BeyondTrust

Privileged Remote Access Appliance Security Whitepaper

TC:5/14/2019

Table of Contents

Security in BeyondTrust Privileged Remote Access (On-Premises)

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 organization stay secure and compliant, while improving the efficiency and success of your organization with a better user experience.

BeyondTrust Overview

BeyondTrust connects and protects people and technology with leading secure access solutions that strengthen security while increasing productivity. BeyondTrust Privileged Remote Access lets you control access to critical systems without hindering the work privileged users need to perform. You can define how users connect, monitor sessions in real time, and record every session for a detailed audit trail.

BeyondTrust Privileged Remote Access integrates with external user directories, such as LDAP, for secure user management. BeyondTrust also integrates with leading systems management and identity management solutions and includes an API for deeper integration.

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.

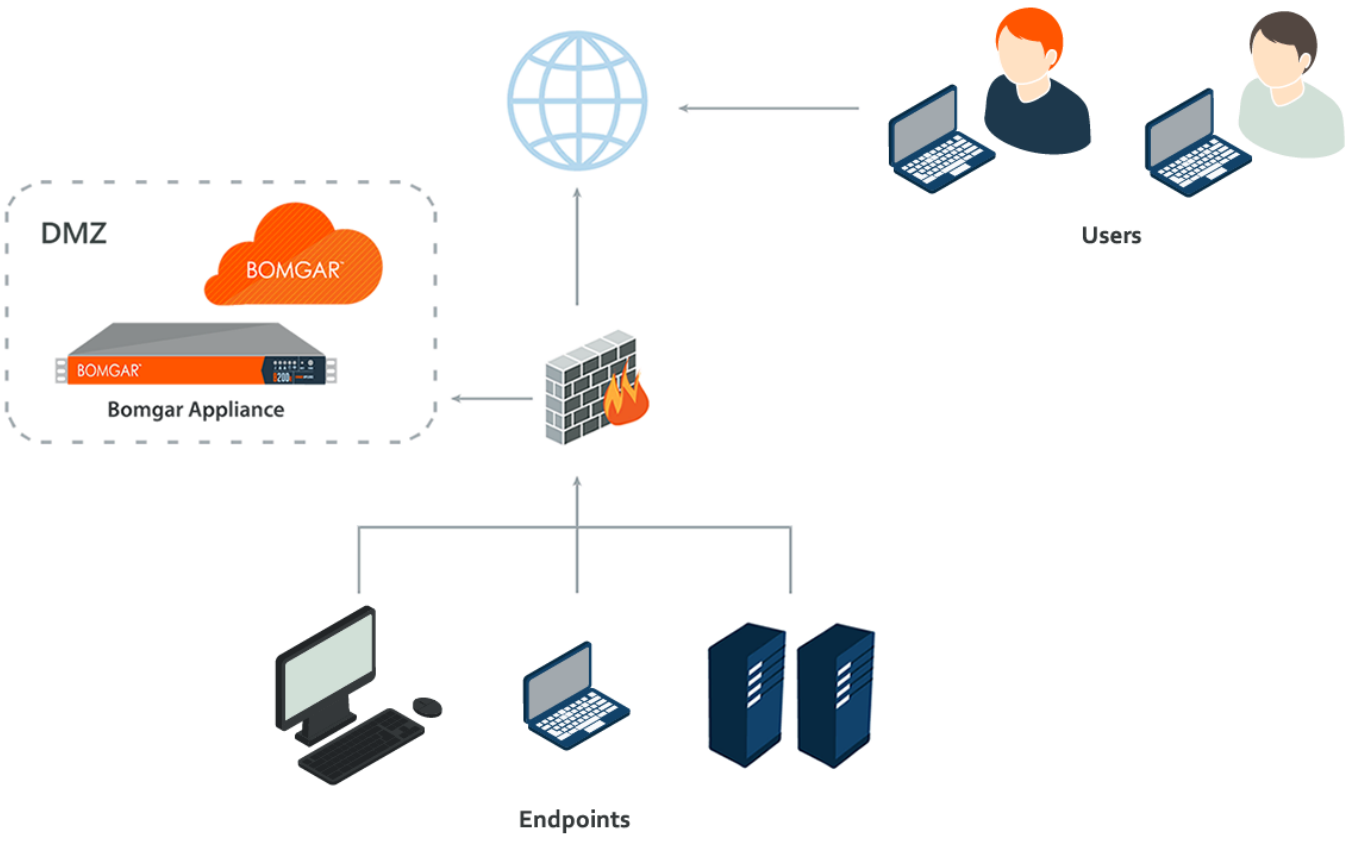
BeyondTrust can work over internal and extended networks, or it can be internet-accessible. BeyondTrust mediates connections between users and remote systems, allowing file downloads/uploads, remote control of desktops, and access to system information and diagnostics, the command line, and the registry editor.

Architecture of BeyondTrust Privileged Remote Access (On-Premises)

To make secure access possible, the BeyondTrust architecture places the BeyondTrust Appliance as the focal point of all communications. The appliance provides an interface using Hypertext Transfer Protocol (HTTP) for unauthenticated services, Secure HTTP (HTTPS) for authenticated services, and direct client connections accepted over a proprietary, BeyondTrust-defined protocol.

BeyondTrust has two primary binary components that provide the appliance's functionality. The first, called Base, is made up of the firmware that provides system-level configuration of a BeyondTrust Appliance. Settings such as IP addresses and security certificate configuration are all configured via the Base interface, which is accessed via the /appliance web interface.

The second component is made up of the software that provides site-level configuration and is accessed via the /login web interface. Behind the /login page is where user configuration and session options take place, and where the BeyondTrust access console, endpoint client, Jump Clients, Jumpoints, and security provider connection agents can be downloaded. Sessions always occur through the appliance, and since the connections are outbound from the clients to the appliance using well known ports, the application can communicate without local firewall changes.



Authentication to BeyondTrust Privileged Remote Access (On-Premises)

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 user 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 user, allowing you to map existing LDAP groups to teams in BeyondTrust.

There are a large number of granular permissions that can be granted to users. These permissions determine which features in BeyondTrust a user has access to.

Credential Management in BeyondTrust Privileged Remote Access (On-Premises)

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

An ECM functions as the middleware for communication, and the ECM can be used to integrate BeyondTrust Privileged Remote Access with password vaults.

Credential injection is a built-in feature of BeyondTrust Privileged Remote Access. It allows administrators and 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.

Encryption and Ports in BeyondTrust Privileged Remote Access (On-Premises)

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

BeyondTrust can natively generate certificate signing requests. It also supports importing certificates generated off the appliance. Configuration options also are available to disable the use of SSLv3, TLSv1, and/or TLSv1.1. BeyondTrust always has TLSv1.2 enabled to ensure proper operation of the appliance. 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 site 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 appliance.

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

Firewall Rules	
Internet to the DMZ	
TCP Port 443 (required)*	Used for all session traffic.
UDP Port 3478 (optional)	Used to enable Peer-to-Peer connections if the "Use Appliance as Peer-to-Peer Server" option is selected.
Internal Network to the DMZ	
TCP Port 161/UDP	Used for SNMP queries via IP configuration settings in the /appliance interface.
TCP Port 443 (required)*	Used for all session traffic.
DMZ to the Internet	
TCP Port 22 to the specific host **gwsupport.bomgar.com** (optional)	Default port used to establish connections with BeyondTrust Support for advanced troubleshooting/repairs. 443 may be used as an alternate port if needed.
TCP Port 443 to the specific host **update.bomgar.com** (optional)	You can optionally enable access from the appliance on port 443 to this host for automatic updates, or you can apply updates manually.
DMZ to the Internal Network	
UDP Port 123 (optional)	Access NTP server and sync the time.
LDAP - TCP/UDP 389 (optional)‡	Access LDAP server and authenticate users.
LDAP - TCP/UDP 636 (optional)‡	Access LDAP server and authenticate users via SSL.
Syslog - UDP 514 (required for logging)	Used to send syslog messages to a syslog server in the internal network. Alternatively, messages can be sent to a syslog server located within the DMZ.
DNS - UDP 53 (required if DNS server is outside the DMZ)	Access DNS server to verify that a DNS A record or CNAME record points to the appliance.
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 for outbound events.

Firewall Rules	
TCP Port 5832 (required if Passive Jump Client option is used)	Used as a listening port by Passive Jump Clients. Operating system firewalls should also be aware of this port. The port number is configurable by an administrator. This port is purely used for wakeup calls to the clients and is therefore not encrypted. After the client is woken, it launches the BeyondTrust session over an encrypted outbound TCP 443 connection.
TCP Port 5696	Allows the BeyondTrust PRA appliance to access the KMIP server located in the internal network for Data at Rest Encryption.

*Each of the following BeyondTrust components can be configured to connect on a port other than 443: access console, endpoint client, Jumpoint, connection agent.

‡ If the LDAP server is outside of the DMZ, the BeyondTrust Connection Agent is used to authenticate users via LDAP.

Auditing of BeyondTrust Privileged Remote Access (On-Premises)

BeyondTrust provides two types of session logging. All the events of an individual session are logged as a text-based log. This log includes users involved, session tools used, chat transcripts, system information, and any other actions taken by the BeyondTrust user. 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 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 endpoint 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 session logging, these recordings can be moved to an external file store using the BeyondTrust API or the BeyondTrust Integration Client.

Each BeyondTrust Appliance model has a certain amount of available disk space. If this space becomes filled, the oldest data is automatically deleted, even if the number of days set to keep logging data has not been reached. The BeyondTrust Integration Client can be used to export data off the appliance 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 one or more BeyondTrust Appliances 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 session data that must be retained for legal and compliance reasons. The reports and recordings are archived in a file system, indexed by the BeyondTrust Appliance and 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, user, or IP address.

All authentication events, such as when a user logs into the access console or accesses the /login or /appliance web interface, generate a syslog event which can be logged on a syslog server. Additionally, any configuration change that is made to the appliance also generates a syslog event showing the change that was made and by which user. If the syslog configuration itself is ever modified, it results in an administrative email sent by the appliance to the configured administrative email account for the appliance.

Validation of BeyondTrust Privileged Remote Access (On-Premises)

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.

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.