United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: BeyondTrust BeyondInsight	
Preparer: Phillip Starke (Alternate) Greg Zurla (Application Owner)	**Office:** OMS-OITO-ECSD OMS-OITO-ECSD
Date: April 26, 2023	**Phone:** 202-566-1416 303-312-6182
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

BeyondTrust BeyondInsight, an Enterprise Services (ESS) application, is a Privileged Access Management (PAM) platform (administrative tool) that provides visibility and control over privileged access activity on EPA Windows operating system (OS) workstations (endpoints) through centralized management, reporting, threat intelligence and analytics.

Beyond Insight enables IT and security professionals to collaboratively reduce user-based risks, mitigate threats to information assets, address security exposures across large, diverse IT environments, and comply with internal, industry, and government mandates.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

- Federal Information Security Modernization Act of 2014 (FISMA, 44 U.S.C. § 3551)
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised July 26, 2016
- The Computer Security Act of 1987 (Pub. L. 100-235)

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

BeyondTrust BeyondInsight is a sub-system application under the Enterprise Services System (ESS) System Security Plan (SSP). BeyondTrust BeyondInsight is covered under the Enterprise Services System (ESS) MA Authorization-to-Operate. The ATO expiration date is January 13, 2025.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not Applicable.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes. BeyondTrust BeyondInsight data is stored on the application maintained by EPA, within the EPA dedicated Amazon Web Services (AWS) Enterprise Hosting Cloud Service (ECHS) cloud which is hosted by an approved Infrastructure-as-a-Service (IaaS) FedRAMP Cloud Service Provider (CSP) AWS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well

as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The data elements captured or collected by BeyondTrust BeyondInsight are:

Personal Identifiable Information (PII): Data elements that can be linked to an individual

- **Username:** The account name of the EPA users LAN ID
- **Name (Dotted accounts):** firstname.lastname (e.g. jane.doe) of EPA Privilege LAN ID

Note: EPA Username/LAN ID (e.g. jdoe) consist of the first initial and up to 7 characters of a employee/contractors last name. If this results in the same Username/LAN ID as another employee/contractor, EPA will typically modify this to include a numerical value (e.g.jdoe01). Name (Dotted accounts) consist of the first and last name of a employee/contractor (e.g. jane.doe).

Non-PII: Data elements that cannot be linked to an individual

- **Reputation**: Shows if one or more reputation providers have been configured to provide threat context and reputation data to help analyze suspicious files, URLs, domains, and IP addresses to detect cybersecurity threats to help determine whether an if it's suspicious or malicious.
- **Time Generated**: Date and time event occurred
- **Event Category**: Event categories can be any number of verbs (BeyondInsight Application Audit, clarity, File Integrity Monitoring, etc.)
- **Event Type**: The type of event you are interested in viewing (e.g., applications that performed privilege operations or applications that were blocked)
- **Event Description**: Additional descriptive details for the event. This varies in level of detail based on the event source, etc.
- **Publisher**: The publisher of the application
- **Host Name**: The host name\computer name of the client the user is logging on from. This field allows you to filter by the name of the endpoint the event came from
- **Policy**: Provides Endpoint Privilege Management polices to assets and policy users.
- **GPO Name**: The name of the GPO that contained the matching policy. You can filter on the Group Policy Object (GPO) name in some of the advanced reports such as Process Detail.
- **Unique ID**: BeyondInsight generates a unique identifier (API Key) that the calling application provides in the authorization header of the web request.
- **Description**: A text field that allows you to filter on the application name.
- **Policy ID**: Assigned number outside of the policy name used in BeyondTrust BeyondInsight
- **Event Number**: Number assigned to the event type and used by Reporting.
- **Elevation Method**: This allows users to filter events by the type of elevation used. For example, Admin account or on-demand.

- **External Source**: This allows users to filter by the type of external source that the application file came from. For example, downloaded over the internet or removable media.
- **Distinct Application ID**: Unique application ID created in Azure
- **Platform Type**: Operating System running on the computer
- **Multi-Platform User**: Captures if user access us across multiple OS platforms
- **Authorizing User Credential Source**: Provides source of the security credentials used to authenticate and authorize user requests.
- **Application ID**: Unique Application (Client) ID created within Azure for that can be used assign policy

2.2 What are the sources of the information and how is the information collected for the system?

The source of the information comes from the BeyondTrust BeyondInsight Events Client running locally on the Windows workstation that is responsible for forwarding information gathered by the Discovery Scanner agent. The Events Client sends the information to the Manager Service which acts as a background service gathering information from the Events Client, which retrieves information from the BeyondInsight agents. The events are then encrypted and sent to the database.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

BeyondTrust BeyondInsight does not use any information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

BeyondTrust BeyondInsight doesn't rely on any manually collected data that can be incorrectly entered during the collection that can make the data inaccurate. The data is collected using automated methods via installed agents performing scans on the workstations. To ensure the accuracy of the data there are security protocols in place to prevent the data fields from being able to be modified or manually entered. In addition, the stored data is encrypted to prevent access and any manipulation of the data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Inaccurate information submitted into BeyondTrust BeyondInsight.

Mitigation:

The risk of mischaracterization of information related to sources, methods of collection, or quality of the data collected by BeyondTrust BeyondInsight is mitigated through policies where personal identifiable information (PII) data collected by the application is fully automated and limited to the EPA LAN IDs which must be used to successfully authenticate to the application to prove the quality of the information submitted.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Does the system have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

BeyondTrust BeyondInsight offers a role-based delegation model to prevent unauthorized users from accessing the application by explicitly assigning permissions to groups on specific product features based on their role.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

BeyondInsight has Administrator and Users guides that explains how roles are created, what permission the roles have, etc. BeyondTrust Privilege Management Version 22.9 for Windows Administration Guide and the BeyondTrust_BeyondInsight User Guide.

3.3 Are there other components with assigned roles and responsibilities within the system?

There are no other components with assigned roles and responsibilities within the system.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Authorized EPA Federal and EPA contractual personnel will have access to this data/information.

The appropriate FAR clauses are included in the contract.

- 52.224-1: Privacy Act Notification
- 52.224-2: Privacy Act
- 52.224-3: Privacy Training

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the

schedule number.

The BeyondTrust BeyondInsight data console data retained for only 90 days.
The BeyondTrust BeyondInsight audit log data is retained for a period of at least 1 year in Splunk to support the requirement to provide the ability to support security investigations. This follows EPA Records Control Schedule 1012.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There's a risk that data is retained for longer periods than 90 days making it more likely that an unauthorized user (For example: a user transferred that no longer need access to the console) accidentally expose/access the data.

Mitigation:

The System auto deletes the data or information after 90 days. In addition, monthly account access reviews are completed to verify that any active accounts are still valid.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No. Information is not shared outside of EPA as part of the normal agency operations.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

Not Applicable. There is no external sharing.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Not Applicable. There is no information shared with any other organization.

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable. There is no information shared with any other organization.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. There is no information sharing.

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

BeyondTrust BeyondInsight ensures that the information is used as stated in section 6.1 by employing technical security controls (identity and access management (IAM) solutions and intrusion prevention systems (IPSs)) and logical security controls (PIV card and role-based access control) to help prevent unauthorized access. Auditing user actions is also captured in the console and Splunk reviewed at least weekly.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Users are required to take the complete the EPA Information Security and Privacy Awareness Training within 60 days of hire. In addition, annual Information Security and Privacy Awareness Training must be completed.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Risk associated with auditing and accountability in relation to BeyondTrust BeyondInsight would be if unauthorized access to the application and data is not maintained and reviewed.

Mitigation:

BeyondTrust BeyondInsight limits access to data and to audit logs to only a few administrators that are approved by the Application Owner. In addition, there are encryption

mechanisms that prevents information loss or theft while data is stored and in transit by having data encrypted in transport and at rest. This prevents data from being readable by anyone other than approved personnel.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

BeyondTrust BeyondInsight uses the information collected to gain visibility or insight onto users that have elevated permissions or privileges to help prevent data breaches related to stolen credentials, misused privileges, and compromised remote access.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X__. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

BeyondTrust BeyondInsight is designed to retrieve program elevation requests by administrative users (using usernames aka computer names) via the reports. Reports can be run using a username or computer name in order to view privilege access a user may or may not have. None of the information in reports is linkable to any other data not already disclosed in all EPA applications using EPA credentials.

Theses reports will not contain any PII of an individual. For the list of data elements displayed in the reports, refer back to Section 2.1, "Non-PII: Data elements that cannot be linked to an individual."

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

A Security Impact Analysis (SIA) was completed for the addition of the BeyondTrust BeyondInsight to the Enterprise Services System SSP.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is always small risk that the information in a system could be used or handled in a manner that isn't authorized.

Mitigation:

All data is encrypted in transit using transport layer security (TLS) over port 443. In addition, role-based access is in place that limits access to only personnel and administrators and training on how to handle information occurs at least annually.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them,

and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: