bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INFORMANDO

Panther SIEM

Ver en el centro de ayuda:
https://bitwarden.com/help/panther-siem/

Panther SIEM

Panther es una plataforma de gestión de información y eventos de seguridad (SIEM) que se puede utilizar con organizaciones de Bitwarden. Los usuarios de la organización pueden monitorear la actividad de eventos con la aplicación Bitwarden en su sistema de monitoreo Panther.

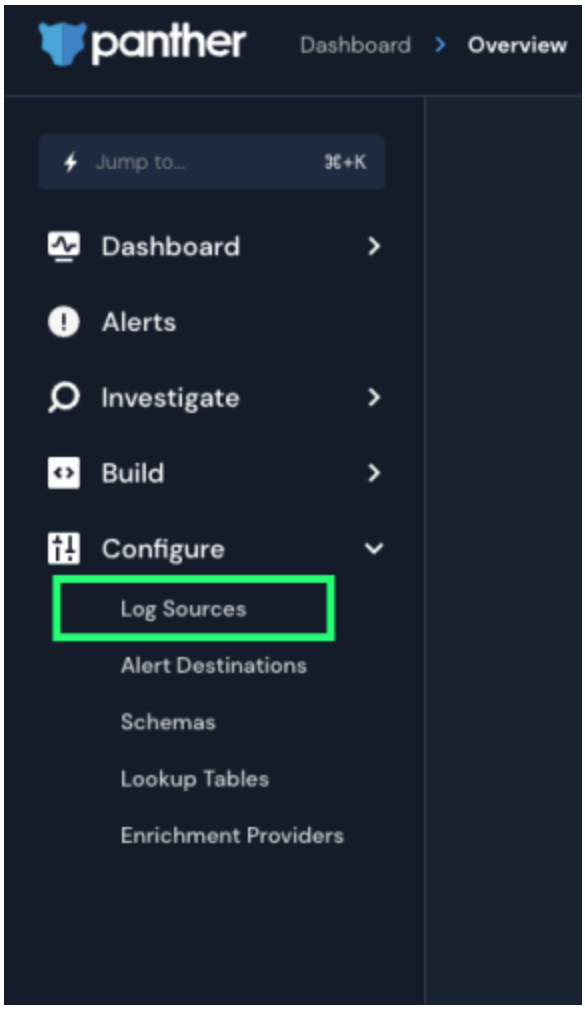
Configuración

Crea una cuenta de Panther

Para comenzar, necesitarás una cuenta de Panther y un tablero de control. Crea una cuenta de Panther en su sitio web.

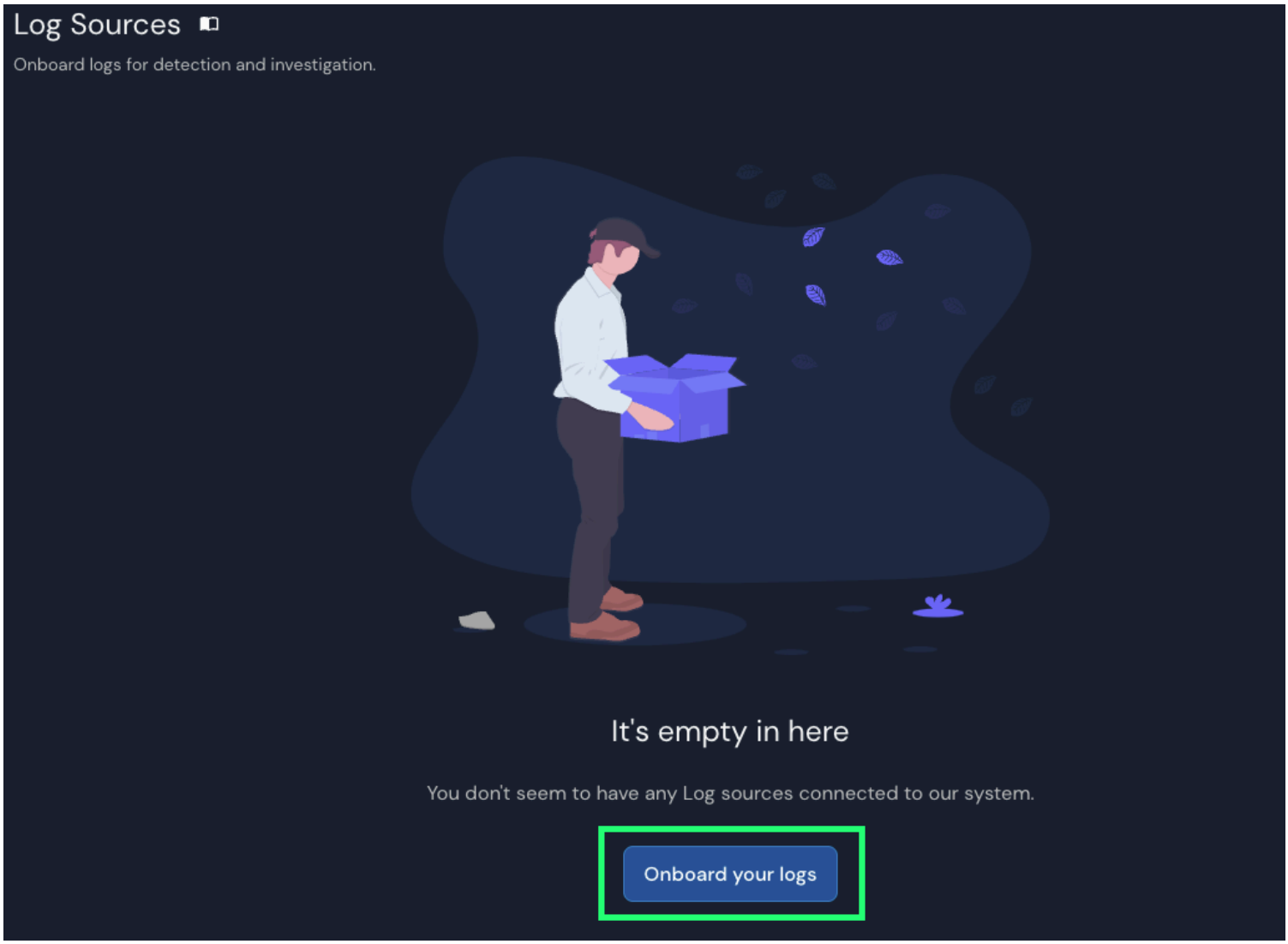
Inicializar Fuente de Registro Bitwarden Panther

1. Accede al panel de control de Panther.
2. En el menú, abre el desplegable **Configurar** y selecciona **Fuentes de Registro**.



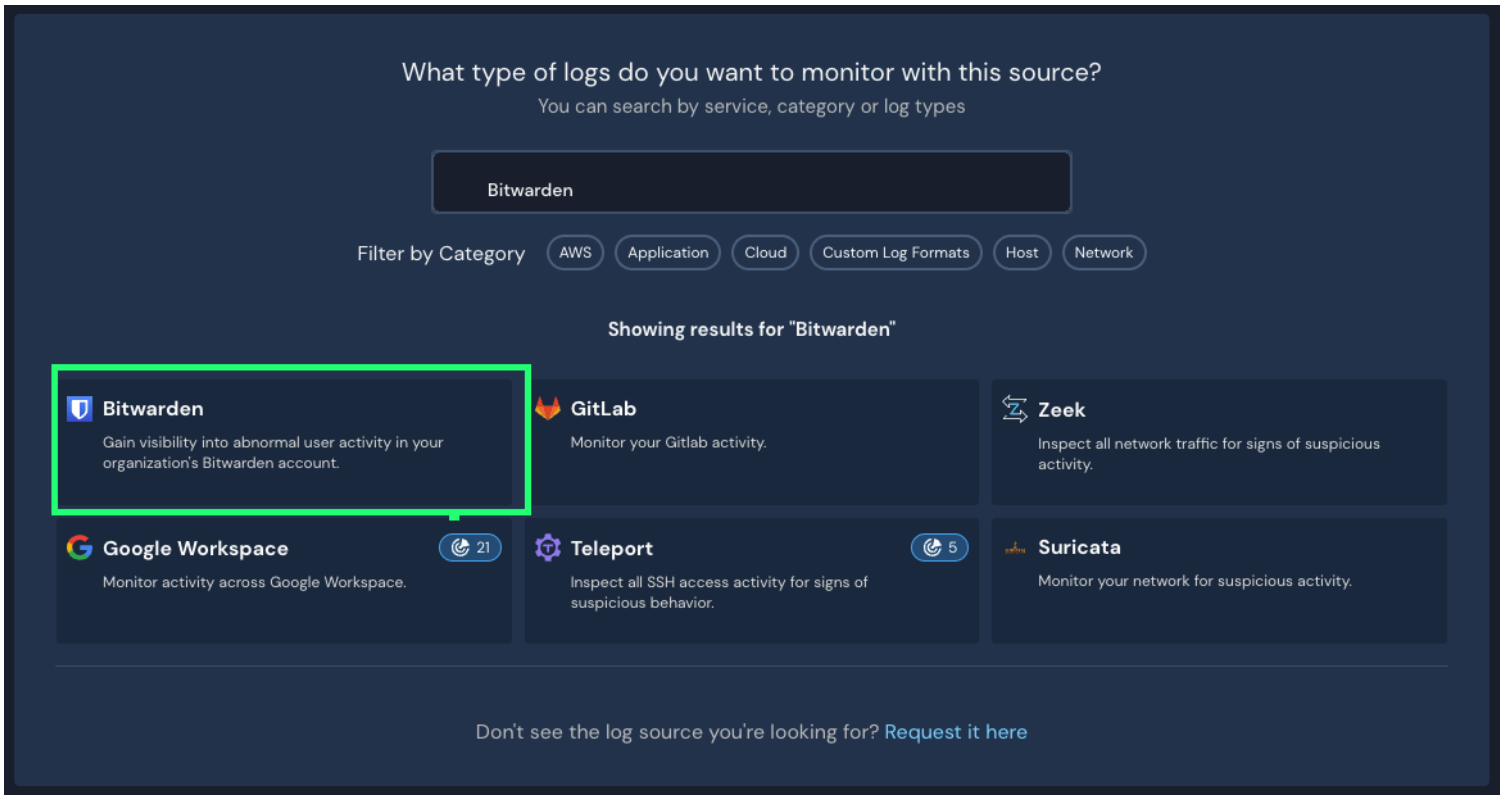
Panther Log Sources

3. Seleccione **Embarque sus registros**.



Panther Onboard logs

4. Busca **Bitwarden** en el catálogo.



Elastic Bitwarden integration

5. Haz clic en la integración de **Bitwarden** y selecciona **Iniciar Configuración**.

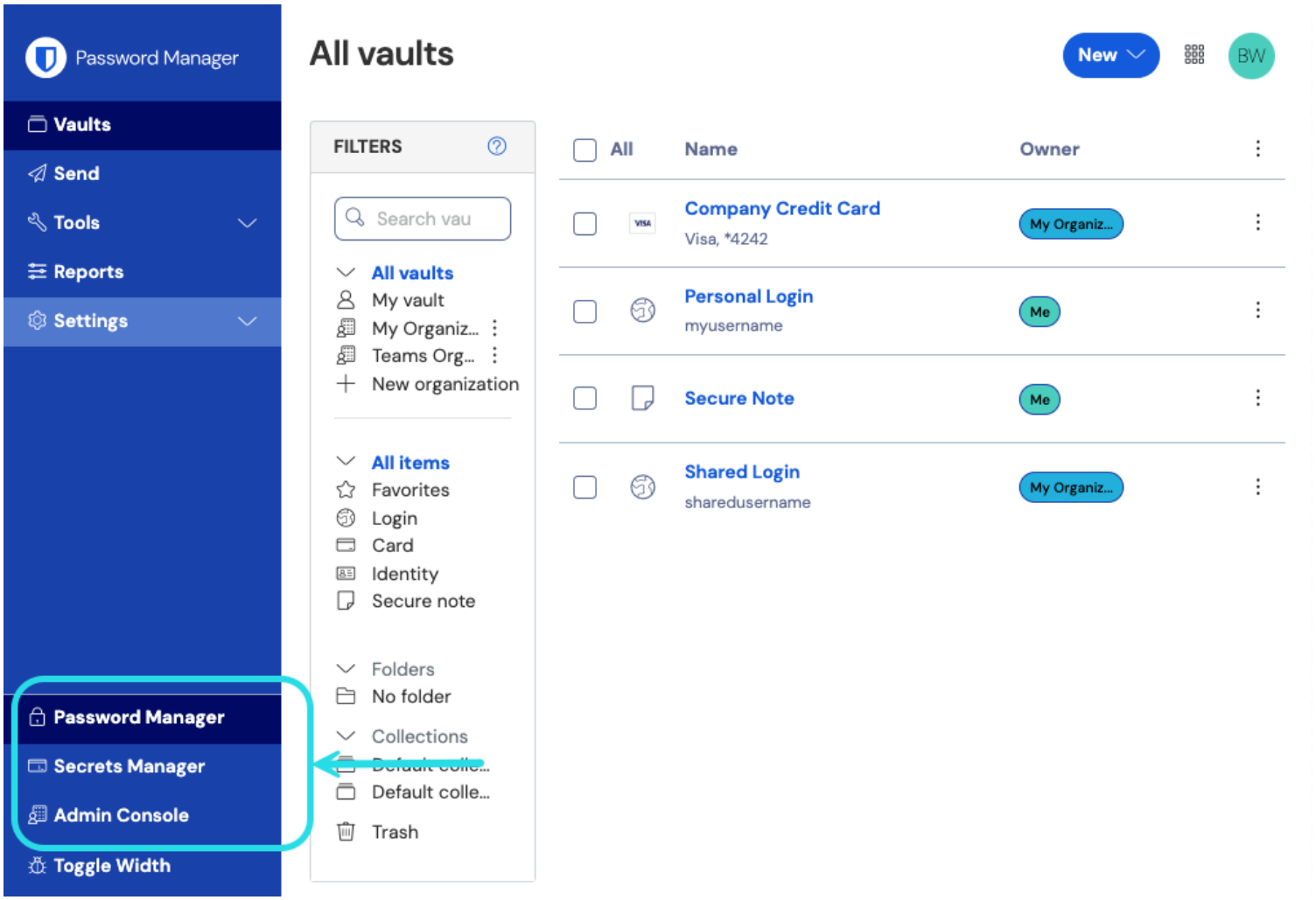
Conecta tu organización Bitwarden

Después de seleccionar **Iniciar Configuración**, serás llevado a la pantalla de configuración.

> **ⓘ Note**
>
> Panther SIEM services are only available for Bitwarden cloud hosted organizations.

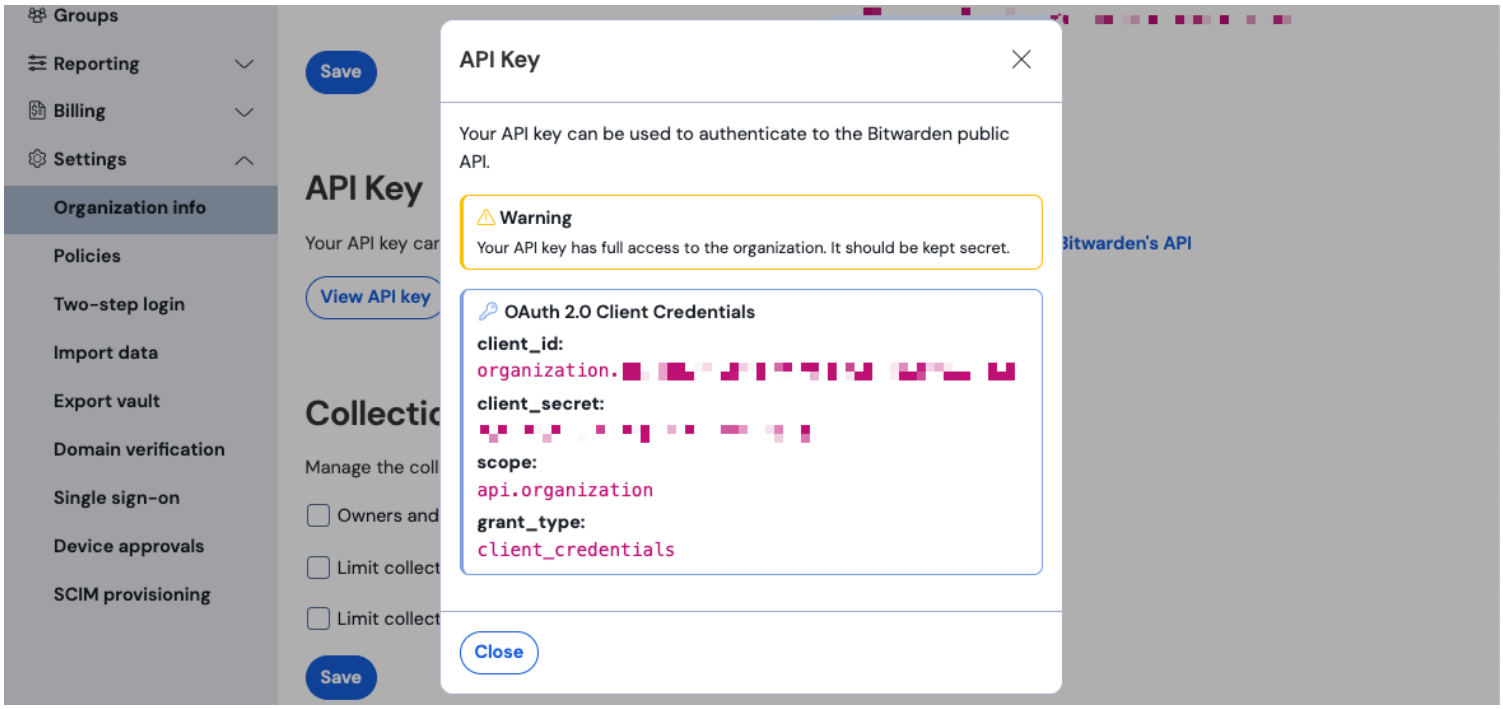
1. Ingrese un nombre para la integración y luego seleccione **Configuración.**

2. A continuación, tendrás que acceder a tu **ID de Cliente** y **Secreto de Cliente** de la organización Bitwarden. Manteniendo esta pantalla abierta, en otra pestaña, inicie sesión en la aplicación web de Bitwarden y abra la Consola de Administrador usando el cambiador de producto (⊞):



Selector de producto

3. Navegue a la pantalla de información de su **ajustes** de la organización → y seleccione el botón **Ver clave API**. Se le pedirá que vuelva a ingresar su contraseña maestra para acceder a la información de su clave API.



Información de API de la organización

4. Copia y pega los valores de `client_id` y `client_secret` en sus respectivas ubicaciones en la página de configuración de la aplicación Bitwarden. Una vez que haya ingresado la información, continúe seleccionando **Configuración** de nuevo.

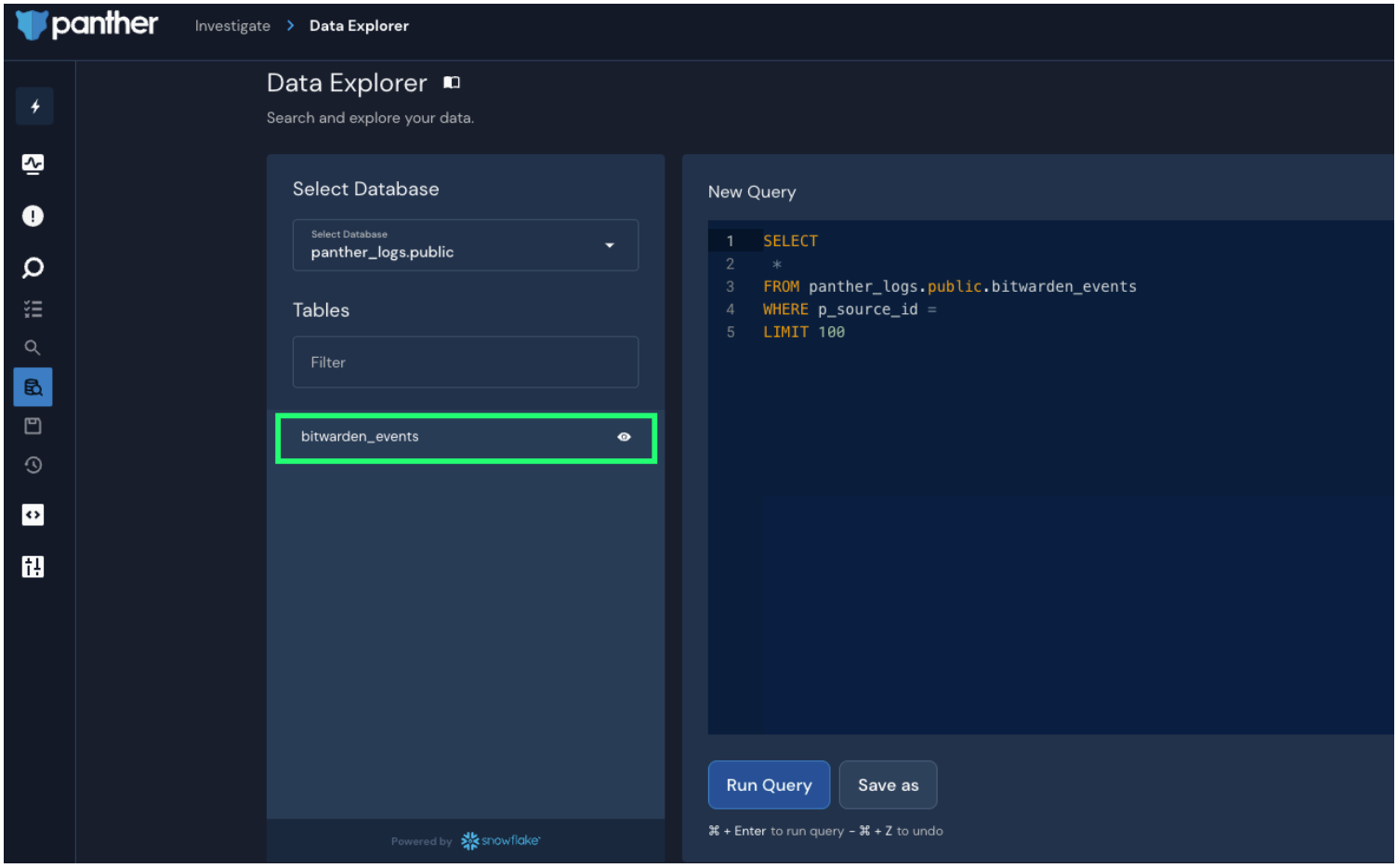
5. La pantera realizará una prueba en la integración. Una vez que se haya completado con éxito una prueba, se le dará la opción de ajustar las preferencias. Completa la configuración presionando **Ver Fuente del Registro**.

> **Note**
> Panther may take up to 10 minutes to ingest data following the Bitwarden App setup.

Comienza a monitorear los datos

1. Para comenzar a monitorear los datos, dirígete al panel principal y selecciona **Investigar** y **Explorador de Datos**.

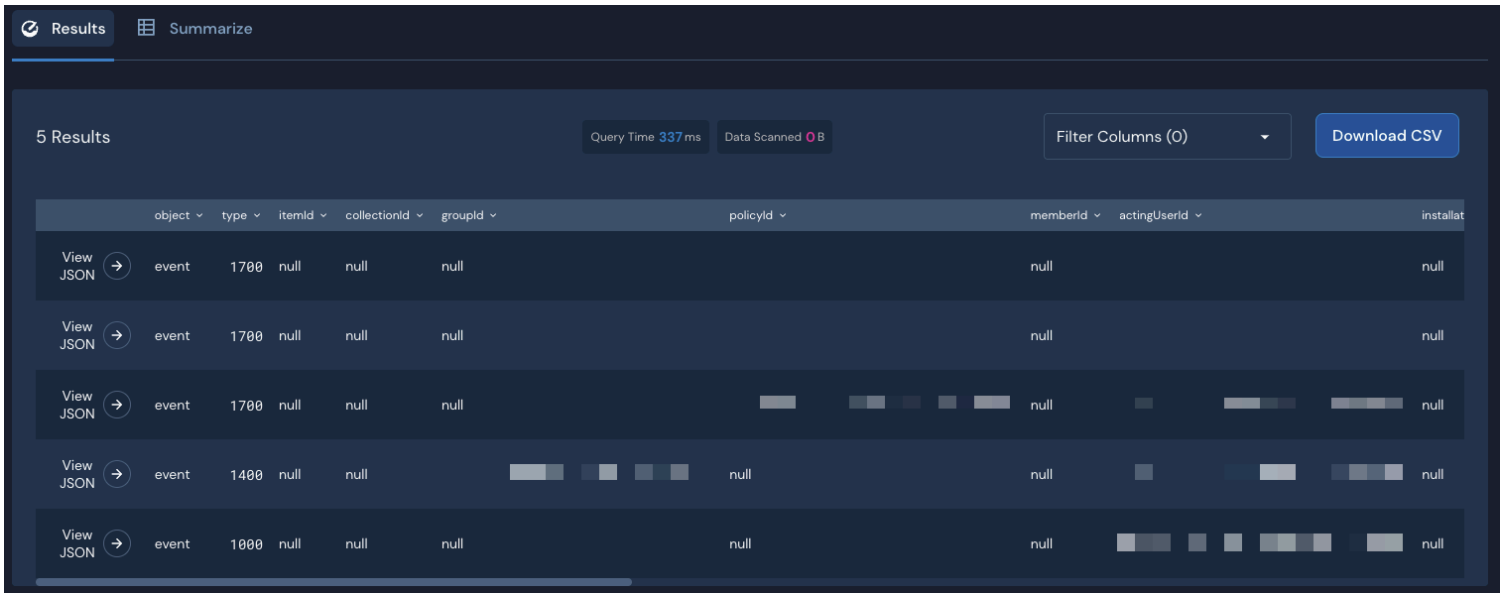
2. En la página del Explorador de Datos, seleccione la base de datos `panther_logs.public` del menú desplegable. Asegúrate de que también se esté viendo `bitwarden_events` .



Panther Data Explorer

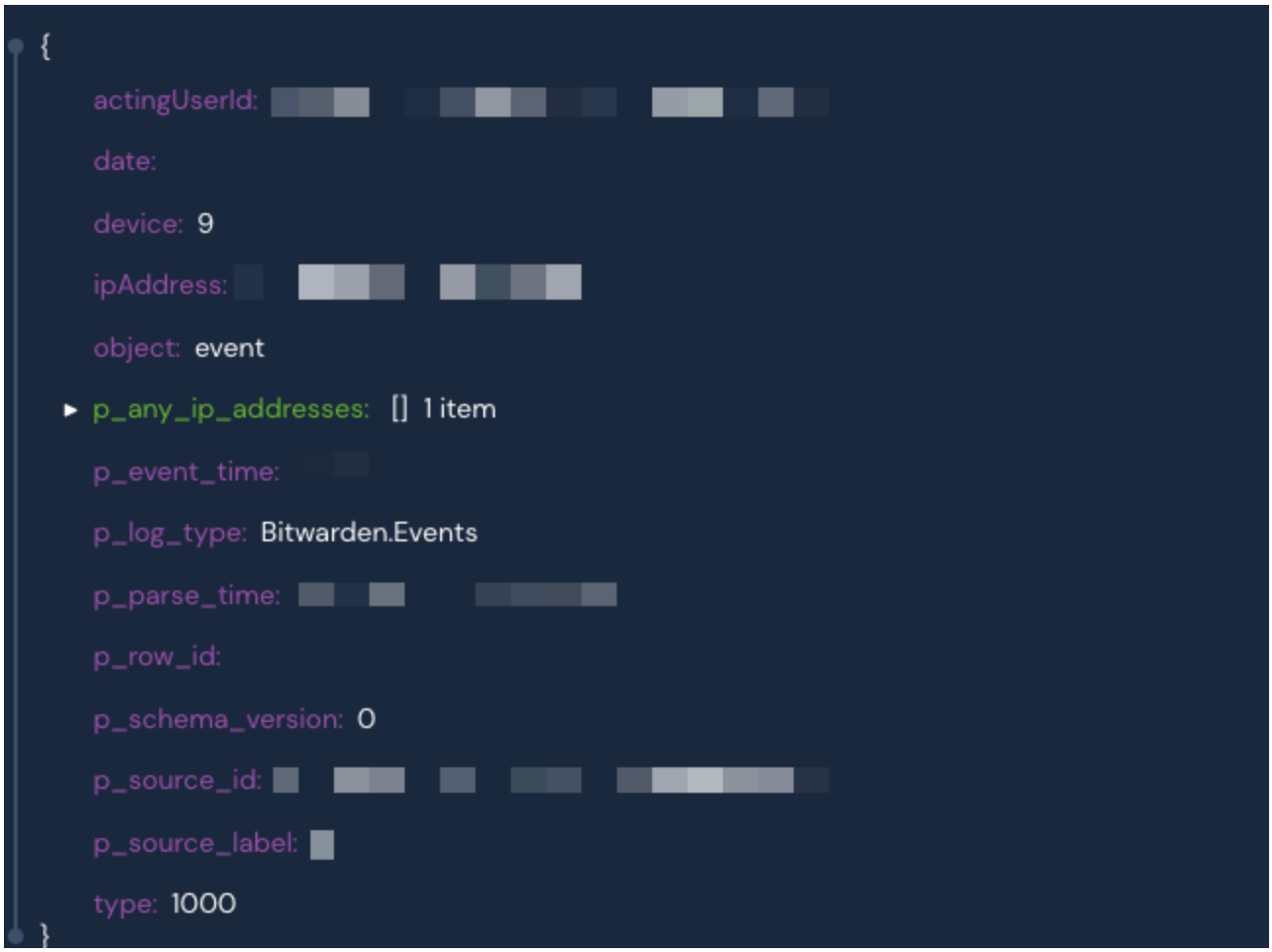
3. Una vez que haya realizado todas sus selecciones requeridas, seleccione **Ejecutar Consulta**. También puedes **Guardar como** para usar la consulta en otro momento.

4. Una lista de eventos de Bitwarden se producirá en la parte inferior de la pantalla.



Panther Event Logs

5. Los eventos se pueden expandir y ver en JSON seleccionando **Ver JSON**. ⊖.



Panther JSON Object

Para obtener información adicional sobre los eventos de la organización Bitwarden, vea aquí. Opciones adicionales para consultas específicas están disponibles, consulte la documentación del Explorador de Datos Panther para obtener más información.