BeyondTrust

Password Safe Cloud 23.3
Security Whitepaper

TC:12/12/2023

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-premesis (physical or virtual) and Infrastructure-as-a-Service (IaaS) counterparts, but is intended to reduce the maintenance burden of the deployment and ongoing maintenance of the solution. With Password Safe, an organization can reduce the risk of privileged credential misuse through automated password and session management.

Features and Capabilities

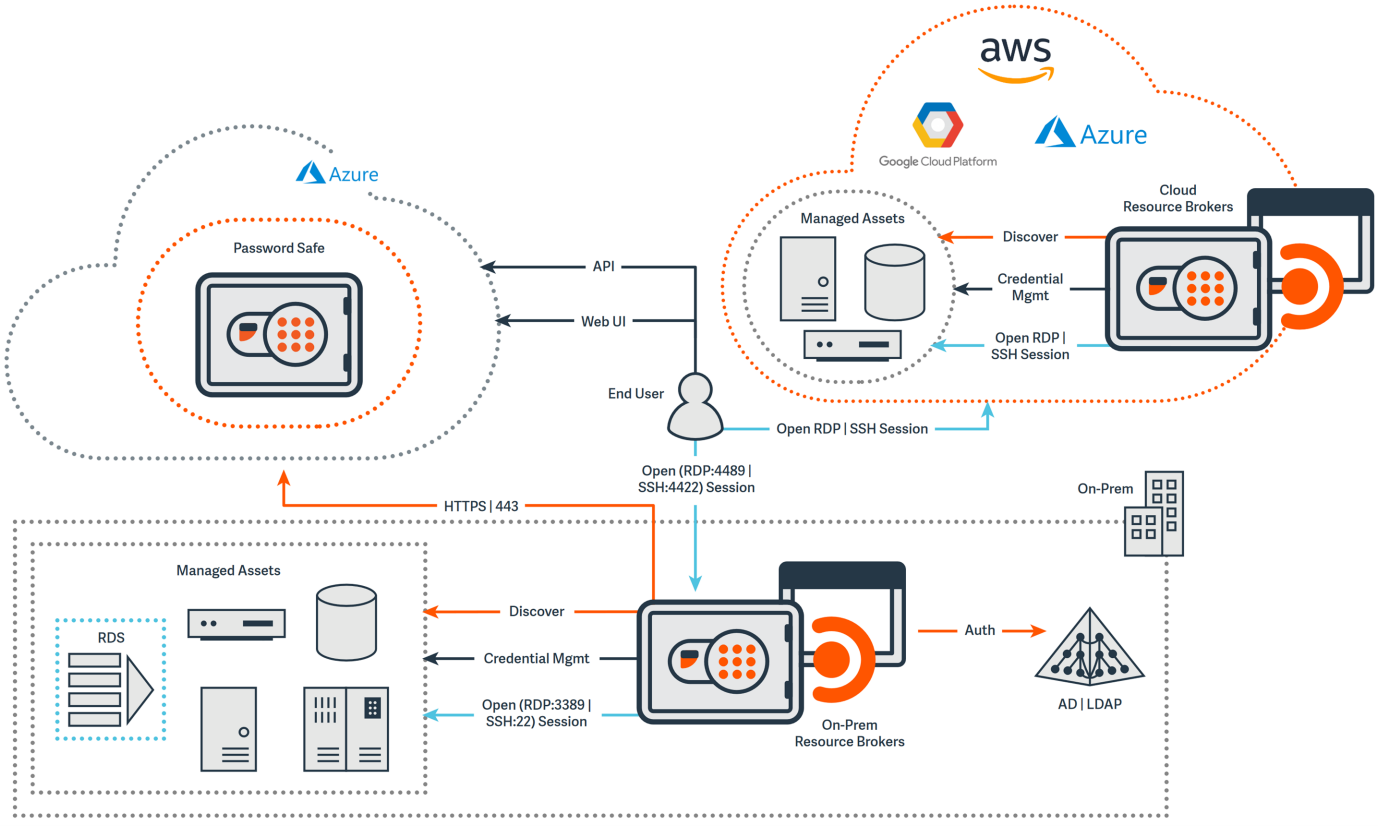
- **Continuous Automated Account Discovery and Auto-Onboarding:** Leverage a distributed network discovery engine to scan, identify, and profile all assets. Dynamic categorization allows auto-onboarding into Smart Groups for efficient management.
- **Secure SSH Key Management:** Automatically rotate 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.

Hosting Locations and Disaster Recovery

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

All customer data is confined to a dedicated instance of BeyondTrust allocated to their organization. The data resides in a siloed BeyondTrust instance and is not shared between customers. Customers can choose their primary instance deployment location based on their geographic location and preference; US-based customer data always remains in the United States. For non-US based customers, a list of sub-processors used to deliver the services can be referenced in Schedule 3 of BeyondTrust's Data Processing Agreement (DPA). From a hosting perspective within Microsoft Azure, Password Safe Cloud can be deployed to the following Azure Regions:

- Australia East
- Canada Central
- Central US
- Japan East
- Northern Europe
- Germany West Central
- Southeast Asia
- Central India
- UK South

> *For more information, please see BeyondTrust Corporation's Data Processing Agreement at https://www.beyondtrust.com/dpa.*

Microsoft Azure Failover Locations

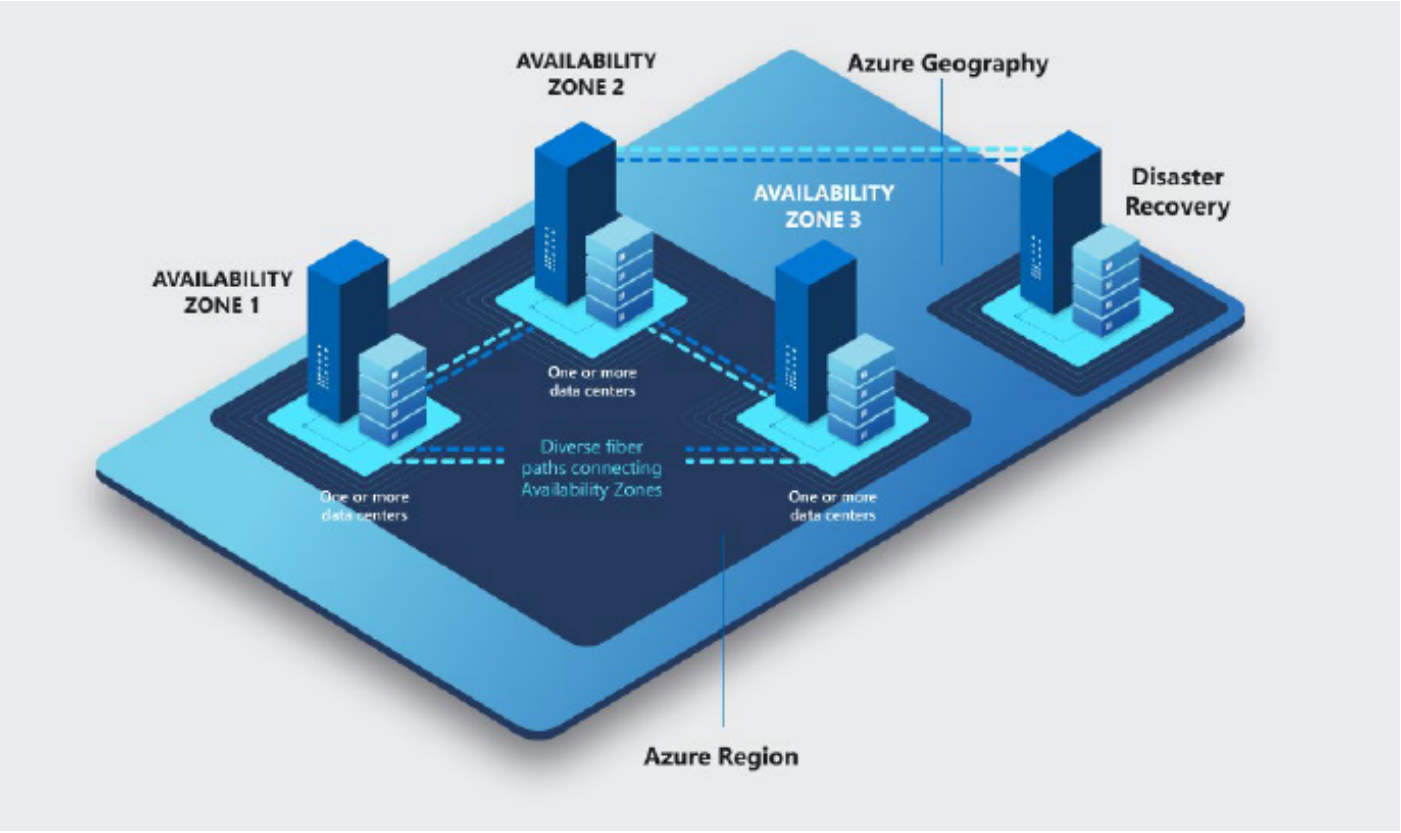
Based on geographic location, the following are the Azure regional paired data centers available among the hosting locations provided by BeyondTrust:

Primary Region	Failover Region
Australia East	Australia Southeast
Canada Central	Canada East
Central US	East US 2
Japan East	Japan West
Northern Europe (Ireland)	West Europe (Netherlands)
Germany West Central (Frankfurt)	Germany North (Berlin)
Southeast Asia (Singapore)	East Asia (Hong Kong)
Central India	South India
UK South	UK West

Microsoft Azure Regions and Availability Zones

Each Azure region contains approximately three availability zones to provide customers with redundancy within the cloud and to support disaster recovery functions. All locations are geographically dispersed to account for environmental issues that could impact the hosting

locations. The following image depicts an Azure Region and how it works with the supporting Availability Zones:



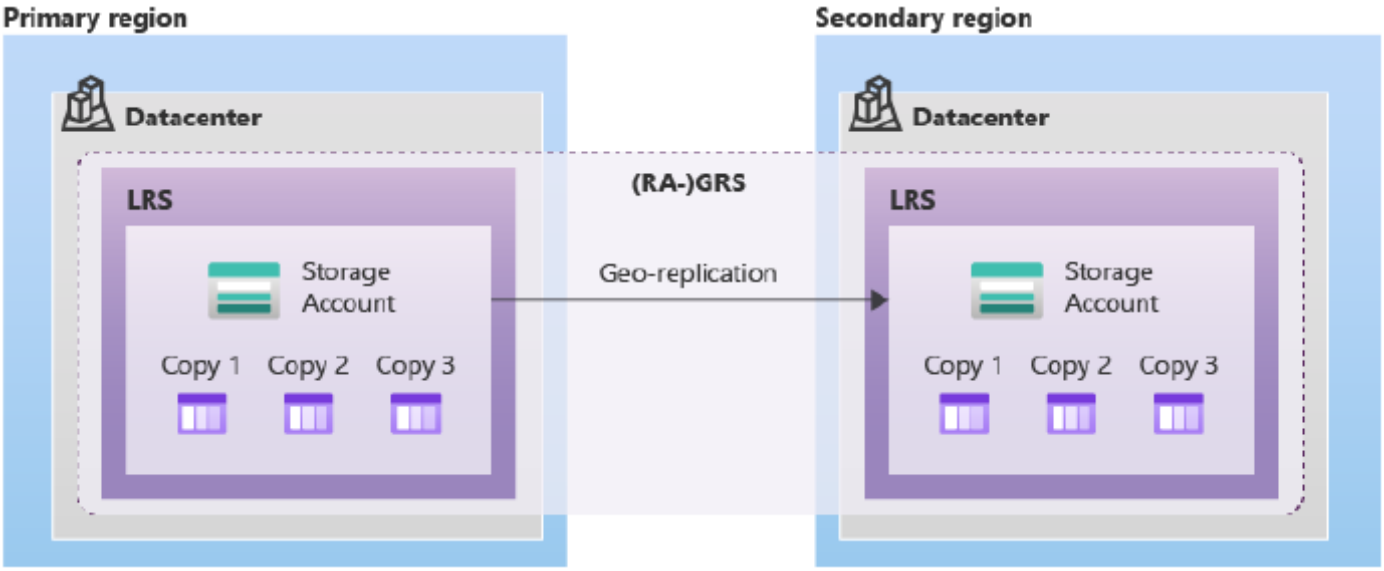
Password Safe Cloud utilizes SQL databases and SQL servers, which serve as the primary storage for all aspects of the solution within the cloud environment. When the instance is created by BeyondTrust Support, backups are automatically scheduled and performed for transactional logs (every 5 to 10 minutes), differential backups (every 12 hours), and full backups (every week) to the SQL server. These backups are then stored in a read-access geo-redundant (RA-GRS) storage blob that is replicated to a paired data center within an availability zone within the customer's chosen Azure region. This aides in ensuring that the cloud instance has appropriate mechanisms in place for availability in the event of a data center outage.

When a database restoration is required, the service (Microsoft Azure) 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.

> *For more information, please see Azure Regions at https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies/#geographies.*

What is Geo-Redundant Storage?

Geo-redundant storage copies data synchronously three times within a single physical location in the primary region using *Locally Redundant Storage*. It then copies data asynchronously to a single physical location in a secondary region that is hundreds of miles away from the primary region. The image below depicts a representation of this process:



Data in the secondary region is not directly accessible to users or applications (read access), unless a failover occurs. The failover process updates the DNS entry provided by Azure Storage so that the secondary endpoint becomes the new primary endpoint for your storage account. During the failover process, your data is inaccessible. After the failover is complete, you can read and write data to the new primary region.

> *For more information, please see Microsoft Azure Resources at https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#geo-redundant-storage.*

BeyondTrust Disaster Recovery Testing & Procedures

Formal Business Continuity (BC) and Disaster Recovery (DR) plans have been implemented for the corporate and cloud environment as well as other defined categories related to personnel shortages and environmental disasters. This plan is aligned to ISO 22301, certified, and audited under ISO 27001 and SOC 2 Type II, reviewed by management, tested annually, and approved by BeyondTrust's GRC Committee.

Scenarios have been developed to ensure that our teams have considered various threats and situations when attempting to restore services within the cloud. Such scenarios include the team creating a single tenant instance and intentionally rendering the service inoperable. This allows for various methodologies to be tested, such as redeploying an instance and/or implementing the last known good backup within the service. All DR testing performed by BeyondTrust is conducted through virtualization to avoid impacting our customer's daily operations and the service.

Another component of the DR testing is from Microsoft Azure's perspective. Microsoft Azure is responsible for performing entire availability zone and Azure region restoration and migration. This information is independently validated as part of Microsoft's Compliance Program and reviewed by BeyondTrust as information becomes available. A copy of the hosting provider's SOC 2 Type II report and other compliance related documentation can be retrieved from the Compliance Program linked below.

It is important to note that BeyondTrust cloud operations only carries out the DR functionality in the event of a true failure. Our organization does not perform DR procedures to account for accidental deletions or errors related to customer data.

> *For more information, please see Microsoft's Compliance Program at https://learn.microsoft.com/en-us/compliance/regulatory/offering-home?view=o365-worldwide.*

Recovery Time, Recovery Point Objectives, and Cloud Uptime

BeyondTrust's Security Requirements states in *Section 12.1.2* of *Business Continuity Management* that our organization is required to update and test the BCP annually at a minimum and is also required to mitigate significant changes to information security risk. With that, recovery time and recovery point objectives are situation specific and will vary depending on the nature of the incident.

The *Cloud Service Guide* states in *Section 4. Availability Service Level, subsection (4)* that BeyondTrust's availability SLA for the service shall be 99.9% during a calendar month. From an historical standpoint (Q1 2022 to present), BeyondTrust has exceeded this SLA uptime averaging (99.997%) but is unable to commit to anything higher to due to these values reflecting the contractual commitments between BeyondTrust and Microsoft Azure.

> *For more information, please see:*
>
> - *BeyondTrust's Security Requirements at https://www.beyondtrust.com/security-requirements*
> - *Cloud Service Guide at https://www.beyondtrust.com/cloud-service-level*

BeyondTrust Customer Support & Cloud Access Procedures

Note: *Public. For Information Purposes Only.*

Customer success and satisfaction are the primary goals of BeyondTrust. We are committed to providing world-class products and exceptional technical support services to our customers. Our mission is to deliver consistent, timely, and professional support that meets the needs of customers of all sizes on a global scale.

Our support staff have formal operating procedures and a detailed customer support guide that can be referenced for determining support windows and identifying various levels of severity.

Support Availability:

- Severity 1 - 24 hours a day, 365 days a year
- Severity 2 and 3 - Sunday, 7pm US Central Time – Friday, 7pm US Central Time

Severity Levels:

- **Severity Level 1**: Encompasses any issue where a production system is down or inoperable, or critical business operations are halted. Issue cannot be resolved by a restart or bypass.
    - Target initial response time: 30 minutes
- **Severity Level 2**: Encompasses any issue where there is mild to medium impact to user experience or product usability.
    - Target initial response time: 8 hours (excluding major holidays and weekends)
- **Severity Level 3**: Encompasses general support related inquiries, cosmetic impairment, or issues with minimal impact.
    - Target initial response time: 24 hours (excluding major holidays and weekends)

BeyondTrust does not access the cloud environment unless the customer creates a support case and gives us consent and authorization. After consent is obtained it triggers an internal approval process where a limited number of InfoSec or cloud operations employees can access the environment. When accessing the cloud, we use our Privileged Remote Access (PRA) solution to perform all activities within the cloud so that it can go through our corporate SSO/MFA and be logged, monitored, and audited. Technical controls have been implemented within this solution to mitigate the potential of data exfiltration by disabling the use of copy and paste functions, screen shots, downloading, etc., to ensure that our staff do not inadvertently store customer data onto their endpoint during a support session.

OS-level access to cloud instances or clusters requires the use of PRA. The site leverages IT-maintained MFA authentication and has granular permissions set to only allow access to approved accounts. A limited number of authorized customer support, cloud operations, and engineering employees can be granted access in this way. A record of all sessions is kept at least 90 days. The endpoint types can include Shell Jump, Jump Clients, Remote RDP, and Web Jump to ensure access can be audited.

A limited number of authorized customer support, cloud operations, and engineering employees can be granted access to the back end of customer instances. Authorized users are provisioned client certificates to enable this access. A support incident is required to access a customer instance, though exceptions to this can occur in the event of Severity Level 1 incidents.

Access is revoked when an employee is terminated or their role within the company changes to one not requiring access to customer data following a joiners, movers, and leavers process.

For more information, please see the Customer Support Guide at https://assets.beyondtrust.com/assets/documents/BT_Customer-Support-Guide-2023.pdf.

BeyondTrust's Security & Compliance Program

BeyondTrust has established and continues to maintain a thorough information security program with the aim of ensuring the protection of sensitive data through multiple layers of defense. The program aims to safeguard systems and customer information from internal and external security threats, as well as prevent unauthorized disclosure of this information. This document aims to detail the various controls, methodologies, and guidelines implemented by BeyondTrust to secure customer information.

Robust control measures are implemented to aid our organization to meet the requirements outlined within ISO/IEC 27001 and ISO/IEC 27701, which are standards for managing information security and data protection. BeyondTrust holds certifications under these standards and the services environment undergoes a SOC 2 Type II audit which can be shared under an NDA.

For more information, please see the BeyondTrust Security Certifications at https://www.beyondtrust.com/security/industry-certifications.

Data Protection in BeyondTrust Password Safe Cloud

Data Elements

The data elements present within Password Safe include entity type (Asset, Database, Directory, or Cloud), platform, system name, domain, DNS, IP address, access policies, password policies, username, name, email address, and role (if applicable).

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.