BeyondTrust

Endpoint Privilege Management 24.2 Security Whitepaper

TC:4/24/2024

Table of Contents

Endpoint Privilege Management Security

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

The purpose of this document is to illustrate to technically-oriented professionals how BeyondTrust can bolster the security of their organization while simultaneously improving efficiency and end-user support.

BeyondTrust Overview

BeyondTrust helps organizations maintain a secure and compliant environment, leading to increased success and improved user experience. BeyondTrust provides a series of solutions to help organizations meet their security and compliance needs, while reducing operational burdens and enabling a more productive workforce.

EPM Overview

The EPM is an invaluable asset for organizations looking to centralize their endpoint privilege management. With this platform, they are able to control all of their computers from one convenient location, ensuring all computers are up-to-date and secure.

Technical Challenge and Least Privilege

To determine the effectiveness of endpoint privilege management solutions in the fight against cyber attacks, one must first consider the underlying security principle of least privilege. By having local administrator rights, a user has the privileges to perform most, if not all, functions within an operating system on a computer. These privileges can range from installing software and hardware drivers, changing system settings, installing system updates, creating user accounts, and changing their passwords. While having these privileges makes life easier for IT Support, the organization is at a much higher risk of breach.

The least-privilege approach is a common method of managing privileged user accounts, by assigning users and programs only the minimum amount of permission necessary to complete specific tasks. This approach was developed over 40 years ago and is still the fundamental security measure for organizations wanting to reduce the number of malicious attacks. Least privilege works best when combined with the concept of allowlisting, which is when an index of approved software applications are specified to be present and active on a computer system.

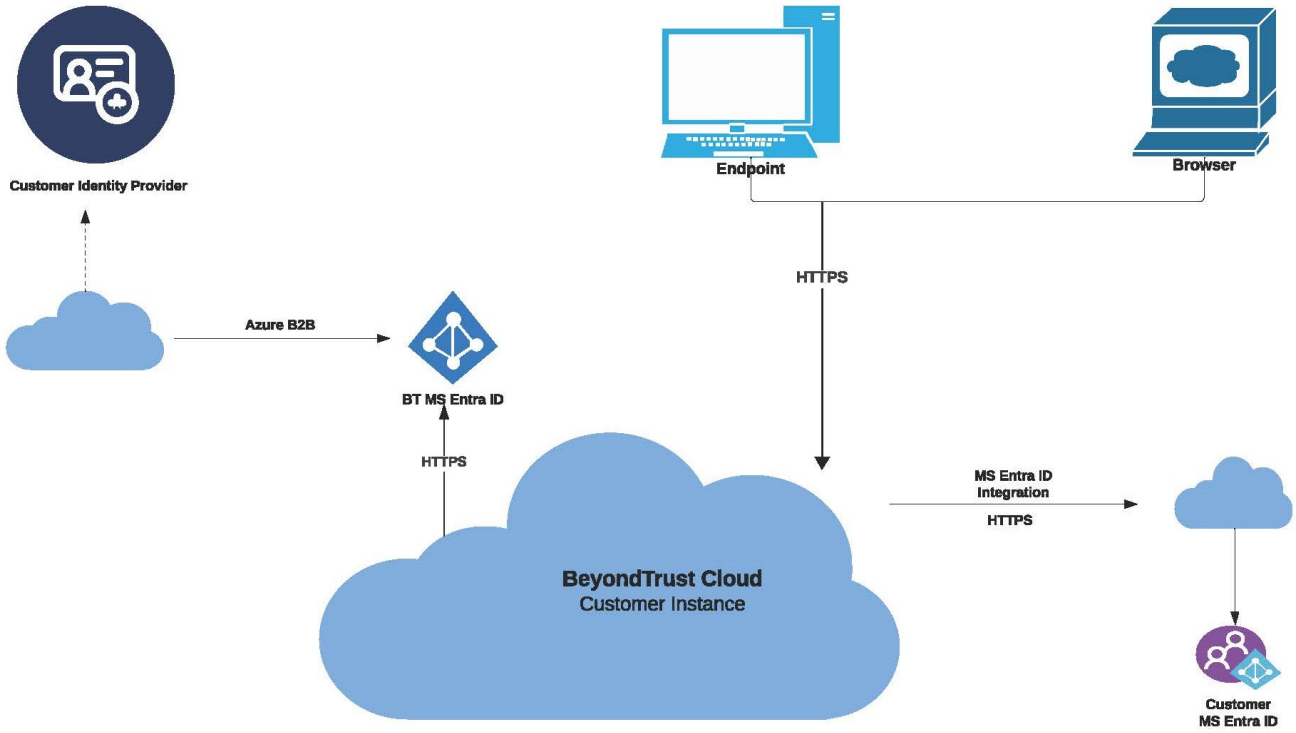
The integration of least privilege and allowlisting is the basis of endpoint privilege management. Over the years, methods for achieving least privilege have evolved. Now, organizations can easily and quickly use SaaS-based solutions to deploy least privilege.

EPM Architecture

Infrastructure

EPM leverages Azure Cloud Services (IaaS and PaaS) to host all its services within Microsoft Azure data centers.

The diagram provides a high-level overview of the Endpoint Privilege Management architecture hosted within Microsoft Azure data centers.



EPM configuration and secret information are securely stored in the Azure Key Vault and Azure storage account. Each customer environment has its own dedicated container within the storage account, with public access strictly blocked and only secure transfer allowed for REST API operations. Data encryption is enabled in the storage account, making use of Microsoft-managed keys, while Managed Identity is used to access the contents of the storage account. All secrets in the Azure Key Vault remain encrypted for enhanced security.

Infrastructure and Physical Security

Information about Azure infrastructure, physical security, and other important details can be found at Microsoft Azure Infrastructure Security. All client deployments are separate from each other, meaning that no client can access another client's infrastructure and services. Clients do not have access to the infrastructure, however, BeyondTrust's Support Team and Cloud Ops can do so if they require it for troubleshooting and production support purposes.

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

Data Security and Encryption

Encryption

Data physically and logically resides in a single tenant instance and is not shared between customers. Data at rest is further protected by Transparent Data Encryption (TDE) enabled by a service-managed key, because Azure automatically generates and manages the necessary keys for encryption. Key rotations are managed seamlessly in the background.

All secrets stored in your Key Vault are encrypted. Key Vault uses a hierarchical encryption scheme to ensure that your secrets are encrypted at rest. Upon adding a secret to the vault, the Azure Key Vault service automatically encrypts it and decrypts it for you upon retrieval.

Azure Storage ensures your data is securely encrypted while it is in our data centers with Microsoft-managed keys. When you access the data, it is automatically decrypted for you. Additionally, soft-delete and purge protection are enabled for the Key Vault to provide even more protection.

Personal Information

EPM stores personal information in the database, which is limited to email address and endpoint details (machine name, host name). Using Transparent Data Encryption (TDE), the data stored in the database is both secure and encrypted.

Blob Storage

In each deployment region we support, we use shared blob storage to store EPM policies and artifacts installed by Package Manager. EPM components running on the endpoints connect directly to these storage accounts to access and download the necessary files.

BeyondTrust follows Azure's recommended security best practices for securing data in blob storage.

BeyondTrust access controls, in addition to multi-factor authentication (MFA), guarantee that only authorized personnel have permission to interact with the storage infrastructure. Files are securely copied from BeyondTrust's repository management solution, verified, and placed into blog storage.

Database Security

All customer data is securely housed within a dedicated instance of EPM allocated exclusively to an organization. The data is classified as physically and logically segregated within a single tenant instance and is never shared with other customers. Additionally, TDE is enabled to ensure maximum security for the data while at rest. BeyondTrust personnel have access to the database only for troubleshooting and customer escalation purposes; they do not grant clients any direct access to the database.

Elastic Cloud Security

BeyondTrust uses Elasticsearch for analytics and reporting purposes, communicating with Elasticsearch and Logstash through REST API. Security for these APIs is provided using OAuth. To ensure the necessary access rights, separate Read-Write users are created with defined privileges; the *Read* user is used for analytics and reporting, whereas the *Write* user is used for logging.

Elasticsearch uses Transparent Data Encryption (TDE) for encryption at rest.

Network Security

All EPM 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; instead, internal access has been locked down to allow connections only from within the cluster subnet. The Jump Client, used for support purposes, is also located in this subnet. Additionally, port 22 has been opened to BeyondTrust IP address for Shell Jump access.

Access to the Azure Management Console is stringently restricted within BeyondTrust. Access is granted only to personnel who have a legitimate need to be able to use the console, and is further secured by phishing-resistant MFA.

Encryption and Ports

EPM 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, which is restricted to a single BeyondTrust IP address.

Encryption in Motion

All traffic to and from EPM is encrypted using TLS 1.2 or TLS 1.3. By default, the site uses the provided wildcard certificate corresponding to the host name in use. For additional security, older ciphers, such as TLS 1.0 / 1.1, SSL 2.0, and SSL 3.0, are disabled.

Encryption at Rest

All data in Endpoint Privilege Management is securely stored in Microsoft Azure SQL databases with transparent encryption enabled.

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

Authentication to Endpoint Privilege Management

Portal

Authentication for Endpoint Privilege Management is achieved through Azure B2B or Open ID Connect (OIDC). User permissions are managed through role-based access control, providing users with access to privileged features based on their role and corresponding privileges.

Azure B2B

Customers using Azure B2B are required to be part of an Entra ID instance. These users authenticate using existing corporate means, such as any MFA that is configured within their Entra ID instance. Customers have full control of the password policy, and BeyondTrust does not have any visibility of end-user credentials. For initial user login, an invitation is sent during the fulfillment process. As such, the first admin email address must be provided prior to deployment.

For customers who do not have Entra ID, we recommend that they federate their existing Identity Provider (IDP) with Entra ID to enable authentication via this method.

OpenID Connect

Endpoint Privilege Management provides support for OpenID Connect (OIDC) authentication. Administrators with privileged permissions in EPM can easily switch the authentication method of any customer from the default Azure B2B to OpenID Connect, or can update their existing OpenID Connect settings quickly and effortlessly, all without having to contact BeyondTrust Support.

EPM supports a range of OpenID authentication providers, including Microsoft Entra ID, Okta OpenID, and Ping Identity Connect.

Once a customer has switched from Azure B2B to OpenID Connect, there is no way to revert back to using Azure B2B.

Endpoints

Endpoints can be registered with EPM using installation keys for secure communication. Authentication for further interactions with other services is enabled via OAuth.

Access Management

Microsoft Azure Console

Access to the Azure management console for the subscription where the customer's deployment lives is exclusively available to BeyondTrust employees who require it for their job responsibilities. To maintain security, phishing-resistant MFA is required to access the console, and all activity is audited for compliance.

BeyondTrust Access to Customer Instances

OS-level access to Endpoint Privilege Management instances or clusters requires the use of Privileged Remote Access (PRA). This access is granted to a limited number of authorized support, cloud operations, and engineering employees, and is subject to IT-maintained phishing-resistant MFA for additional security. Furthermore, granular permission-setting ensures that only approved accounts are granted access. To ensure accountability, all sessions must be recorded and stored for a minimum of 90 days.

Only a select few authorized support, cloud operations, and engineering personnel are allowed access to the backend of customer instances.

A support incident is required to access a customer instance, except for in the case of Severity Level 1 incidents, for which an exception may apply.

Hosting Regions

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
- Brazil

Backup and Recovery

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 read-access geo-redundant storage (RA-GRS) blobs, which are replicated to a paired data center to protect against any possible data center outages. The restore process automatically determines which full, differential, and transaction log backups must be used to restore the database.

The initial full backup of a newly deployed database is scheduled immediately.

Monitoring

Site24x7

Site24x7 is used to monitor the performance of Endpoint Privilege Management instances. During the build process, each hosted instance is linked to Site24x7 automatically. Regular health checks are conducted to guarantee every instance functions as expected. If a health check fails twice in a row, the instance is flagged as *down* and an alert is sent. Alerts come in the form of notifications on the Site24x7 dashboard and emails. Taking advantage of multiple geographical locations, global accessibility is ensured.

Logging

Application-level logs are sent to a dedicated Elasticsearch (ELK) instance maintained by the BeyondTrust Cloud Operations team within the Azure infrastructure. The purpose of the ELK system is to collect comprehensive application-level logs, which are then used by the support teams for troubleshooting purposes. Logs are retained for up to 30 days and then automatically overwritten.

Security and Vulnerability Monitoring

BeyondTrust provides an agentless vulnerability management solution for full visibility across the company's cloud accounts and resources. Using side-scanning, the solution ingests itself into the snapshot process. It assesses snapshots for security threats and gains contextual data and alerting based on criticality. BeyondTrust's solution creates alerts both in the native console and SIEM platform for easy review and action.

The BeyondTrust SIEM receives comprehensive security logging from Azure Security center, such as ingress authentication logging to track user access and activity, threat analytics to detect any suspicious software installations, and third-party access detection to alert BeyondTrust personnel to any potential malicious activities. All such incidents are automatically reported to the BeyondTrust InfoSec team for analysis and appropriate action taken based on the severity and relevance of the alert.