BeyondTrust

Remote Support
Security in Cloud Whitepaper

TC:7/14/2020

Table of Contents

Security in BeyondTrust Remote Support (Cloud)

The purpose of this document is to help technically-oriented professionals understand the security-related value BeyondTrust can bring to your organization. BeyondTrust can help your support organization stay secure and compliant, while improving the efficiency and success of your organization with a better end-user support experience.

BeyondTrust Overview

BeyondTrust connects and protects people and technology with leading secure access solutions that strengthen security while increasing productivity. BeyondTrust Cloud gives support technicians secure remote control of computers over the internet. This specialized software provides exceptional performance, reliability, ease of use, and scalability through a solution that is optimized for remote support. With BeyondTrust, a support technician can see the supported screen and control the supported system remotely, as if physically present.

Using multiple features designed to ensure the security of remote support sessions, BeyondTrust integrates with external user directories, such as LDAP, for secure user management, and supports extensive auditing and recording of support sessions. Logging is performed on the BeyondTrust Cloud instance, which allows for the review of all customer and support representative interactions, including video playback of all desktop screen interactions. BeyondTrust also integrates with leading systems management and identity management solutions and includes an API for deeper integration. With BeyondTrust, support managers can create support teams, customize queues, and report on all support activity.

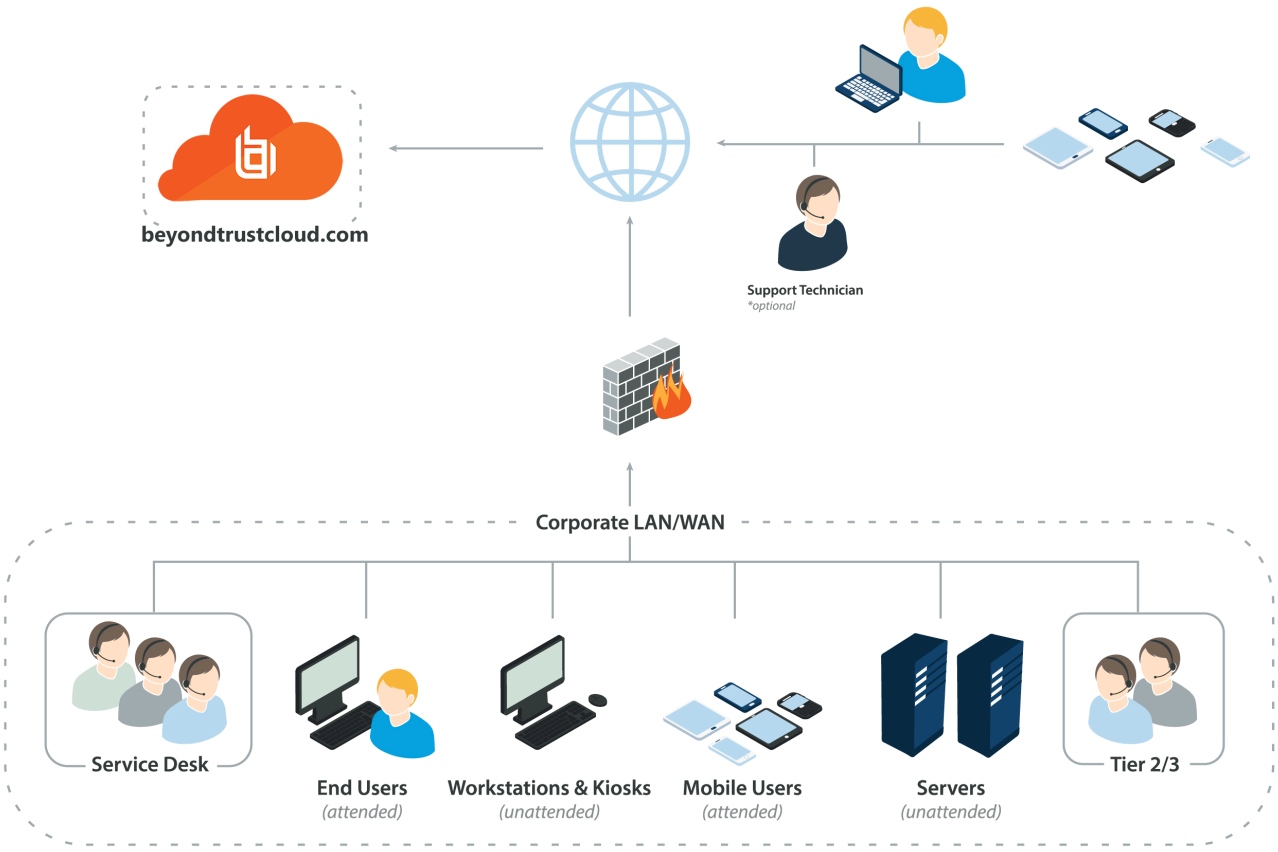
BeyondTrust enables remote access to multiple operating systems, including Windows, Mac, various Linux distributions, and mobile operating systems. BeyondTrust also enables remote control of various kinds of systems, including laptops, desktops, servers, kiosks, point-of-sale systems, smartphones, and network devices.

BeyondTrust allows support organizations to avoid less effective means of support by driving requests through custom support portals. BeyondTrust can match support requests with the appropriate technician or team. BeyondTrust then mediates connections between customers and support representatives, allowing chat sessions, file downloads/uploads, remote control of desktops, screen-sharing in either direction, running of presentations, and access to system information and diagnostics.

Architecture of BeyondTrust Remote Support (Cloud)

Infrastructure

The BeyondTrust Cloud infrastructure is currently spread across six Tier 3 or higher data centers. BeyondTrust customers can designate a regional data center to host their BeyondTrust solution so that performance is not hindered by geographic distance between users of the solution. All data centers leverage advanced electrical and cooling systems and N+1 redundancy with uninterruptable power solutions and generator backup. The data centers have advanced networking capabilities such as 10Gb+ connectivity and a 40Gb+ core network.



Compliance

Data centers hosting the BeyondTrust Cloud have achieved ISO/IEC 27001 certification of its information security management systems. Additionally all data centers have completed the following examinations:

- SOC II Type 1
- SSAE 16
    - SOC 1 Type II
    - SOC 2 Type II

They are also Privacy Shield certified to meet European Data Privacy compliance regulations.

Physical Security

All BeyondTrust Cloud servers are housed in data centers that employ a high standard of physical protection. The measures include multiple levels of physical security, such as:

- Man traps / air lock
- Badged access
- Securely locked cages
- Biometric access
- Securely isolated storage area
- 24/7 security personnel on duty

Network Security

The network architecture is built to protect all entry points assigned to customers. Highly-available edge gateways and segmented network components are dedicated and configured in BeyondTrust. The infrastructure is continuously monitored, and vulnerability testing is conducted regularly by internal security staff.

Customer Data

All customer data is confined to a dedicated instance of BeyondTrust allocated to your organization. The data physically and logically resides in a siloed BeyondTrust instance and is not shared between customers. This unique approach to the segregation of customers keeps your data safe.

Authentication to BeyondTrust Remote Support (Cloud)

BeyondTrust may be provisioned for locally defined BeyondTrust user accounts or can be integrated into existing authentication sources. For instance, a commonly integrated authentication source is Microsoft Active Directory. When using a directory such as this, all authentication follows the existing controls and processes in place for safeguarding user accounts.

Additional security providers are available that allow for representative authentication using Kerberos or SAML (for single sign-on) or using RADIUS (for multi-factor authentication). Each of these providers can be configured to use LDAP groups to set the permissions for the support representative, allowing you to map existing LDAP groups to support teams in BeyondTrust.

There are a large number of granular permissions that can be granted to support representatives. These permissions determine which features in BeyondTrust a representative has access to and can require end-user prompting so that the user receiving support must approve representative actions.

Credential Management in BeyondTrust Remote Support (Cloud)

BeyondTrust Remote Support can be integrated with an Endpoint Credential Manager (ECM) to improve password security for representatives, privileged users, and vendors.

An ECM functions as the middleware for communication, and the ECM can be used to integrate BeyondTrust Remote Support with third-party password vaults as well as with BeyondTrust Privileged Identity.

For more information about BeyondTrust Privileged Identity, former RED IM, please see BeyondTrust Privileged Identity at https://www.beyondtrust.com/docs/privileged-identity/index.htm.

***Note:** The ECM is not required when using the on-appliance credential store, BeyondTrust Vault.*

Credential injection is a built-in feature of BeyondTrust Remote Support. It allows administrators, representatives, and other privileged users to seamlessly inject credentials into systems without exposing plain text passwords, and this feature can also be used with third-party vault tools.

Credential Management with BeyondTrust Vault

BeyondTrust Vault is an on-appliance credential store, enabling discovery of and access to privileged credentials. You can manually add privileged credentials, or you can use the built-in discovery tool to scan and import Active Directory and local accounts into BeyondTrust Vault.

BeyondTrust Vault fits seamlessly with service desk workflow because it is integrated directly with the Remote Support solution. Technicians do not have to learn to use another tool or even exit BeyondTrust to retrieve passwords. With just one click in the BeyondTrust representative console, users can simply select the correct credential from the dropdown and log directly into a remote system - without ever having to know or even see the actual password.

Frequently Asked Questions about BeyondTrust Vault

What communication pathways are used with BeyondTrust Vault (ports, protocols, connection types, etc.)?

- **Active Directory and Discovery:**
  - By default, discovery occurs over LDAP via the Active Directory Service Interface (ADSI) on port 389.
  - If LDAPS is enabled, Active Directory queries run over LDAP under an SSL/TLS layer on port 636, unless another port is specified. This transport-layer security encrypts all data communicated to and from Active Directory.
- **Windows Local Discovery**
  - Local Windows accounts are discovered via a series of calls directly to Windows APIs.
  - These APIs use Remote Procedure Calls (RPCs) and named pipes as the network protocol.
  - The RPC process translates the request parameters as well as any response data into a standard, encoded format for transmission.
  - Protection is negotiated at the operating system level.

Where does encryption for BeyondTrust Vault occur?

- Passwords and private SSH keys are encrypted at rest using AES-256-GCM in addition to any full disk encryption enabled for the Secure Remote Access Appliance.
- Passwords and private SSH keys are encrypted in transit using an ephemeral public+private key pair when used for injection. This encryption occurs in addition to Remote Support's use of TLS to encrypt communication among all BeyondTrust components, such as the appliance, Jumpoint, customer client, etc.
- Passwords are encrypted in transit by TLS.
- Passwords used by Jumpoints to authenticate with Active Directory are never sent in plaintext to Active Directory.

Where is the Vault encryption key stored? Can it be accessed via /login or /appliance?

- The Vault encryption key is needed to decrypt credentials managed by BeyondTrust Vault. This key is stored on disk in your Secure Remote Access Appliance.
- The encryption key can be backed up by going to **/login > Management > Software Management > Backup Vault Encryption Key**. The backup file format used for the encryption key is the same .nsb file format used for configuration and reporting data.

Is the BeyondTrust application database encrypted, and if so, how?

- BeyondTrust Vault stores data in an encrypted format in the database. If full disk encryption is enabled for your Secure Remote Access Appliance, the BeyondTrust application database is also encrypted. However, this is independent of the encryption performed by BeyondTrust Vault.

What best practices are recommended to maintain the highest level of security across all points of connection (discovery, injections, support, etc)?

- BeyondTrust recommends using a valid CA-signed SSL certificate to protect communication among all BeyondTrust components.
- Jumpoints should run on a system only a few privileged users have permissions to access.

For more information about Jumpoints, please see Remote Support Jumpoint Guide: Unattended Access to Computers in a Network at https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.

***Note:** At this time, there are no user-visible security settings for BeyondTrust Vault.*

Encryption and Ports in BeyondTrust Remote Support (Cloud)

BeyondTrust can be configured such that it enforces the use of SSL for every connection made to the site. BeyondTrust requires that the SSL certificate being used to encrypt the transport is valid.

BeyondTrust can natively generate certificate signing requests. Configuration options also are available to disable the use of TLSv1 and/or TLSv1.1. BeyondTrust always has TLSv1.2 enabled to ensure proper operation of the software. Available cipher suites can be enabled or disabled and reordered as needed to meet the needs of your organization.

The BeyondTrust software itself is uniquely built for each customer. As part of the build, an encrypted license file is generated that contains the support portal Domain Name System (DNS) name and the SSL certificate, which is used by the respective BeyondTrust client to validate the connection that is made to the Cloud site.

The chart below highlights the required ports and the optional ports. Note that there is very minimal port exposure of the BeyondTrust Cloud infrastructure. This drastically reduces the potential exposed attack surface of the site.

Below are example firewall rules for use with BeyondTrust Cloud, including port numbers, descriptions, and required rules.

Firewall Rules	
Internal Network to the BeyondTrust Cloud Instance	
TCP Port 80 (optional)	Used to host the portal page without the user having to type HTTPS. The traffic can be automatically rolled over to port 443.
TCP Port 443 (required)	Used for all session traffic.
BeyondTrust Cloud Instance to the Internal Network	
TCP Port 25, 465, or 587 (optional)	Allows the appliance to send admin mail alerts. The port is set in SMTP configuration.
TCP Port 443 (optional)	Appliance to web services (e.g., HP Service Manager, BMC Remedy) for outbound events.

Auditing of BeyondTrust Remote Support (Cloud)

BeyondTrust provides two types of support session logging. All the events of an individual support session are logged as a text-based log. This log includes representatives involved, permissions granted by the customer, chat transcripts, system information, and any other actions taken by the BeyondTrust representative. This data is available on the appliance in an un-editable format for up to 90 days, but it can be moved to an external database using the BeyondTrust API or the BeyondTrust Integration Client. All support sessions are assigned a unique session ID referred to as an LSID. The session LSID is a 32-character string that is a unique GUID for each session. The LSID is stored as part of each session log for every session conducted.

BeyondTrust also allows enabling video session recordings. This records the visible user interface of the customer screen for the entire screen sharing session. The recording also contains metadata to identify who is in control of the mouse and keyboard at any given time during the playback of the recorded session. The period of time these recordings remain available depends on the amount of session activity and the available storage, up to 90 days maximum. As with the support session logging, these recordings can be moved to an external file store using the BeyondTrust API or the BeyondTrust Integration Client.

The BeyondTrust Integration Client can be used to export data from the site and store it if needed to comply with security policies. BeyondTrust can also be configured to store data for a shorter period of time to help comply with security policies.

The Integration Client (IC) is a Windows application that uses the BeyondTrust API to export session logs, recordings, and backups from the BeyondTrust Cloud site according to a defined periodic schedule. The IC uses plug-in modules to determine the repository for the exported data.

BeyondTrust provides two IC plug-in modules. One handles export of reports and video recordings to a file system destination. The second exports select report information (a subset of the entire data collection) to a Microsoft SQL Server database. Setup of the IC for SQL Server includes all of the procedures needed to automatically define the necessary database, tables, and fields.

In practice, the Integration Client is used to export support session data that must be retained for legal and compliance reasons. The reports and recordings are archived in a file system, indexed by session IDs. Data stored in the SQL Server tables may be queried to locate the BeyondTrust session ID corresponding to given search criteria such as date, representative, or IP address.

All authentication events, such as when a representative logs into the representative console or accesses the /login interface, generate a syslog event which can be logged on a syslog server. Additionally, any configuration change that is made to the BeyondTrust Cloud instance also generates a syslog event showing the change that was made and by which user.

Validation of BeyondTrust Remote Support (Cloud)

To ensure the security and value of our product, BeyondTrust incorporates vulnerability scanning in our software testing process. We track the results of vulnerability scans performed prior to a software release and prioritize resolution based on severity and criticality of any issues uncovered. Should a critical or high-risk vulnerability surface after a software release, a subsequent maintenance release addresses the vulnerability. Updated maintenance versions are distributed to our customers via the update manager interface within the BeyondTrust administrative interface. When necessary, BeyondTrust Support contacts customers directly, describing special procedures to follow to obtain an updated maintenance version. Additionally, BeyondTrust Cloud instances may be automatically updated based on the update interval chosen by the customer at the time of purchase.

In addition to internal scanning procedures, BeyondTrust contracts with third-parties for a source code level review as well as penetration testing. The source code review conducted essentially provides validation from a third party that coding best practices are followed and that proper controls are in place to protect against known vulnerabilities. A penetration test is conducted to confirm the findings.