BeyondTrust

Cloud Privilege Broker 22.1
Security Whitepaper

TC:11/2/2022

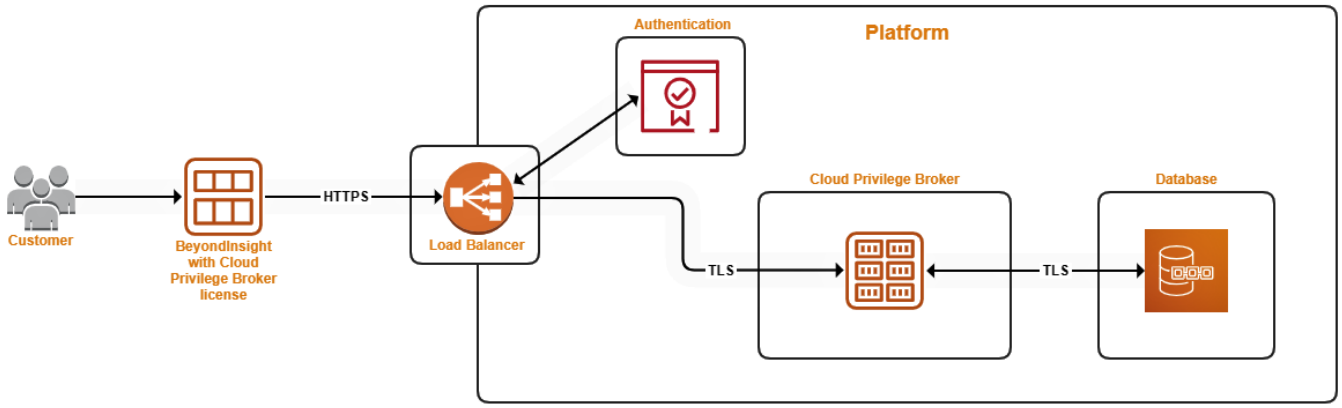
Table of Contents

Cloud Privilege Broker Cloud Security

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

Architecture

Summary of Cloud Privilege Broker architecture, as hosted within Amazon Web Services.



Network Security

All network access controls within Cloud Privilege Broker are secured within the underlying platform.

Cloud Privilege Broker exists within its own isolated namespace and network ingress/egress within namespaces is controlled by the platform. All service-to-service communications are mutually authenticated and encrypted via Transport Layer Security (TLS) encryption provided by the platform. All customer logins are handled via BeyondInsight.

For more information, please see "Network Security" on page 5.

Customer Data

Each service within Cloud Privilege Broker has its own dedicated database and no user has access to database secret keys. Database credentials are provisioned by the platform and the services are allowed access via an IAM policy.

Cloud Privilege Broker's backup data stores employ encryption at rest using AES-256, an industry standard. Storage volume snapshots of the database instance are backed up nightly and retained for 30 days.

For more information on customer data security, please see "Customer Data" on page 5.

Encryption

There is complete end-to-end encryption from BeyondInsight with Cloud Privilege Broker through to the Cloud Platform Infrastructure. Cloud Privilege Broker services communicate with each other through distributed queues over TLS encryption.

Access Management

Within Cloud Privilege Broker, no administration access is required or allowed, and administration access is contained within the platform. All services run on hardened images with read-only file systems.

Using IRSA (IAM Roles for Service Accounts), service-to-service communication is restricted to the session required. Service boundaries are set and only the service account annotated to talk to the database can communicate with the database. This ensures that no credential leak for the database can occur.

For more information, please see "Access Management" on page 6.

Process Control

Using GitOps enables continuous deployment when operating infrastructure. GitOps also provides benefits such as deployment and change logging to assist with compliance requirements.

A Git repository contains declarative descriptions of the infrastructure currently desired in the production environment and an automated process to make the production environment match the described state in the repository. This system state is version managed.

Platform Security

Physical Security

Physical Security is managed by Amazon data center controls.

> *For more information, please see Our Controls at https://aws.amazon.com/compliance/data-center/controls/.*

Network Security

The BeyondInsight platform uses an N-Tier architecture which ensures that processing, data management, and presentation functions are physically and logically separated. The benefits of this model are that resources are not shared and services are delivered at top capacity. Each layer can be secured based on the services contained within.

All platform cloud instances are running within Amazon Virtual Private Cloud (Amazon VPC) and subnets with firewall rules set via well-defined security groups. Nodes are set to least privilege, only allowing access to the services required. Remote access via SSH and RDP are disabled.

Access to the AWS Console where the network/VPC configuration is managed is also highly restricted within BeyondTrust, available only to those who have a requirement to access the console. All access must go through a security account with multi-factor authentication enforced when assuming roles across AWS accounts.

Service Mesh

The BeyondInsight platform uses a service mesh to help reduce complexity for service-to-service communication. A service mesh provides the following benefits for Infrastructure:

- Lock down data plane traffic using mutual Transport Layer Security (mTLS), making service-to-service communication more secure.
- Availability and resilience (for example, setup retries, failovers, circuit breakers, and fault injection).
- Automatic metrics, logs, and traces for all traffic within a cluster, including cluster ingress and egress.

> *For more information, please see What's a Service Mesh? at https://www.redhat.com/en/topics/microservices/what-is-a-service-mesh.*

Customer Data

Customer Data is handled with the utmost care whether in transit or at rest, using industry best practices for encryption. Regular data backups and retention policies are set to ensure data is always highly available yet secure.

Access to databases that contain customer data is tightly controlled with auditing and monitoring in place. Using the principal of least privilege, only those who require access have access, with time limitation in place.

Availability and Disaster Recovery

The BeyondInsight platform is deployed across six availability zones within Amazon Web Services, along with full high availability and fault tolerances across all resources.

Encryption

The BeyondInsight platform Infrastructure is configured to use complete end-to-end encryption.

Encryption in Motion

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

Encryption at Rest

All data in the platform is stored in databases and Elastic Block Storage (EBS) volumes using Amazon-managed keys (AWS Key Management Service).

Access Management

AWS Identity and Access Management (IAM)

All access to the platform is routed through an AWS security account. This account is used to manage authentication and authorization to the production environment. With a single point of entry, this allows for greater visibility via auditing and logging. This method is enhanced via AWS Config and AWS CloudTrail.

> *For more information, please see the following AWS documents:*
> - *What is IAM? at https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.*
> - *What is AWS Config? at https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html.*

IAM Roles for Service Accounts

IRSA (IAM roles for service accounts) are used with the platform.

With IRSA, an IAM role is associated with a service account. This service account can then provide AWS permissions to the containers in any pod that uses that service account. Applications must sign their AWS API requests with AWS credentials to gain access to authorized AWS Services.

The IAM roles for service accounts feature provides the following benefits:

- Least privilege: By using the IAM roles for service accounts feature, it is not necessary to provide extended permissions to the node IAM role so that pods on that node can call AWS APIs. IAM permissions are scoped to a service account, and only pods that use that service account have access to those permissions.
- Credential isolation: A container can retrieve credentials only for the IAM role that is associated with the service account to which it

belongs. A container never has access to credentials that are intended for another container that belongs to another pod.

- Auditability: Access and event logging are available through CloudTrail to help ensure retrospective auditing.

> *For more information, please see IAM Roles for Service Accounts at https://docs.aws.amazon.com/eks/latest/userguide/iam-roles-for-service-accounts.html.*

Application, Security, and Vulnerability Monitoring

AWS CloudTrail

AWS CloudTrail is an AWS service that helps enable governance, compliance, and operational and risk auditing of the AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

AWS CloudTrail logs are forwarded to the BeyondTrust SIEM for analysis.

> *For more information, please see What is AWS CloudTrail? at https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html.*

Monitoring Service

The platform uses an industry standard monitoring service. This service provides the following benefits:

- Increased visibility to platform services
- Realtime monitoring of critical systems
- Reduced incident response time
- Increased uptime
- Dashboards and alerting

Intrusion Detection System

The platform uses industry best practices for container runtime security. All events are monitored and report against a rules engine. Once a rule is violated, an alert is issued and forwarded to the BeyondTrust monitoring service.

Within the monitoring service, a dashboard and monitors are set up to ensure the correct parties are notified when an alert is triggered.

Vulnerability Monitoring

The BeyondInsight platform is connected to vulnerability management software.

The following items are monitored, and alerting is set up for any failures.

- Infected assets
- Misconfigurations
- Vulnerabilities

- Weak or leaked credentials
- Insecurely stored keys or secrets