wireless technology within a network are some of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, it can allow an attacker to easily and "invisibly" enter the network. Unauthorized wireless devices may be hidden within or attached to a computer or other system component or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment. Knowing which wireless devices are authorized can help administrators quickly identify non-authorized wireless devices and responding to the identification of unauthorized wireless access points helps to proactively minimize the exposure of CDE to malicious individuals. Due to the ease with which a wireless access point can be attached to a network, the difficulty in detecting their presence, and the increased risk presented by unauthorized wireless devices, these processes must be performed even when a policy exists prohibiting the use of wireless technology. The size and complexity of a particular environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment.	BeyondTrust supports the scanning and detection of wireless access points. Scanning and detection can be configured to run based upon an organization's requirements. *Also Applicable to 11.1.1 – 11.1.2*	●		

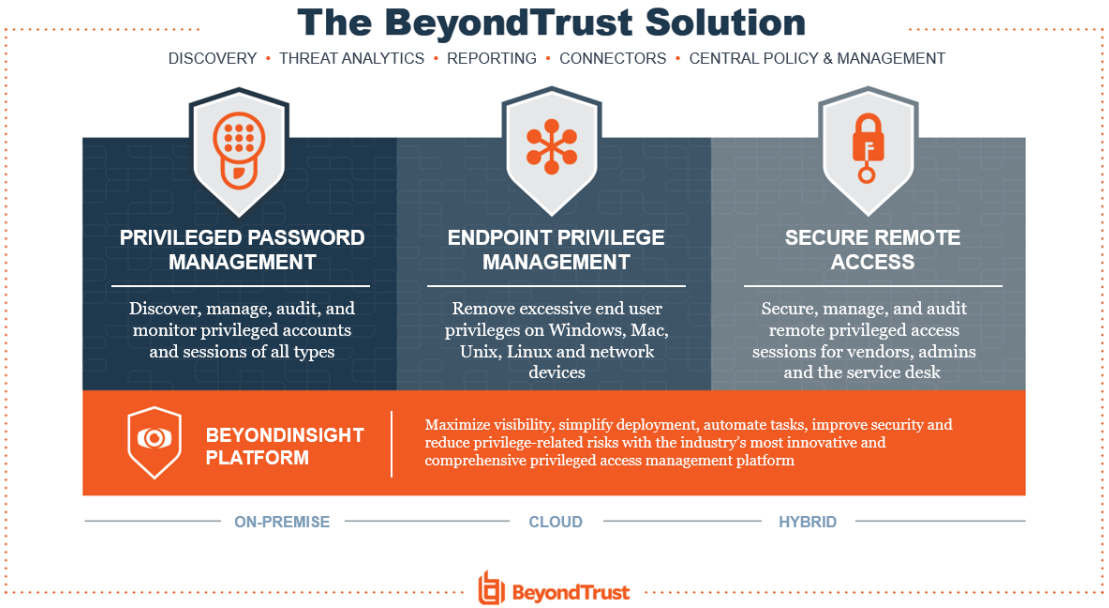
PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.	BeyondTrust support File Integrity Monitoring.			●

Requirement 12: Maintain A Policy That Addresses Information Security For All Personnel

PCI DSS 3.2 Requirements		Guidance	BeyondTrust Response	PPM	SRA	EPM
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Remote-access technologies are frequent "back doors" to critical resources and cardholder data. By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS vendor, other vendors, or business partners), access and risk to networks is minimized.	BeyondTrust supports idle session timeout.	●	●	
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use		BeyondTrust supports immediate remote access activation and deactivation.		●	
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	To ensure all personnel are aware of their responsibilities to not store or copy cardholder data onto their local personal computers or other media, your policy should clearly prohibit such activities except for personnel that have been explicitly authorized to do so. Storing or copying cardholder data onto a local hard drive or other media must be in accordance with all applicable PCI DSS requirements.	BeyondTrust supports policy configurations relative to file transfer capabilities.	●		

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions. BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace. By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

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

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

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

Learn more at beyondtrust.com.