TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Mapping BeyondTrust Solutions to HIPAA Requirements

Privileged Access Management and Vulnerability Management

Table of Contents

Purpose of This Document

This guide has been prepared so that IT and security administrators can quickly understand how BeyondTrust solutions for privileged access management and vulnerability management map into requirements set forth in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. For a quick view of how BeyondTrust solutions map into these requirements, please see table 1 below.

Table 1: Summary Mapping of BeyondTrust Solutions to HIPAA Requirements

Note: For a description of BeyondTrust products as they relate to achieving HIPAA compliance, please see the appendix.

HIPAA STANDARD	REF.	Requirement addressed or enhanced by BeyondTrust Platform	Requirement addressed by Retina Vulnerability Management	Requirement addressed by PowerBroker for Unix & Linux	Requirement addressed by PowerBroker for Windows & Mac	Requirement addressed by PowerBroker Identity Services	Requirement addressed by PowerBroker Password Safe
Security Management Process	164.308(a)(1)	No	No	Yes	Yes	No	No
Assigned Security Responsibility	164.308(a)(2)	No	No	No	No	No	No
Workforce Security	164.308(a)(3)	No	No	Yes	Yes	Yes	Yes
Information Access Management	164.308(a)(4)	No	Yes	Yes	Yes	Yes	Yes
Security Awareness and Training	164.308(a)(5)	Yes	Yes	Yes	Yes	Yes	Yes
Security Incident Procedures	164.308(a)(6)	No	No	No	No	No	No
Contingency Plans	164.308(a)(7)	No	No	Yes	No	No	No
Evaluation	164.308(a)(8)	Yes	Yes	No	No	No	No
Business Associate Contracts and Other Arrangements	164.308(b)(1)	No	No	No	Yes	No	No
Facility Access Controls	164.310(a)(1)	No	No	No	No	No	No
Workstation Use	164.310(b)	No	No	No	No	No	No
Workstation Security	164.310(c)	No	No	No	No	No	No
Device and Media Controls	164.310(d)(1)	No	No	No	No	No	No
Access Control	164.312(a)(1)	Yes	No	Yes	Yes	Yes	Yes
Audit Controls	164.312(b)	Yes	No	Yes	Yes	No	No
Integrity	164.312(c)(1)	No	No	No	Yes	No	No
Person or Entity Authentication	164.312(d)	No	Yes	Yes	Yes	Yes	Yes
Transmission Security	164.312(e)(1)	Yes	Yes	Yes	Yes	Yes	No
Business Associate Contracts or Other Arrangements	164.314(a)(1)	No	No	No	No	No	No
Requirements for Group Health Plans	164.314(b)(1)	No	No	No	No	No	No
Policies and Procedures	164.316(a)	No	No	No	No	No	No
Documentation	164.316(b)(1)	No	No	No	No	No	No

What is the Health Insurance Portability and Accountability Act (HIPAA)?

Enacted by the United States Congress in 1996, the Health Insurance Portability and Accountability Act (HIPAA) provides provisions to protect health insurance coverage for workers and their families when they change or lose their jobs, and require the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers. Along with HITECH and HITRUST, HIPAA has become a de facto standard for protecting the privacy and security of individually personally identifiable health information in the healthcare industry.

The Security Rule within HIPAA deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. Please see the requirements in HIPAA for a full explanation of these safeguards.

Challenges for IT Organizations in Meeting HIPAA Requirements

IT organizations face several challenges when working to prove their compliance with HIPAA.

Fines and penalties: Compliance is mandatory

With civil penalties ranging from $100 per incident to $1.5 million per year, the cost of violating provisions of HIPAA can be crippling to a healthcare organization.

Complexity, time, and resource constraints: HIPAA compliance can distract from core operations

Applying, maintaining, and proving administrative, physical, and technical safeguards against electronic protected health information can quickly become a significant resource drain on even the most well-resourced IT organizations. Therefore, solutions are needed to help IT organizations quickly prove and maintain compliance with the Security Rule.

Since these are fundamental technologies to achieving compliance, this technical brief explains how to map BeyondTrust privileged access management and vulnerability management solutions to HIPAA requirements to more easily demonstrate and maintain compliance.

Summary of HIPAA Safeguards

This section of the tech brief contains a table that summarizes the administrative, physical, and technical safeguards laid out in the HIPAA Security Rule needed to achieve compliance.

Table 2: HIPAA Safeguards

Standard	Specification
Administrative Safeguards Policies and procedures designed to clearly show how the entity will comply with the act	Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures. The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls. Procedures should clearly identify employees, or classes of employees, who will have access to electronic protected health information (EPHI). Access to EPHI must be restricted to only those employees who have a need for it to complete their job function. The procedures must address access authorization, establishment, modification, and termination. Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions. Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors, and to monitor whether appropriate contracts and controls are in place. A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures. Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based. Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or through the normal course of operations.

Standard	Specification
Physical Safeguards Controlling physical access to protect against inappropriate access to protected data	Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired, it must be disposed of properly to ensure that PHI is not compromised.) Access to equipment containing health information should be carefully controlled and monitored. Access to hardware and software must be limited to properly authorized individuals. Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts. Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public. If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.
Technical Safeguards Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.	Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional. Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner. Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity. Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems. Covered entities must make documentation of their HIPAA practices available to the government to determine compliance. In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing. Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the Act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

How BeyondTrust Solutions help with HIPAA Requirements

This section of the tech brief contains a detailed table that summarizes how BeyondTrust solutions map to HIPAA requirements to ensure compliance.

Table 3: Detailed Mapping of BeyondTrust Solutions to HIPAA Requirements

Note: Only relevant standards and implementation specifications to BeyondTrust solutions are included here.

HIPAA APPLICABILITY MATRIX		
HIPAA STANDARD DESCRIPTION	**IMPLEMENTATION SPECIFICATIONS ADDRESSED**	**COMMENT**
Security Management Process - § 164.308(a)(1): Implement policies and procedures to prevent, detect, contain, and correct security violations.	Information System Activity Review - § 164.308(a)(1)(ii)(D)	**PowerBroker for Unix & Linux** partially supports procedures to review information system activity of privileged users by auditing all privileged user activity and providing tools to search review and report against audit logs. § 164.308(a)(1)(ii)(D) **PowerBroker for Windows** partially supports procedures to review information system logged events via the Policy Monitor that is installed with PowerBroker for Windows. § 164.308(a)(1)(ii)(D)
Assigned Security Responsibility - § 164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity.	N/A	*No implementation specifications in this Standard are addressed by the BeyondTrust solution.*
Workforce Security - § 164.308(a)(3): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management standard], and to prevent those workforce members who do not have access under [the Information Access Management standard] from obtaining access to electronic protected health information.	Authorization and/or Supervision § 164.308(a)(3)(ii)(A)	**PowerBroker for Unix & Linux** partially supports procedures to ensure that privileged users have appropriate access rights to ePHI through fine-grained authorization access rights on Unix/Linux platforms, which restrict access based upon management's policies for granting access. § 164.308(a)(3)(ii)(A) **PowerBroker for Windows** partially supports procedures to ensure that privileged users have appropriate access rights to ePHI by providing the capability to define access rules for administrators, thus defining specific access rights as appropriate to their job responsibilities. § 164.308(a)(3)(ii)(A)

		In conjunction with procedures for assigning and administering workforce access rights, **PowerBroker Identity Services** supports implementation specification § 164.308(a)(3)(ii)(A) by allowing an organization to define access rights using discretionary or role-based methods. In conjunction with procedures for assigning and administering workforce access rights, **PowerBroker Password Safe** supports implementation specification § 164.308(a)(3)(ii)(A) by allowing an organization to assign and approve access to passwords stored in the password safe based upon job responsibilities of users.
Information Access Management - § 164.308(a)(4): Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part [the Privacy Rule].	Access Authorization - § 164.308(a)(4) (ii)(B) Access Establishment and Modification - § 164.308(a)(4)(ii)(C)	With policies and procedures for granting access, **Retina** can augment support technical specification §164.308(a)(4) (ii)(B) by scanning user lists to report administrative rights assignment that can be used to monitor that access rights are consistent with job responsibilities. **PowerBroker for Unix & Linux** partially supports procedures for authorizing access to electronic protected health information by: • controlling what commands a privileged user is authorized to perform § 164.308(a)(4)(ii)(B) • providing the capability to modify the privileged users in the PowerBroker master host policy. §164.308(a)(4)(ii)(C) In conjunction with policy and procedures**, PowerBroker for Windows** supports Information Access Management by: • defining specific rules to each administrator and defining what user rights the administrator is authorized to run § 164.308(a)(4)(ii)(B) • giving an organization ability to change user access rights and define specific rules for each user §164.308(a)(4)(ii)(C) In conjunction with policy and procedures, **PowerBroker Identify Services** supports Information Access Management by: • allowing an organization to define access using discretionary or role-based methods§ 164.308(a)(4)(ii)(B) • generating reports for access review and documenting modifications to access rights §164.308(a)(4)(ii)(C). **PowerBroker Password Safe** partially supports procedures for authorizing access to electronic protected health information by:

		• providing a password management system used to control access to shared accounts passwords by providing one-time use passwords to access shared accounts § 164.308(a)(4)(ii)(B) • providing the ability administer access to the password safe, including deleting and granting access to the passwords stored in the system needed to access privileged/shared accounts §164.308(a)(4)(ii)(C), while eliminating the need to change passwords for shared accounts should the user access list change
Security Awareness and Training - § 164.308(a)(5): Implement a security awareness and training program for all members of its workforce (including management).	Protection from Malicious Software §164.308(a)(5)(ii)(B), Password Management - §164.308(a)(5)(ii)(D) Log-in Monitoring § 164.308(a)(5)(ii)(C)	With procedures for monitoring antivirus and password settings configurations and status, **BeyondInsight** in conjunction with **Retina** supplements support of the implementation specifications with enhanced vulnerability reporting associated with the antivirus anti-virus status § 164.308(a)(5)(ii)(B) and password configuration settings § 164.308(a)(5)(ii)(D). While not an anti-malware tool, in conjunction with a workforce security awareness program and anti-malware tools, **PowerBroker for Unix & Linux** can augment support of technical specification § 164.308(a)(5)(ii)(B) by removing local admin/root privileges on workstations and replacing with access right limited to least privilege required for job will reduce the attack surface. In conjunction with procedures and anti-malware tools, **PowerBroker for Windows** augments support for implementation specification § 164.308(a)(5)(ii)(B) by allowing an organization to implement the principle of least privilege by removing local admin/root privileges. According to Microsoft, this practice reduces the Windows workstation attack surface available to malicious software by 92%.[1] **PowerBroker Identity Services** augments support for implementation *Standard* § 164.308(a)(5)(ii)(B) by logging authentication attempts. In conjunction with organization policies and procedures, **PowerBroker Password Safe**: • partially supports implementation specification § 164.308(a)(5)(ii)(B) by logging authentication attempts to the password safe

[1] http://technet.microsoft.com/en-us/library/bb456992.aspx

		• supports implementation specification § 164.308(a)(5)(ii)(D) by providing a password management tool for shared accounts that eliminates the need for all users to know a shared password in order to access a privileged or other shared account
Security Incident Procedures - § 164.308(a)(6): Implement policies and procedures to address security incidents.	N/A	*No implementation specifications in this Standard are addressed by the BeyondTrust solution.*
Contingency Plan - § 164.308(a)(7): Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Data Backup Plan § 164.308(a)(7)(ii)(A)	**PowerBroker for Unix & Linux** augments Data Backup Plan procedures with its capability to backup all audit trails produced by PowerBroker for Unix & Linux. § 164.308(a)(7)(ii)(A)
Evaluation - § 164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule].	Evaluation § 164.308(a)(8)	**BeyondInsight** supplements support of the implementation specification related to activities provided by **Retina**, with enhanced reporting and analysis of vulnerabilities identified in vulnerability scans § 164.308(a)(8).
Business Associate Contracts and Other Arrangements - § 164.308(b)(1): A covered entity, in accordance with § 164.306 [the Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) [the Organizational Requirements] that the business associate will appropriately safeguard the information (Emphasis added).	N/A	*No implementation specifications in this Standard are addressed by the BeyondTrust solution.*

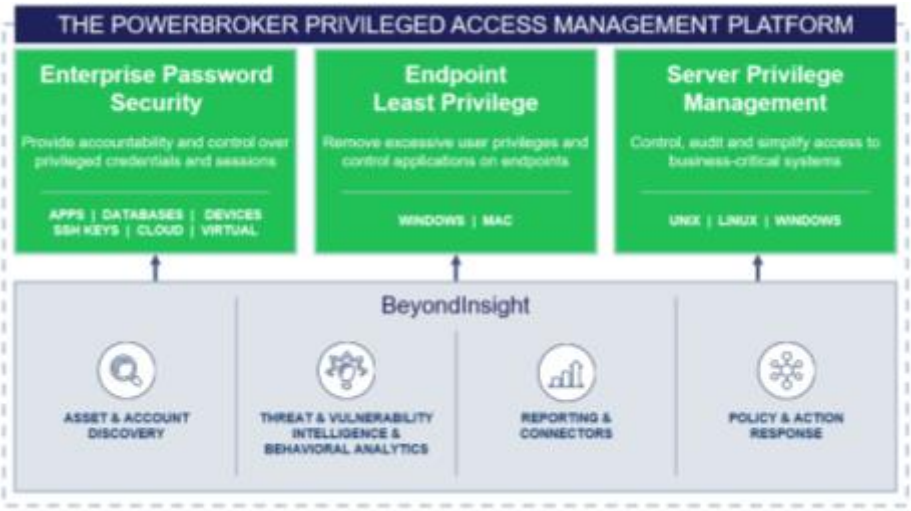
Access Control - § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) [Information Access Management].”	Unique User Identification § 164.312(a)(2)(i) Emergency Access Procedure § 164.312(a)(2)(ii) Automatic Logoff § 164.312(a)(2)(iii) Encryption and Decryption § 164.312(a)(2)(iv)	**BeyondInsight** augments support for Access Control procedure requirements by: • requiring the use of unique user IDs for accessing BeyondInsight reports and monitoring tools § 164.312(a)(2)(i) • providing enhanced reporting of information about security settings, including automatic logoff settings § 164.312(a)(2)(iii) **PowerBroker for Unix & Linux** augments support of the requirements defined in § 164.312(a)(2)(iv) by encrypting all PowerBroker related traffic, data, files, and log files. **PowerBroker for Windows/Mac** allows the creation of policy that controls the access rights of applications which access protected health information as defined in § 164.312(a)(i). **PowerBroker Identity Services** supports implementation specification § 164.312(a)(2)(i) by enforcing the use of unique user IDs in Windows Active Directory. **PowerBroker Password Safe**: • augments support for implementation specification § 164.312(a)(2)(ii) by providing the ability to assign individuals, authorized as emergency personnel, access rights to privileged account passwords for an emergency • supports implementation specification § 164.312(a)(2)(iii) by providing the ability to define a timeout procedure per target system and requiring a password to be entered prior to re-entry

Audit Controls - § 164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	This standard has no implementation specification.	**BeyondInsight** augments support for HIPAA safeguard § 164.312(b) by logging users' BeyondInsight activities including access to audit logs that might contain ePHI data. **PowerBroker for Unix & Linux** supports standard § 164.312(b) by auditing all privileged user activity and providing tools to search review, and report against audit logs. **PowerBroker for Windows** augments support for standard § 164.312(b) by auditing all privileged user activity and providing tools to search, review. and report against audit logs
Integrity - § 164.312(c)(1): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Mechanism to Authenticate Electronic Protected Health Information - § 164.312(c)(2)	**PowerBroker for Windows** augments support for implementation specification § 164.312(c)(2) by performing file integrity monitoring of directories and files on Windows systems.
Person or Entity Authentication - § 164.312(d): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	This safeguard has no implementation specification.	**Retina** directly supports safeguard § 164.312(d) by detecting network user accounts that do not have passwords. **PowerBroker for Unix & Linux** supports safeguard § 164.312(d) by having the ability to enable step-up authentication to verify that a person is who he/she was originally authenticates as by requiring them to enter their credentials again prior to performing a certain operation. **PowerBroker for Windows** supports safeguard § 164.312(d) by enabling step-up authentication to verify that a person is who he/she was originally authenticated as by requiring the user to enter their credentials again prior to performing a certain operation. **PowerBroker Identity Services** directly supports safeguard § 164.312(d) by supporting smart cards and also by enforcing the use of passwords. **PowerBroker Password Safe** directly supports safeguard § 164.312(d) by assigning dynamic passwords to each user requiring access to a privileged/shared account for an application – eliminating the need for multiple users to have access to a shared password.

Transmission Security - § 164.312(e)(1): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network	Encryption - § 164.312(e)(2)(ii)	**BeyondInsight** partially supports the transmission encryption requirements associated with § 164.312(e)(2)(ii) by providing the ability for encrypted transmissions with **Retina** and **PowerBroker** applications, thus audit records or other transmissions with ePHI data are encrypted. **PowerBroker for Unix & Linux** partially supports the encryption requirements associated with § 164.312(e)(2)(ii) by default encrypting all PowerBroker network related traffic thus encrypting any ePHI data in audit trails or other PowerBroker activity. **PowerBroker for Windows** partially supports the encryption requirements associated with § 164.312(e)(2)(ii) by default encrypting all PowerBroker network related traffic thus encrypting any ePHI data in audit trails or other PowerBroker activity. **PowerBroker Identity Services** partially supports the encryption requirements associated with § 164.312(e)(2)(ii) by default encrypting all PowerBroker network, thus encrypting any ePHI data in audit trails or other PowerBroker activity.

Appendix: The PowerBroker Privileged Access Management Platform

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



Product Capabilities within the PowerBroker Privileged Access Management Platform

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

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

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

Conclusion

By partnering with BeyondTrust, organizations can address their compliance and security requirements as defined in HIPAA, leaving fewer gaps, and improving efficiency over their privileged access management and vulnerability management practices.

About BeyondTrust

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

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

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