BeyondTrust Remote Support Version 20.1

New and Updated Features

BeyondTrust Remote Support empowers help desk teams to quickly and securely access and fix any remote device, on any platform, with a single solution. Organizations of all sizes can boost service desk productivity, efficiency, and security by consolidating and standardizing help desk support with BeyondTrust.

Remote Support version 20.1 introduces NEW market-leading features and enhanced capabilities to simplify workflows and enhance both the user and customer experience. NEW features like Chatbot integrations are available to serve as the hand off and automate customer support experience, allowing customers to be served immediately and free up agents for more complex issues and higher value work. In this release customers will also benefit from additional enhancements to our credentials Vault with improved security and additional functionalities. Please see the release notes for additional details on these important enhancements.

New Feature Highlights

NEW! Chatbot Integration

Bring your own Chatbot! Chatbots have been growing in popularity as more companies are looking for new ways that they can use these solutions as the first line of contact to help resolve more frequent issues before getting to a live agent. In this release we have created new API's to be used for handling inbound chat handoff and chat history from the bot. These new API's will allow for a handoff between the solutions so that end user experience is not a retelling of the same issue they went through with the bot and were sent to the person that can help them.

NEW! Linux Jumpoint

BeyondTrust Jump Technology enables privileged users to connect to an unattended remote system to start a session—without end-user assistance. Dependent upon the representative's permissions, the user may access any computer on their LAN/VPN or on a network with a Jump Point agent. In this release, we are introducing Jumpoint support for Linux installs. In the past our Jumpoint technology could only be deployed on Windows-based OS's. This requirement created problems for licensing by having to deploy a Windows-based operating system in more Linux-centric deployments.

NEW! Vault – Scheduled Rotation

The Remote Support Vault has been enhanced to include a simple and efficient method to rotate user-selected groups of credentials or all Vault credentials at one time, making it simpler for our customers to manage large numbers of credentials with Vault and removing time-consuming individual manual rotation.

NEW! TLS1.3 (Transportation Layer Security)

TLS provides secure communication between web browsers and servers. The connection itself is secure because symmetric cryptography is used to encrypt the data transmitted. The keys are uniquely generated for each connection and are based on a shared secret negotiated at the beginning of the session. TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. In this release, we have integrated the newest version of the encryption standards for TLS which is critical in today's environment.

NEW! Outbound Proxy Support

Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests. Proxy servers can provide a high level of privacy and security for the user's network. In this release, we have added the ability to use a proxy to send outbound events to single destination instead of needing to open communication to other applications directly. This feature allows admins to control the dataflow for the information they are sending off the appliance. This security function on the appliance is only for outbound events and API's in this release.

NEW! VAULT – Associate credentials to Endpoint

Customers need a better way for local account and specific account to only be associated to that endpoint. We have added the ability to now add a credential to a discovered endpoint. This feature allows for a better experience when selecting a system to Jump(TM) to and have the needed credential at the top of the list.

NEW! Mobile Device Management (MDM) for the Android Representative Console

The Android Representative Console has been improved for deployment through Mobile Device Management solutions, such as Microsoft Intune. The Remote Support site URL can be pre-configured when deployed through a MDM. Your Representatives no longer need to type the URL when access is required. In addition, the Remote Support site URL can be set as read-only so that your Representatives can only connect to your appliance.

NEW/ENHANCED! Chrome Browser sharing

We have added the ability to now allow for view-only screen sharing through click-to-chat sessions without a client download. This allows for greater support on the Chromebook but applies to all Chrome browser click-to-chat sessions giving better support experience and increased support. This feature helps with the transition of not needing to download a client for basic co-browse use cases.

Enhanced Feature Highlights

ENHANCED! SAML Options

By using SAML (Security Assertion Markup Language), an open standard for exchanging authentication and authorization data between parties, representatives can now log directly into /console from a SAML IdP. This is a customer requested feature and extends the usage of /console and Single Sign-on. Admins now have the ability to set what the behavior is for either launching the /login or the /console interfaces after using an IdP.

NEW Authentication Option for /Appliance

By using SAML (Security Assertion Markup Language), an open standard for exchanging authentication and authorization data between parties, representatives can now log directly into /appliance from a SAML IdP. Previously, we only had local authentication for /appliance. This enhancement gives users the ability to use non-local accounts to authenticate to the appliance interface to increase security and usability. Admins and Users don't have to remember or manage the local accounts so they can use more modern authentication methods.

ENHANCED! Reporting Permission by Jump Group

Jump groups contain specific endpoints a user or group can access, as well as the specific methods to access the endpoints with associated policies for those sessions. Jump Group Reporting enables users to view access sessions associated with this grouping by selecting it as a filter.

ENHANCED! Click-to-Chat

With the click of a button on the user's site, their customers can immediately connect with their IT or customer service team. This feature has been enhanced to achieve a more modern framework.

ENHANCED! Android Support Client

With this release the we have updated the Android Support Client to support full control on Samsung devices.

BeyondTrust Cloud Highlights

CLOUD! AWS Encryption key support

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules.