BeyondTrust

Privileged Remote Access
Data at Rest Encryption Whitepaper

TC:2/8/2019

Table of Contents

Introduction to Data at Rest Encryption with BeyondTrust Privileged Remote Access

Introduction

BeyondTrust Privileged Remote Access's (PRA) data at rest encryption allows organizations to use their existing key management solution to encrypt their BeyondTrust configuration, text-based session audit history, and session recordings for on-premises or cloud-based BeyondTrust PRA deployments. With BeyondTrust PRA's data at rest encryption feature, organizations can comply with data encryption policies put forth by your organization's Information Security team.

Prerequisites

- BeyondTrust Appliance[1] must be using BeyondTrust Base version 5.0 or above.
- The key management solution must support Key Management Interoperability Protocol (KMIP) version 1.0 or above.
- For cloud deployments, BeyondTrust PRA Cloud must be able to access the KMIP server over port 5696.
- A root Certification Authority (CA) certificate must be provided by the KMIP server.
- A client Transport Layer Security (TLS) certificate that defines the KMIP user account to be used for authentication, which must be provided by the KMIP server and uploaded to the BeyondTrust Appliance.

[1]BeyondTrust Appliance is used interchangeably to refer to both on-premises and cloud deployments.

Configure the BeyondTrust Privileged Remote Access Appliance to use Data at Rest Encryption

Technical Overview

With BeyondTrust Base 5.0, BeyondTrust administrators can now enable data at rest encryption. This includes block-level encryption using XTS-AES 128-bit encryption for the following content:

- **BeyondTrust configuration**
- **Text-based session audit history**
- **Session recordings**

BeyondTrust's data at rest encryption implementation uses KMIP to generate an encryption key for initial encryption of your content and requests the key when decrypting your content, as well.

KMIP Server Information and Testing

To configure data at rest encryption for your BeyondTrust Appliance, go to one of the following locations:

- For physical and virtual BeyondTrust Appliances, go to **/appliance > Storage > Encryption**.
- For BeyondTrust PRA Cloud, go to **/login > Appliance > Storage > Encryption**.

Then configure the following details noted below.

KMIP Server Hostname and Port

- **KMIP Server Hostname:** The hostname of your key management solution.
- **Port:** The port used to connect to the KMIP Server.

> ***Note:*** *BeyondTrust PRA Cloud instances are static to port 5696. However, for on-premises deployments, the port is configurable but defaults to port 5696.*

The KMIP server must be reachable from your BeyondTrust PRA site via Transmission Control Protocol (TCP) over the KMIP hostname and port. For on-premises deployments, the KMIP server can be on a local network or accessible via the internet. However, please ensure your firewall allows TCP connections over the specified KMIP TCP port from your BeyondTrust Appliance.

Server CA Certificate, Client TLS Certificate, Passphrase, Username, and Password

KMIP requires bi-directional authentication. The BeyondTrust PRA Appliance must trust the KMIP server from which it is requesting encryption keys, and the KMIP server must trust the BeyondTrust Appliance for which it is storing and granting encryption keys as an authorized service. To create this level of trust, the following information is needed:

- **Server CA Certificate:** The root CA certificate presented by the KMIP server to verify its authenticity to the BeyondTrust Appliance.
- **Client TLS Certificate:** The client TLS certificate with the KMIP user account defined for the KMIP server to verify the authenticity of the BeyondTrust Appliance.
- **Passphrase:** The passphrase needed by the BeyondTrust Appliance to open and read the client TLS certificate.

- **Username/ Password:** The username and password associated with the KMIP user account being used to verify the authenticity of the BeyondTrust Appliance. This is the same user account defined in the client TLS certificate.

The BeyondTrust Appliance authenticates the KMIP server through the root CA certificate, which is uploaded to BeyondTrust /appliance. KMIP requires two-factor authentication to verify authorized services, and in this scenario, the KMIP server uses the username and password for the KMIP user account and the client TLS certificate to authenticate the BeyondTrust Appliance.

When the **Save and Test Changes** button is selected, the BeyondTrust Appliance issues a KMIP command and waits for a response back from the KMIP server, ensuring communication is possible. If successful, the **Encrypt** button becomes available in BeyondTrust /appliance. If not successful, the **Encrypt** button remains whited out and unavailable, and you must recheck the KMIP details entered on /appliance to ensure the information is correct.

IMPORTANT!

The length of time needed to initially encrypt your BeyondTrust content depends on the amount of storage consumed by your BeyondTrust Appliance. For new deployments of BeyondTrust PRA, it is recommended to configure data at rest encryption before production use of your BeyondTrust Appliance. In the event your BeyondTrust Appliance is consuming 4GB of data or more, please contact BeyondTrust Technical Support at help.bomgar.com.

The Encryption Process

Once the KMIP server is configured successfully, you can click the **Encrypt** button. The BeyondTrust Appliance reaches out to the KMIP server and issues a command to create an encryption key, which is stored on the KMIP server with an associated secret ID. The encryption key and the associated ID are then provided to the BeyondTrust Appliance for initial encryption of the data, and the BeyondTrust Appliance starts backing up the session,. The data is then encrypted, and the backup is restored.

Note: *During encryption, the BeyondTrust Appliance stores the secret temporarily in its memory.*

At this point, the BeyondTrust Appliance stores the secret's associated ID - not the secret itself - in a decrypted portion of the BeyondTrust Appliance. In the event the BeyondTrust Appliance is rebooted, it makes a request to the KMIP server, asking for the secret associated ID. This allows the BeyondTrust Appliance to decrypt your data, while also ensuring the availability of your BeyondTrust site.

Note: *For more information on how to configure data at rest encryption, please see Encryption: Configure KMIP Server and Encrypt Session Data at www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/storage-encryption.*