BeyondTrust Privileged Remote Access Version 20.2

New and Updated Features

New Feature Highlights

NEW! Vendor Onboarding

With this release, administrators can delegate the management of vendor and internal users to a trusted vendor administrator, or another internal user. Administrators will now be able to create a new Group Policy type in order to better onboard and manage vendor or other users. Once the PRA Admin defines the policy settings for the new Group Policy and assigns a Vendor Admin to that policy, the Vendor Admin can manage the onboarding and offboarding of managed users for the specified policy. Additionally, Notification and Approval workflows are available for the User onboarding process. This functionality is designed to decrease the manual administration requirements of Vendor management, as well as provide a quicker path to Access for new users.

NEW! Vault – Account Groups

Vault Administrators can now organize Vault Accounts into Account Groups, providing a better management experience for Vault Admins. Vault Admins can now assign Account Groups to Group Policies, rather than only individual Vault Accounts. Additionally, Vault Accounts can be assigned to an Account Group during the Import process.

NEW! Vault – Schedule Rotation

The Privileged Remote Access 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! Vault – Personal Accounts

With this release, all Privileged Remote Access users can utilize the Vault functionality in order to create private Generic Accounts in their own private Vault. This functionality improves the daily lives of users by allowing the user to manage their own Vault Accounts privately for use during Privileged Remote Access sessions.

NEW! Vault – Associate Credentials to Endpoint

Vault Accounts are now automatically associated with Endpoints, providing a better user experience when injecting credentials into Privileged Remote Access Sessions. This functionality requires Admins to use the Vault Discovery and Import functionalities in order to bring the Accounts and Endpoints under Vault management. Once under Vault management, the Credential to Endpoint association will occur automatically for the relevant Jump Items. Users will now be presented with these associated Vault Accounts when injecting during session initiation.

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. Linux Jumpoints support RDP and SSH sessions in this release.

NEW! Copy Jump Items

With this release, Jump Items can now be copied and can belong to multiple Jump Groups. This new functionality does include Jump Client items, providing administrators with the ability to set separate policies and group permissions without requiring an additional Jump Client installation on the target endpoint. Users with the appropriate permissions will now see the option to "Copy" Jump Items in the Access Console by right clicking the item. Users can perform this function on multiple Jump Items as well.

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.

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! Elevated Tool Access Granularity

This new setting allows the administrator to either Allow or Restrict Elevated Tool Access during Jump Client sessions. Elevated Tools include File Transfer, Command Shell, Registry Access and Power Controls. If this setting is disabled, access to elevated functionality will not be available for the session unless the logged in user has those explicit rights on the remote endpoint. This setting applies where allowed by the endpoint's platform.

ENHANCED! Configuration API

In this release, new Configuration APIs have been added to enable API use cases, including Jump Groups, Vendor Groups and Users, Group Policies, Vault Accounts, and Personal Vault Accounts.

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.