BeyondTrust Privileged Remote Access

Version 20.1

Market Launch – April 7, 2020

New and Updated Features

BeyondTrust Privileged Remote Access empowers IT teams to control, manage, and audit remote privileged access by authorized employees, contractors, and vendors, without compromising security. Enforce least privilege and exert granular control and visibility over remote access for both insiders and third parties, while enabling user productivity. Privileged Remote Access version 20.1 introduces NEW, market-leading features and enhanced capabilities to simplify workflows, improve security, and provide a better user experience with consolidated reporting. Please see the release notes for additional details on these important enhancements.

New Feature Highlights

NEW! macOS Catalina Support

The macOS Access Console fully supports macOS Catalina, the sixteenth major release of macOS, Apple's desktop operating system for Macintosh computers. With the release of Catalina, applications that perform screen sharing must be whitelisted by the user in macOS, be notarized by Apple, and follow additional new restrictions around access to certain file system paths like Desktop, Downloads, and Documents. Our new release includes security changes to meet the new security requirements of Catalina.

NEW! iOS 13 Support

With this release, the iOS Access Console now supports iOS 13, including support for new iPhone 11/11 Pro and iPad models.

NEW! Enhanced RDP Logging

This release has a new setting for RDP Jump Items that provides administrators with additional logging details for RDP Jump sessions. Users can leverage this new functionality by enabling the "Enhanced Logging" setting in the RDP Jump Item properties. This "Enhanced Logging" functionality will capture additional session events; for example, "Focused Window Changed Event" and "Mouse Click Event". This new functionality enhances security by providing administrators with RDP Jump session details that previously were only supported in Jump Client sessions.

NEW! Configuration APIs

This release has a new set of APIs that enable Privileged Remote Access administrators to automate and orchestrate administrative tasks within /login and the Access Console. There are specific methods exposed via an API that enable a programmatic way to create, list, update, and delete certain configuration items in Privileged Remote Access. For example, this enables Privileged Remote Access administrators to use the API to create local user accounts or delete Jump Clients that have been offline for a specified number of days.

NEW! Vault – Configurations APIs

It is now possible to list Vault accounts with the Vault Configuration API. Vault administrators can also create generic username/password and username/SSH key accounts using the API. This provides a programmatic way to onboard Vault accounts that can't be automatically discovered through Domain Discovery (Active Directory).

NEW! Vault – Bulk Rotation

Users and administrators can now select groups of Vault credentials and perform a password rotation on all credentials in the selected group, with just one click! This functionality provides administrators with a simple and efficient method to rotate user-selected groups of credentials or all Vault credentials at once, making it simpler for our customers to manage large numbers of credentials with Vault, while eliminating the need for time-consuming manual rotation of individual credentials.

NEW! BeyondInsight Integration – Reporting and Session Details

Our Privileged Remote Access customers have expressed their desire for further integrations with BeyondTrust products. With this release, administrators can leverage our BeyondInsight platform for session details and reports of Privileged Remote Access sessions. This integration includes a new Dashboard view for Privileged Remote Access sessions, which users can access in the BeyondInsight interface. Administrators who utilize our existing reporting functionality of /login can continue to view session details, reports, and session recordings in the /login interface.

Enhanced Feature Highlights

ENHANCED! Vault, Domain Filtering in Vault Discovery

Users can now traverse Organizational Units (OUs) within the targeted Active Directory Domain when using the Vault Discovery functionality. Vault Discovery allows administrators to discover credentials in the specified network. Administrators can then import credentials into Vault, enabling users to inject and use the discovered credentials within Privileged Remote Access sessions. Being able to traverse the OU's provides greater flexibility, while saving time and resources. Instead of running a general discovery to the domain, admins can specifically target the OU's of the teams and credentials that they wish to manage with Vault, decreasing the amount of managed credentials in Vault, and making it easier to use and control the most important credentials.

ENHANCED! Vault, New User Permissions

It is now possible to define which Vault users can inject credentials while in a session, and which Vault users can view credentials when checked out in /login. Previously, these permissions were grouped together, and we heard feedback that some customers wished to make this more granular.

ENHANCED! Jump Access – Cancel Access Request

Users can now cancel pending Jump Access authorization requests from the Web Console, giving users more flexibility and control over the authorization process, extending the existing functionality of the desktop Access Console.

ENHANCED! Access Console – Credential Store Limit Increase

With this release, the limit for displayed credentials in the Access Console has been increased from 250 to 2000, providing our customers with more flexibility and scalability in larger and more complex deployments.

ENHANCED! Session Reports – Additional Details

Session reports now contain details regarding the Access Approver Name,
Email Address, and Comments for sessions that require approval. Additionally, the session report now contains the Request Reason for sessions that require users to specify a reason for their access request.

ENHANCED! ECM- Error Messages

With this release, the Endpoint Credential Manager (ECM) will display an error message if the ECM is unable to retrieve the credential list from the configured password store. This makes it simpler for administrators to troubleshoot potential ECM configuration issues as well as communicate with the BeyondTrust Support team in order to resolve the issue. The error messages will be displayed in the Access Console if a user attempts to leverage the credential store and the ECM is unable to retrieve the relevant credential.

BeyondTrust Cloud Highlights

BeyondTrust Cloud URL

Bomgar Cloud is now BeyondTrust Cloud. New Cloud customers will now receive a beyondtrustcloud.com URL when they sign up for BeyondTrust Cloud. As before, Cloud customers can choose to use a custom DNS name for their site, if desired.