BeyondTrust

Password Safe Cloud 23.1
Security Whitepaper

TC:5/31/2023

Table of Contents

Security in BeyondTrust Password Safe Cloud

> ***Note:*** *Public. For Information Purposes Only.*

The purpose of this document is to help technically-oriented professionals understand the security-related value BeyondTrust can bring to their organization. BeyondTrust can help your support organization stay secure and compliant, while improving the efficiency and success of your organization with a better end-user support experience.

Password Safe Cloud Overview

BeyondTrust connects and protects people and technology with leading privileged access management solutions that strengthen security while increasing productivity. BeyondTrust Password Safe unifies privileged password and privileged session management, providing secure discovery, management, auditing, and monitoring for any privileged credential. Password Safe enables organizations to achieve complete control and accountability over privileged accounts. Password Safe Cloud is the same product as our on-prem (physical or virtual) and Infrastructure-as-a-Service (Azure, AWS, or GCP) counterparts, but is intended to reduce the maintenance burden of the deployment and ongoing maintenance of the solution. This Cloud deployment option of Password Safe provides nearly identical functionality through a solution that is optimized for being consumed in a Software-as-a-Service (SaaS) model. With Password Safe, an organization can reduce the risk of privileged credential misuse through automated password and session management.

Features and Capabilities

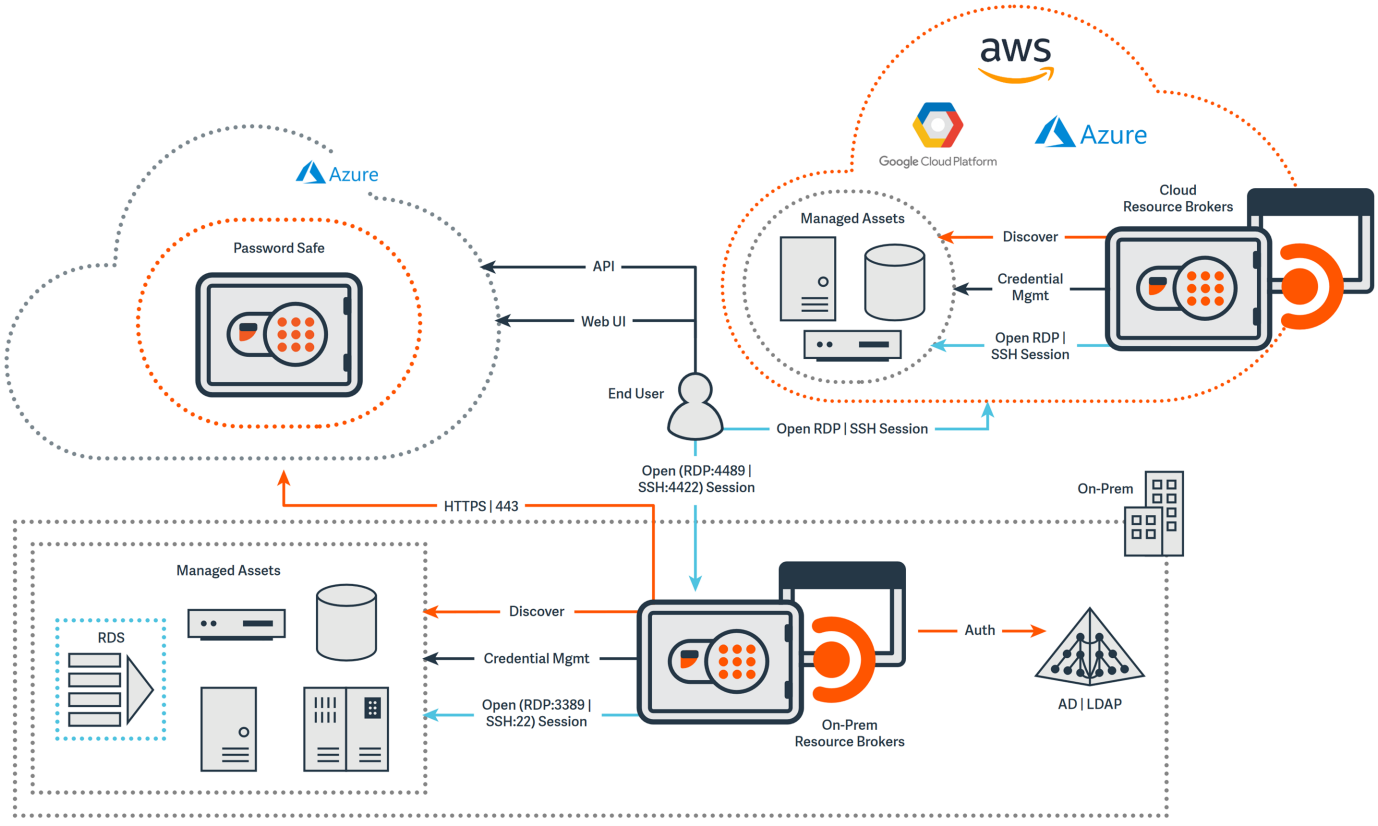
- **Continuous Automated Account Discovery and Auto-Onboarding:** Leverage a distributed network discovery engine to scan, identify, and profile all assets. Dynamic categorization allows auto-onboarding into Smart Groups for efficient management.
- **Secure SSH Key Management:** Automatically rotate SSH keys according to a defined schedule and enforce granular access control and workflow. Leverage private keys to securely log users onto Unix/Linux systems through the proxy, with no user exposure to the key, and with full privileged session recording.
- **Application-to-Application Password Management:** Eliminate hard-coded or embedded application credentials through an adaptable API interface that includes an unlimited number of Password Caches for scalability and redundancy.
- **Enhanced Privileged Session Management:** Live session management enables true dual control, enabling admins to record, lock, and document suspicious behavior without killing sessions – or productivity.
- **Adaptive Access Control:** Evaluate just-in-time context and simplify access requests by considering the day, date, time, and location when a user accesses resources to determine their authorization to access those systems.

Architecture of BeyondTrust Password Safe Cloud

Infrastructure

Password Safe Cloud is hosted within Microsoft Azure. A Password Safe Cloud deployment consists of:

1. Management Console
    - BeyondTrust Cloud hosted management console and Password Safe user portal
2. Resource Brokers
    - An on-prem agent deployed in the customers network facilitating the necessary local functions for password and session management
    - Authentication against your local AD/LDAP services
    - Asset and account discovery
    - Credential management
    - Session proxy



> *For more information, please see Azure infrastructure security at https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure.*

Compliance

Microsoft Azure data centers come with high levels of compliance standards which are fully documented and available to view.

The virtual machine images are hardened to the latest CIS benchmark. Nightly scans against the VM image check for compliance against the CIS benchmark.

> *For more information, please see Azure compliance documentation at https://docs.microsoft.com/en-gb/azure/compliance/.*

Physical Security

> *For more information, please see the "Physical Security" section of Azure facilities, premises, and physical security at https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security.*

Network Security

The network architecture is built to protect all entry points assigned to customers. Highly available edge gateways and segmented network components are dedicated and configured in BeyondTrust. The infrastructure is continuously monitored, and vulnerability testing is conducted regularly by internal security staff and third-party security teams.

Access to the Azure Management Console where the network/VNet configuration is managed is also highly restricted within BeyondTrust, available only to those who have a requirement to be able to access the console. This access is also subject to MFA.

All inbound traffic to a customer's Password Safe Cloud site uses standard encrypted HTTP on port 443. The on-prem Resource Broker also communicates with a Password Safe Cloud instance using 443, but additionally requires other specific traffic enabled, which is described in detail in the application's documentation.

Authentication

Authentication is managed entirely within the application. There is no dependency on cloud identity resources. Detail regarding application authentication can be found in the Password Safe Cloud administration guide.

Data Protection in BeyondTrust Password Safe Cloud

Data Isolation

All customer data is confined to a dedicated instance of BeyondTrust allocated to your organization. The data resides in a siloed BeyondTrust instance and is not shared between customers.

Disaster Recovery

The SQL Database uses SQL Server technology to create full backups every week, differential backups every 12 hours, and transaction log backups every five to ten minutes. The backups are stored in RA-GRS (read-access geo-redundant storage) blobs that are replicated to a paired data center for protection against a data center outage. When you restore a database, the service determines which full, differential, and transaction log backups need to be restored. The first full backup is scheduled immediately after a database is created. Each database has sufficient point in time restore coverage and long-term retention backup availability for comprehensive data restoration if required.

Recovery is available through Microsoft's Azure Management Portal and is subject to specific incident response times.

Encryption in Motion

All traffic to and from Password Safe Cloud is encrypted using TLS 1.2. Every site leverages a trusted TLS certificate for access to the web console. Older cryptographic protocols such as TLS 1.0/1.1, SSL 2.0, and SSL 3.0 are disabled.

Encryption at Rest

All data in Password Safe Cloud, except for session recordings, is stored in Azure SQL databases with transparent encryption enabled.

Session recording files are stored in Azure data storage resources allocated specifically to each customer. These files are encrypted using the standard application level encryption leveraging a customer's unique data encryption key.

For more information, please see Transparent data encryption for SQL Database, SQL Managed Instance, and Azure Synapse Analytics at https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal.

Access Management and Monitoring in BeyondTrust Password Safe Cloud

Access Management

Access to the Azure management console is only available to employees who require it to fulfill their assigned duties. Conditional access restrictions are used to manage access to the console, and all activity is audited.

Microsoft Azure

Azure Monitoring monitors the application, threshold, and event management through the alarming system for availability and troubleshooting. It applies to all the production applications, servers, core infrastructures systems components, OS, and network layer.

> *For more information, please see Azure Monitor overview at https://docs.microsoft.com/en-us/azure/azure-monitor/overview.*

Site24x7 Monitoring

Site24x7 is utilized for monitoring functionality of Password Safe Cloud instances. Each hosted instance is associated with Site24x7 automatically during the build process. Health checks are performed periodically to ensure each instance is operating correctly. Instances that fail two consecutive health checks are then marked as down and an alert is triggered. Alerts are in the form of both email and notifications on the Site24x7 portal. Multiple geographic locations are utilized to ensure global availability.

Application Logging

General application logging is generated for the purposes of monitoring and troubleshooting. These logs are centrally stored and available only to employees who require it to fulfill their assigned duties.

Security and Vulnerability

BeyondTrust uses a vulnerability management solution in our cloud environment(s). The solution scans at least every 24 hours and submits its findings back to the main console as well as to our SIEM. This includes IAM misconfigurations, authentication, lateral movement, data at risk, neglected assets, network misconfigurations, and vulnerabilities. All of the items listed above are alerted to the BeyondTrust InfoSec team, analyzed, and acted on based on validity and criticality.