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.

BeyondTrust

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

Real-Time Management Oversight

With real-time monitoring and reports, problems can be dealt with as they occur. Administrators can join, take over, or terminate active sessions, transfer sessions between reps, and temporarily elevate a rep's privileges.

Third Party Validation

BeyondTrust routinely undergoes extensive internal scans and tests by McAfee, IBM, Nessus, and Qualisys, as well as a full product penetration assessment by Symantec. And crucial for government agencies, BeyondTrust is the only vendor to offer a remote support solution that is FIPS 140-2 Level 2 validated. The following diagram was taken from the CJIS (Criminal Justice Information Services) security policy in the USA and depicts where BeyondTrust would fit into a conceptual topology diagram for a law enforcement agency:

In the diagram beside, BeyondTrust would be located in the agency's DMZ. BeyondTrust 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 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 Rep Invite feature. This BeyondTrust-specific functionality is applied to a third-party vendor coming in via the Internet, without requiring a VPN connection. This connection is also FIPS-compliant encrypted.

The same concept can also be extended to employees who need to access internal systems while working remotely.

About BeyondTrust

BeyondTrust is the leader in enterprise remote support solutions for easily and securely supporting computing systems and mobile devices. The company's appliance-based products help organizations improve tech support efficiency and performance by enabling them to securely support nearly any device or system, anywhere in the world — including Windows, Mac, Linux, iOS, Android, BlackBerry and more. More than 8,500 organizations across 63 countries have deployed BeyondTrust to rapidly improve customer satisfaction while dramatically reducing costs.

BeyondTrust

We provide innovative, customized business process consulting, software implementation services and Level 1 bilingual support for multiple ITSM and DEM solutions and add-ons. We understand that in today's day and age, technology leaders are focused on transforming how IT operates. Digital transformation and automation are key elements in ensuring that most organizations keep up with how fast-paced both technology and information are consumed and delivered – at work and at home; on premise and in the cloud.