BeyondTrust

Privilege Management Cloud 22.9 Security Whitepaper

TC:11/23/2022

Table of Contents

Privilege Management Cloud Security

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.

BeyondTrust Overview

BeyondTrust helps organizations meet security and compliance needs while easing operational burdens through a more productive workforce through its Endpoint Privilege Management solutions.

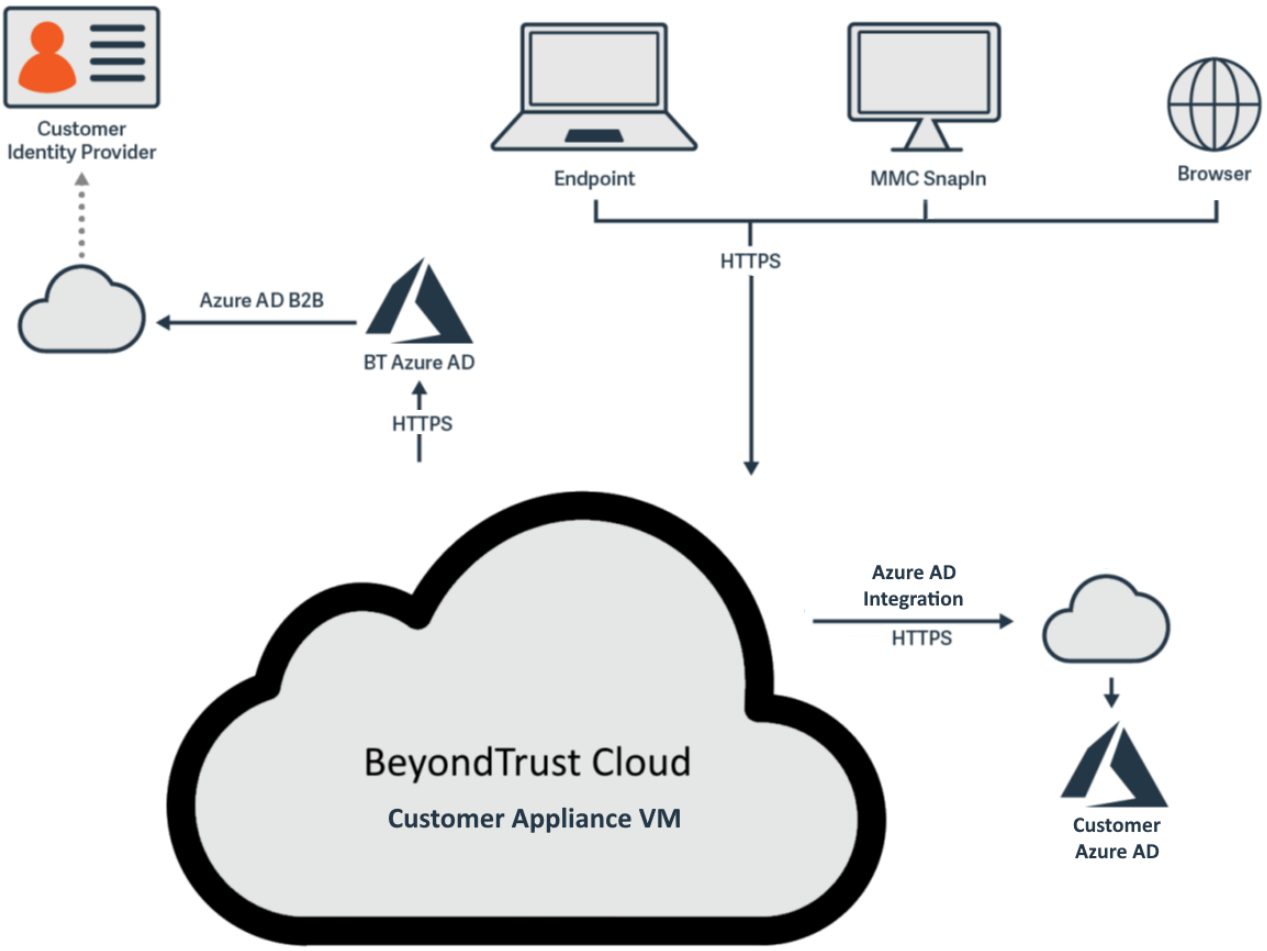
To determine the effect of endpoint privilege management solutions in the fight against cyber attacks, consider the underlying security principle of least privilege. Having local administrator rights means a user has privileges to perform most, if not all, functions within an operating system on a computer. These privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates, creating user accounts, and changing their passwords. While many organizations assign local admin rights to ease the need for IT Support, they are leaving themselves at high risk of a security breach. A common approach to managing privileged user accounts, the least privilege model is the practice of assigning users and programs the least amount of permission required to complete specific tasks.

The least privileged approach was conceived over 40 years ago and remains the fundamental security measure for organizations looking to mitigate the growing number of malicious attacks. This is primarily achieved by removing local admin rights from users. Least privilege works most effectively when combined with the concept of application allowlisting. Allowlisting is the practice of specifying an index of approved software applications that are permitted to be present and active on a computer system. The goal of allowlisting is to protect computers and networks from potentially harmful applications. An efficient solution sets a handful of broad rules based on trusted application types, automatically stopping unapproved applications from running. The integration of these two approaches is where endpoint privilege management comes into force. Methods of achieving least privilege have evolved somewhat since the concept's inception, as users look for ways to implement best practices, and make deployment easier than ever and deliver rapid time-to-value. As such, it is now possible to take significant steps towards a least privilege environment via software-as-a-service (SaaS) based solutions, which delivers all of the above benefits from the cloud as a subscription model.

Architecture of Privilege Management Cloud

Infrastructure

Summary of Privilege Management Cloud architecture, as hosted within Microsoft Azure data centers.



Physical Security

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

Network Security

All Privilege Management Cloud instances are running within an Azure virtual network (VNet) with firewall rules applied at the VNet level. No direct database access is available from outside the instance, with internal access locked down to allow connections only from the cluster subnet, which includes the Jump Client used for support purposes. Port 22 is open to support for shell jump access (restricted to a single BeyondTrust IP address).

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.

Customer Data

All customer data is confined to a dedicated instance of Privilege Management Cloud allocated to your organization. The data physically and logically resides in a single tenant instance and is not shared between customers.

Hosting Locations and Disaster Recovery

Azure hosting locations include:

- East US
- Central US
- West US
- Canada Central
- UK South
- Germany West Central
- North Europe
- South Africa North
- Central India
- South East Asia (Singapore)
- East Japan
- Australia East

SQL Database uses SQL Server technology to create full backups every week, differential backups every 12 hours, and transaction log backups every 5 to 10 minutes. The backups are stored in RA-GRS (read-access geo-redundant storage) blobs that are replicated to a paired datacenter for protection against a datacenter 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.

Individual Cloud Instance Backups

Azure SQL

- Computer Management Database
- Policy Database
- Reporting Database

Each database has sufficient point in time restore coverage and long-term retention backup availability for comprehensive data restoration if required.

Azure Key Vault

- Utilizes regional redundancy
- Employs Soft Delete of encryption keys and passwords

Recovery

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

Authentication to Privilege Management Cloud

Authentication for Privilege Management Cloud is achieved through Azure B2B, which allows end users in an Azure AD instance to be authenticated into the platform. Customers, therefore, require their users to be in an Azure AD instance; users authenticate through existing corporate means, including any MFA configured within their Azure AD. Customers retain control of password policy and BeyondTrust has no visibility of any end user credentials. The initial user for login will be invited during the fulfillment process, so the first admin email address is required before deployment.

For customers without Azure AD, the recommended approach is for customers to federate their current IDP with Azure AD to enable authentication by this method.

There are a number of granular permissions that can be granted to users of Privilege Management Cloud. These permissions determine which features a user has access to.

BeyondTrust does not have any access to login to the customers' web management console.

Encryption and Ports

Privilege Management Cloud is configured such that it enforces the use of SSL over port 443 for every connection made to the site.

The Azure firewall is configured to only allow 443 connections and Port 22 for shell jump access (restricted to a single BeyondTrust IP address).

Encryption in motion

All traffic to and from Privilege Management Cloud is encrypted using TLS 1.2. By default, the site leverages the provided wildcard certificate corresponding to the host name in use.

Older ciphers such as TLS 1.0 / 1.1 and SSL 2.0, and SSL 3.0 are disabled.

Encryption at rest

All data in Privilege Management Cloud is stored in Azure SQL databases with transparent encryption enabled.

> *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.*

Data Summary

The Privilege Management Cloud management platform consists of three databases.

Management Database

The management database is responsible for storing information about the endpoints connected to the Privilege Management Cloud management console, which includes information such as:

- Host name
- Primary User (this is the registered owner during OS install and is typically a company name or blank)
- Operating System and version
- Last connected (to management console) date
- Policy version applied
- Endpoint software version

We do not store information such as IP address or any associated user names with the endpoint.

Policy Database

The Policy Database is responsible for storing the created policy xml files which are send down to the endpoints. The policy .XML file contains the rules which will be applied on the endpoint by the Privilege Management client.

Reporting Database

The reporting database contains audit event data which is generated based on the policy .XML file applied on the endpoint. Audit event data is tied to the user name of the user that performed an action, such as running an application, which requires elevated rights. Reporting data is held for 90 days before being automatically purged. Typical information recorded includes:

- Description
- Publisher
- File name / location
- File hash
- File owner
- User name (of event operation)
- Host name (where event operation took place)
- Authorizing user name (if present)
- User reason (if given)

Access Management

Microsoft Azure

Access to the Azure management console is only available to employees who require it to fulfill their assigned duties. MFA is also used as part of access to the console, and all activity is audited.

Access to Customer Instances

OS level access to Privilege Management Cloud instances or clusters requires the use of Privileged Remote Access (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 support, cloud operations, and engineering employees may be granted access in this way. A record of all sessions is kept at least 90 days. The endpoint types may include Shell Jump, Jump Clients, Remote RDP, and Web Jump to ensure access can be audited.

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

Access is revoked anytime 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.

Application, Security, and Vulnerability Monitoring

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 Privilege Management 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.

ELK (Elasticsearch) Logging

Application level logs are sent to an ELK instance maintained by the cloud operations team within the Azure infrastructure. The purpose of the ELK system is to collect application level logs to aid in troubleshooting by the support teams. Logs are retained for up to 30 days and then overwritten. No customer data is stored as part of application level logging.

Security & Vulnerability Monitoring

BeyondTrust uses an agentless vulnerability management solution to provide full visibility across BeyondTrust's cloud accounts and all resources within. The solution utilizes a side-scanning technique that ingests itself into the snapshot process, assesses the snapshot for security threats, and provides contextual data and alerting based on criticality. The solution alerts both in the native console and into the BeyondTrust SIEM for quick review and action.

The BeyondTrust SIEM also receives security logging from Azure Security center. This includes Ingress authentication logging to track who is accessing what and when from a user perspective, threat analytics to alert us to any questionable software being installed and third-party access detection to notify us if a bad actor is trying to access our environment.

All of the items listed above are alerted to the BeyondTrust InfoSec team, analyzed and actioned based on validity and criticality.