BeyondTrust

Remote Support

The B Series Appliance and CJIS

TC:3/4/2024

Table of Contents

Overview

BeyondTrust Remote Support is a comprehensive remote support solution using a B Series Appliance-based architecture that can enable organizations to maintain and comply with Criminal Justice Information Services (CJIS) mandated policies. The BeyondTrust Appliance B Series gives support technicians secure remote control of computers over the Internet or over the entire agency local networks.

Maintain Compliance

With BeyondTrust Remote Support, a support technician can see the supported screen and control the supported system remotely as if physically present, all while maintaining compliance.

Support Systems

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

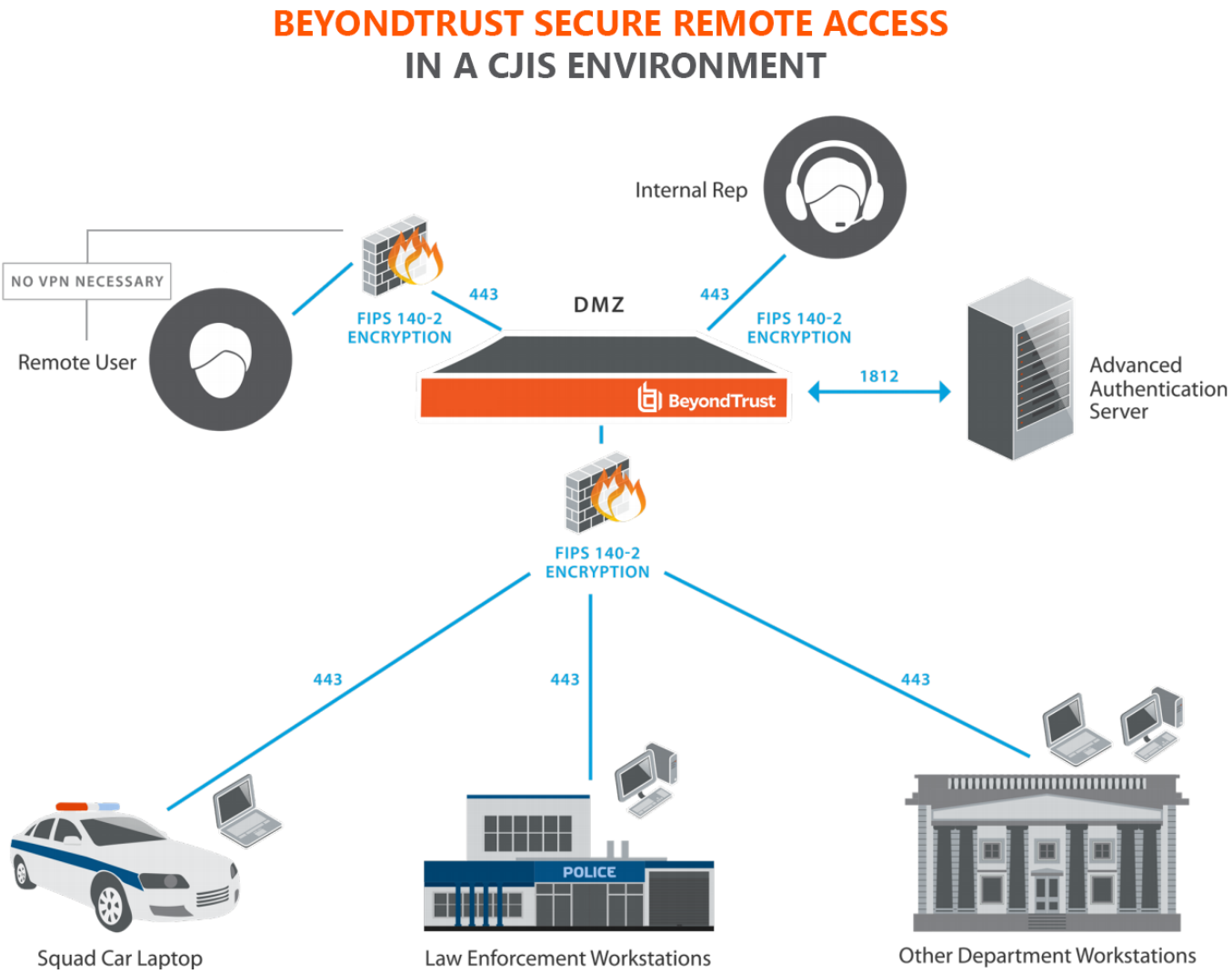
Access Anywhere

BeyondTrust Remote Support can work over internal and extended networks, or it can be Internet accessible. This allows support organizations to avoid less effective means of support by driving requests through customer support portals hosted on a hardened B Series Appliance. BeyondTrust can match support requests with the appropriate technician/support representative or team. BeyondTrust then mediates connections between customers and technicians, 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.

BeyondTrust Remote Support Architecture

Using multiple features designed to ensure the security of remote support sessions, BeyondTrust Remote Support integrates with existing advanced authentication identity management systems. This assists agencies in securing sensitive data by making sure that the technicians providing support have been validated properly. BeyondTrust Remote Support also adds a layer of additional auditing capabilities via detailed session logs and video recordings of every support session conducted. BeyondTrust Remote Support sessions are also encrypted in transmission using FIPS 140-2 compliant algorithms. The Rep Invite functionality can be carried out impromptu, removing the need to create a service account over a FIPS-compliant VPN. An invited outside rep is actively monitored and controlled by an internal agency technician for the duration of the support session.

The following diagram was taken from the CJIS security policy and depicts where BeyondTrust Remote Support would fit into a conceptual topology diagram for a law enforcement agency:



In the diagram above BeyondTrust Remote Support would be located in the agency's DMZ. BeyondTrust Remote Support uses the advanced authentication server to validate all technicians/reps. When supporting any end systems the session traffic is encrypted using FIPS-compliant encryption. BeyondTrust Remote Support can be used to securely support all agency systems that are internal as well as external to the agency network. Also depicted in the diagram is the BeyondTrust Remote Support Rep Invite feature. This BeyondTrust-specific functionality can also be extended to employees who need to access internal systems while working remotely, without requiring a VPN connection. This connection is also FIPS-compliant encrypted.

Authentication

BeyondTrust Remote Support may be provisioned for locally-defined BeyondTrust Remote Support user accounts, or can be integrated into existing authentication sources. For instance, a commonly integrated authentication source is RADIUS which enables agencies to leverage their existing advanced authentication server. 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 SAML, Kerberos, or LDAP. Each of these providers can be configured to use LDAP groups to set the permissions for the support technician, allowing you to map existing LDAP groups to support teams in BeyondTrust Remote Support.

There are a large number of granular permissions that can be granted to support technicians. These permissions determine what features in BeyondTrust Remote Support a technician has access to, and can require end-user prompting so that the user receiving support must approve the actions of the technician or support representative. Additionally, a technician can be allowed view-only support access if the organizationally preferred permission is restricted to that level.

SSL/TLS

BeyondTrust Remote Support can be configured such that it enforces the use of SSL for every connection made to the B Series Appliance. BeyondTrust Remote Support requires that the SSL certificate being used to encrypt the transport is valid, and also can be configured to ensure that only FIPS 140-2 compliant algorithms are used.

BeyondTrust Remote Support can natively generate CSR request using RSA 2048, 3072, or 4096 bit RSA key length choices or ECDSA keys using P-256 or P-384 curves, but also supports importing certificates generated off of the B Series Appliance. Available cipher suites can be enabled or disabled and re-ordered in the preferred preference of use. The BeyondTrust Remote Support software itself is also uniquely built for each customer and a unique encrypted license file is created that ensures all BeyondTrust Remote Support clients are only valid for the site in which they are built. Additionally, customer SSL certificates are built into the license file and must match the certificates being used on the B Series Appliance.

Auditing

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

BeyondTrust Remote Support also allows the ability to enable session recordings. This records the GUI of the customer screen for the entire support session. This recording 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 is dependent on the amount of session activity, and the available storage. As with the support session logging, these recordings can be moved to an external file store using the BeyondTrust Remote Support IC.

Each B Series Appliance model has differing amounts of available disk space, and by default is set to purge data over 90 days old. The BeyondTrust Remote Support IC can be used to export data from the B Series Appliance and store it externally if needed to comply with security policies.

The Integration Client is a Windows application used to export reports, recordings, and backups from one or more B Series Appliances according to a defined periodic schedule. The IC uses plug-in modules to determine the repository for the exported data. BeyondTrust Remote Support 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 the B Series Appliance and session ID. Data stored in the SQL Server tables may be queried to locate the BeyondTrust session ID corresponding to given search criteria such as date, service desk technician/representative, or IP address.

Validation

To ensure the security and value of our product, BeyondTrust Remote Support 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 version release addresses the vulnerability. Updated maintenance versions are distributed to our customers via the update manager interface within the BeyondTrust Remote Support administrative interface. Where necessary, BeyondTrust Technical Support will contact customers directly, describing special procedures to follow to obtain an updated maintenance version.

Currently BeyondTrust Remote Support conducts internal vulnerability assessments using IBM Rational App Scan.

BeyondTrust offers distinct products that have successfully undergone FIPS 140-2 Level 2 certification. In order to receive this certification the BeyondTrust Secure Remote Access software and the physical BeyondTrust Secure Remote Access hardware passed a very stringent review conducted by the National Institute of Standards and Technology.

- Current FIPS Certified Software Version: 16.2.1 FIPS
- Current FIPS Certified Firmware Version: 4.4.2 FIPS
- NIST Certification for the BeyondTrust Cryptographic Engine algorithms:

AES	Cert. #4767
CVL	Certs. #1411 and #1546
DRBG	Cert. #1648
ECDSA	Cert. #1196
HMAC	Cert. #3180
KTS	AES Cert. #4767 and HMAC Cert. #3180; key establishment methodology provides 128 or 256 bits of encryption strength
RSA	Cert. #2608
SHS	Cert. #3912

All B Series Appliances running Base software versions 5.3.0 – 5.5.0, including the RS Virtual Appliance and Cloud Appliance, make use of the same FIPS-validated version of the BeyondTrust Secure Remote Access Cryptographic Engine that is available in the FIPS-validated B Series Appliances. The BeyondTrust Secure Remote Access Cryptographic Engine also supports additional, non-FIPS validated algorithms in order to support a broader array of potential encryption requirements.

All of the encryption algorithms included with a B Series Appliance can be enabled or disabled at your discretion. For information about BeyondTrust Remote Support and FIPS, please see the appropriate BeyondTrust Remote Support FIPS Security Policy.