



Enterprise Remote Support

BeyondTrust

BeyondTrust Security Overview

BeyondTrust understands that encryption alone is not enough to secure remote support. Customers deploy the BeyondTrust appliance on-premises, behind their own firewall and security measures, and control physical access to the appliance, ensuring no unauthorized party gains access to sensitive data or systems.

BeyondTrust's unique appliance-based design ensures remote support security from beginning to end.

ARCHITECTURE

Centralized, Pre-Hardened Appliance

The BeyondTrust appliance is deployed within your own network, giving you complete, centralized control over all remote support activity. Data is routed and stored centrally over standard ports, enabling effective auditing. And keeping the BeyondTrust appliance in-house prevents third-party tampering, limiting your organization's circle of liability. BeyondTrust's architecture enables secure support of end-users both over the internet and within secure closed networks.

Strong Cryptography

In addition to using SSL data encryption, BeyondTrust is the only remote support provider to offer a solution that's been fully FIPS (Federal Information Processing Standards Publications) 140-2 Level 2 validated for both software and hardware elements.

Authentication

BeyondTrust seamlessly integrates with your existing identity management and authentication methods (e.g. LDAP, Active Directory, RADIUS, Kerberos), allowing users to login with secure directory credentials, as well as smart or CAC cards. BeyondTrust administrators can apply permissions and password policies on the group or individual level, ensuring only authorized users have access to your systems.

The BeyondTrust software itself is also uniquely built for each customer and a unique encrypted license file is created that ensures all BeyondTrust 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 BeyondTrust appliance.

AUDIT

Full Audit Trails & Video Recordings

BeyondTrust 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 technician or support representative. This data is available on the appliance in an un-editable format for 90 days, but can be moved to an external database using the BeyondTrust Integration Client (IC). All 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.



For all the benefits of this product and more visit RJRinnovations.com

