

ADMIN CONSOLE > OVERSIGHT & VISIBILITY > SIEM INTEGRATIONS

Sumo Logic SIEM

View in the help center:

<https://bitwarden.com/help/sumo-logic-siem/>

Sumo Logic SIEM

Sumo Logic is a solution that can provides visibility into your Bitwarden organization's user and vault activity. The Sumo Logic Bitwarden integration allows users to monitor important organization activity such as logins, failed two-step verifications, mater password reset, and decryption key migrations.

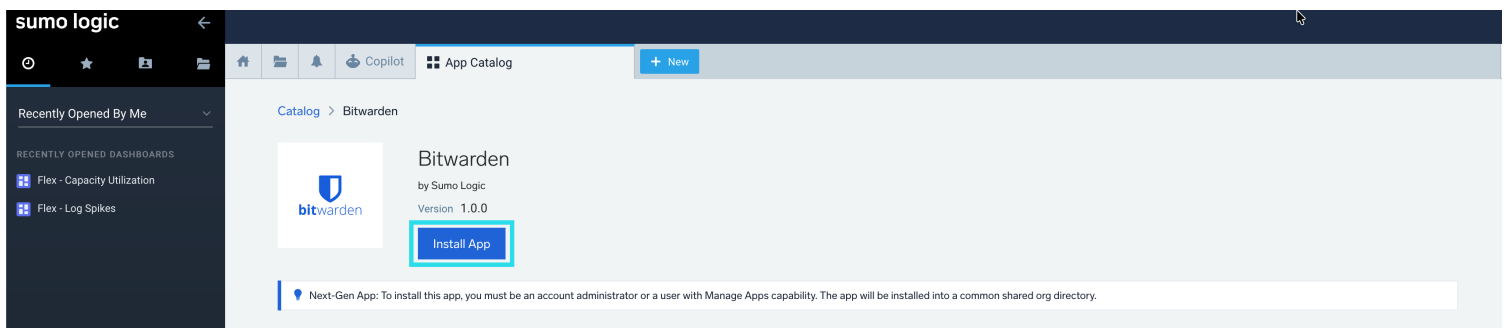
Setup

Create a Sumo Logic account

To begin, [create a Sumo Logic account](#), or log into an existing Sump Logic account with permission to create and manage an application.

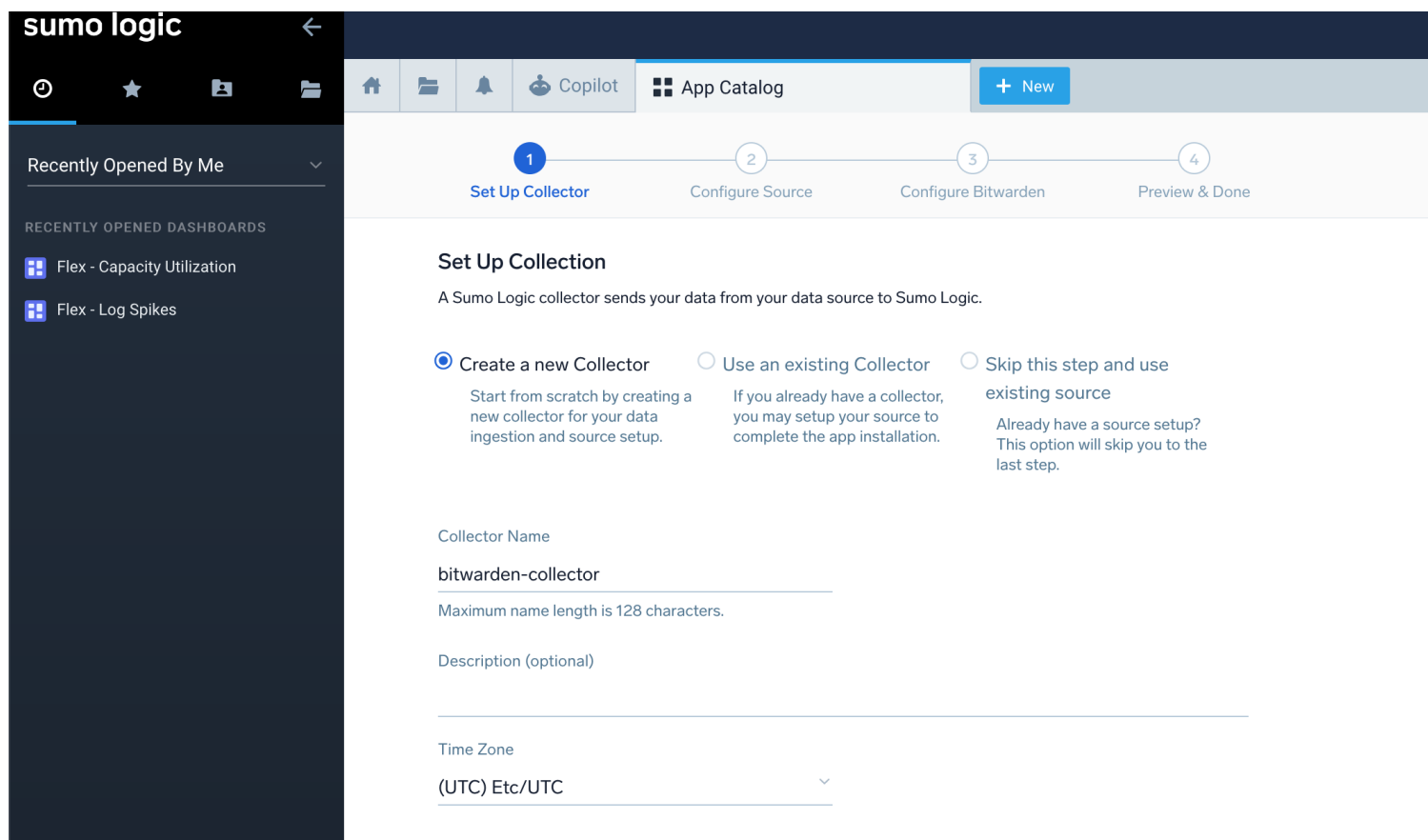
Download the Bitwarden app

1. From the Sumo Logic dashboard, navigate to the **App Catalog** and search Bitwarden. Select **Install App**.



Install Bitwarden app

2. Next, on the **Set Up Collection** screen select **Create a new Collector**.



sumo logic

Home Recent Copilot App Catalog + New

1 Set Up Collector 2 Configure Source 3 Configure Bitwarden 4 Preview & Done

Set Up Collection

A Sumo Logic collector sends your data from your data source to Sumo Logic.

☒ Create a new Collector ☐ Use an existing Collector ☐ Skip this step and use existing source

Start from scratch by creating a new collector for your data ingestion and source setup.

If you already have a collector, you may setup your source to complete the app installation.

Already have a source setup? This option will skip you to the last step.

Collector Name

bitwarden-collector

Maximum name length is 128 characters.

Description (optional)

Time Zone

(UTC) Etc/UTC

Create a collector

3. Input a **Collector Name**, **Timezone**, and optional **Metadata**. Once complete, select **Next**.

4. On the **Configure Source screen**, provide a **Name** for the application, such as Bitwarden Event Logs.

The screenshot shows the Sumo Logic App Catalog interface. On the left is a sidebar with navigation options: App Catalog, Manage Data, Administration, Help, and Switch to New UI. The main area displays the configuration steps for Bitwarden: 1. Set Up Collector, 2. Configure Source, 3. Configure Bitwarden, and 4. Preview & Done. The 'Next' button at the top right is highlighted with a red box. The configuration form includes fields for Name (Bitwarden Event Logs), Description (optional), Source Category (optional), Fields (a table with Key and Value columns), Bitwarden API Server Base URL (https://api.bitwarden.com), OAuth 2.0 Client ID (organization.), OAuth 2.0 Client Secret, Polling Interval (Set how frequently to poll, Interval (optional), 15m), and a Learn More link.

configure application connection

5. Keep this screen open and in a new tab, open your Bitwarden organization's web vault.

Connect your Bitwarden organization

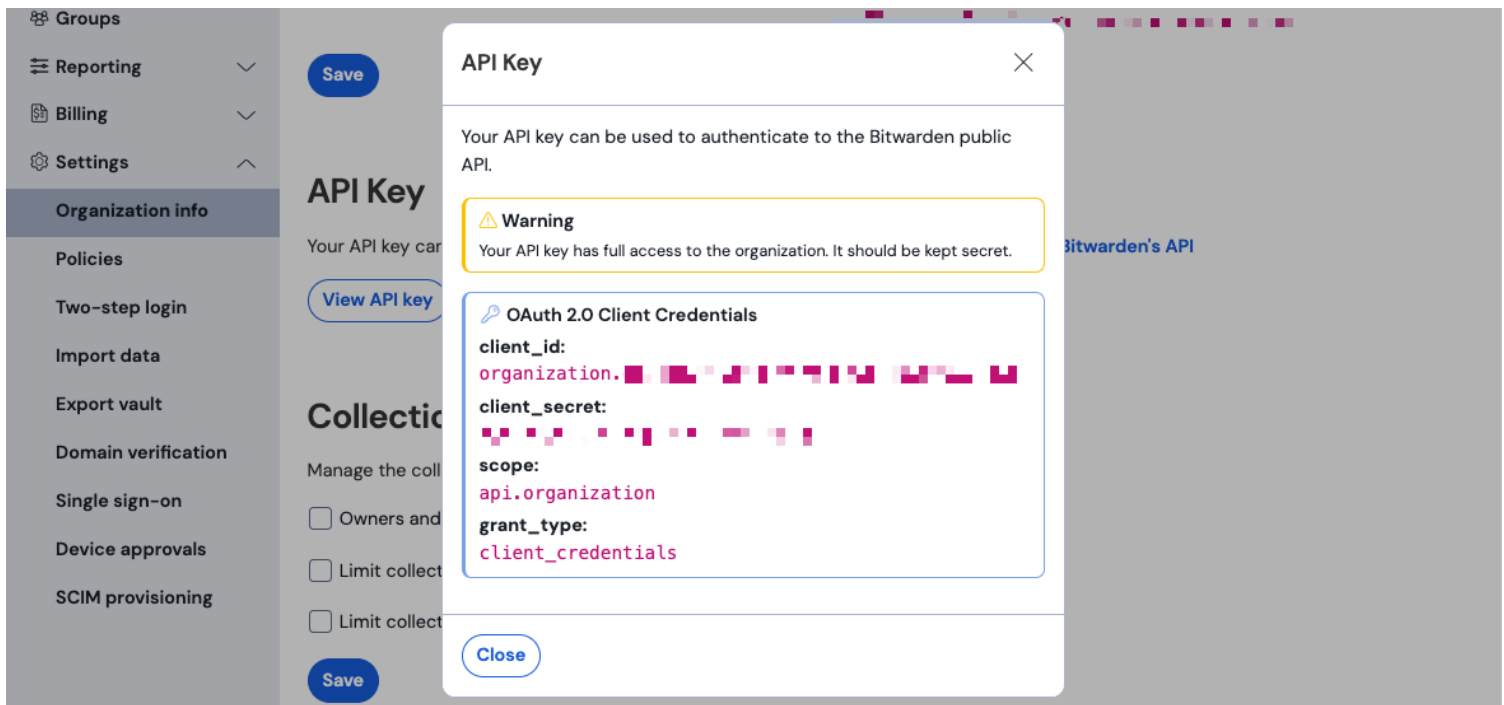
At this point in the setup, you will be required to return to your Bitwarden web vault in order to retrieve the values for **Client ID** and **Client Secret**.

1. To access your Bitwarden organization's `client_id` and `client_secret`, log in to the Bitwarden web app and open the Admin Console using the product switcher:

The screenshot displays the Bitwarden web application interface. On the left, a dark blue sidebar contains navigation links: 'Password Manager', 'Vaults', 'Send', 'Tools', 'Reports', 'Settings', 'Password Manager' (highlighted with a red box), 'Secrets Manager' (indicated by a red arrow), 'Admin Console', and 'Toggle Width'. The main content area is titled 'All vaults' and features a 'New' button and a 'BW' profile icon. Below the title is a 'FILTERS' panel with a search bar and expandable sections for 'All vaults' (listing 'My vault', 'My Organiz...', 'Teams Org...', and 'New organization'), 'All items' (listing 'Favorites', 'Login', 'Card', 'Identity', and 'Secure note'), 'Folders' (listing 'No folder'), 'Collections' (listing 'Default colle...' and 'Default colle...'), and 'Trash'. The main vault list shows four items: 'Company Credit Card' (Visa, *4242), 'Personal Login' (myusername), 'Secure Note', and 'Shared Login' (sharedusername), each with an owner indicator (e.g., 'My Organiz...' or 'Me') and a three-dot menu icon.

Product switcher

2. Navigate to your organization's **Settings** → **Organization info** screen and select the **View API Key** button. You will be asked to re-enter your master password in order to access your API key information.



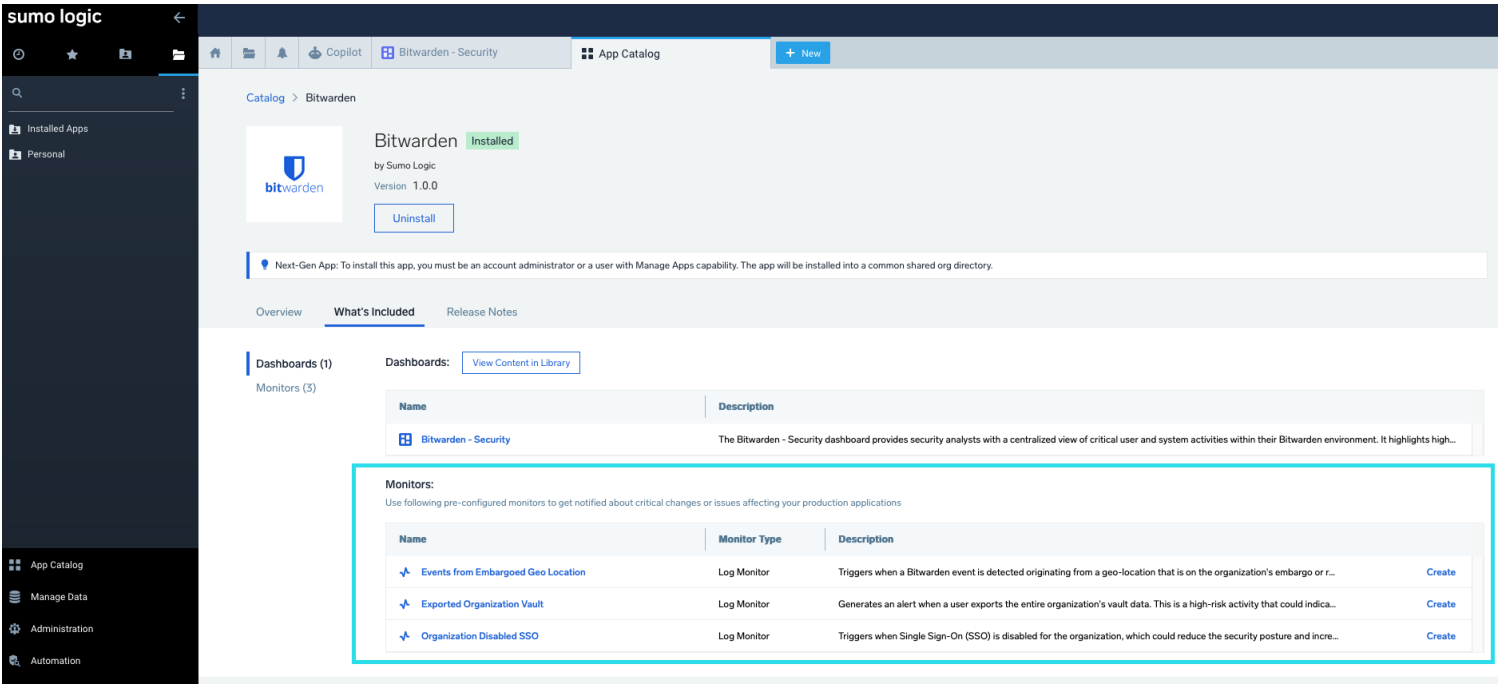
Organization api info

3. Copy and paste the `client_id` and `client_secret` values into their respective locations on the Sumo Logic **Configure Source** screen.
4. Once complete, select **Next**.

Create a monitor for Bitwarden app

The Sumo Logic Bitwarden app includes pre-configured monitors that can proactively detect threats such as data exports, compromised accounts, and policy violations. Monitors provide automated alert mechanisms that will notify you when conditions are met.

1. Return to the **App Catalog** and search and select Bitwarden app.
2. If the app is already installed, navigate to the **What's Included** tab.



create monitors

3. In the **Monitors** section, select **Create** for the per-configured monitor you with to use. Sumo Logic provides three pre-configured monitors:

- Events from Embargoed Geo Location
- Exported Organization Vault
- Organization Disabled SSO

4. On the New Monitor setup screen, set your desired monitor **Trigger Conditions**, **Alert Grouping**, and **Trigger Types**.

New Monitor



1 Trigger Conditions

Choose Logs, Metrics, or SLO, enter or select a query, and set thresholds to trigger alerts.

Monitor Type

Logs

Metrics

SLO

Detection Method

Static

Anomaly

Query

#A



```
_sourceCategory=source-category-1
| json "actingUserName", "date", "object", "type", "typeName",
"ipAddress", "deviceName", "actingUserEmail" as user_name, date, object,
event_code, event_name, ip, device_name, user_email
| lookup event_name from https://sumologic-app-data.s3.us-east-1.amazonaws.com/
bitwarden_events.csv on event_code=event_code

| where isValidIPv4(ip) or isValidIPv6(ip)
| where !isNull(ip)
| if(isValidIPv4(ip), if(!isPrivateIP(ip), true, false), true) as is_public
| where is_public
```

Trigger alerts on

returned row count

Numeric Value

Alert Grouping

☒ One alert per monitor ☐ One alert per Choose field/(s) from the dropdown or enter them manually

Trigger Type

Critical

Warning

Missing Data

☒ Alert when result is greater than 0 within 1 Hour | Evaluate every 2 Minutes ? Edit recovery settings

Recover automatically when result is less than or equal to 0 within a 1 hour window, for 1 Hour consecutively

Historical Trend

🕒 -3d

10 -

Cancel

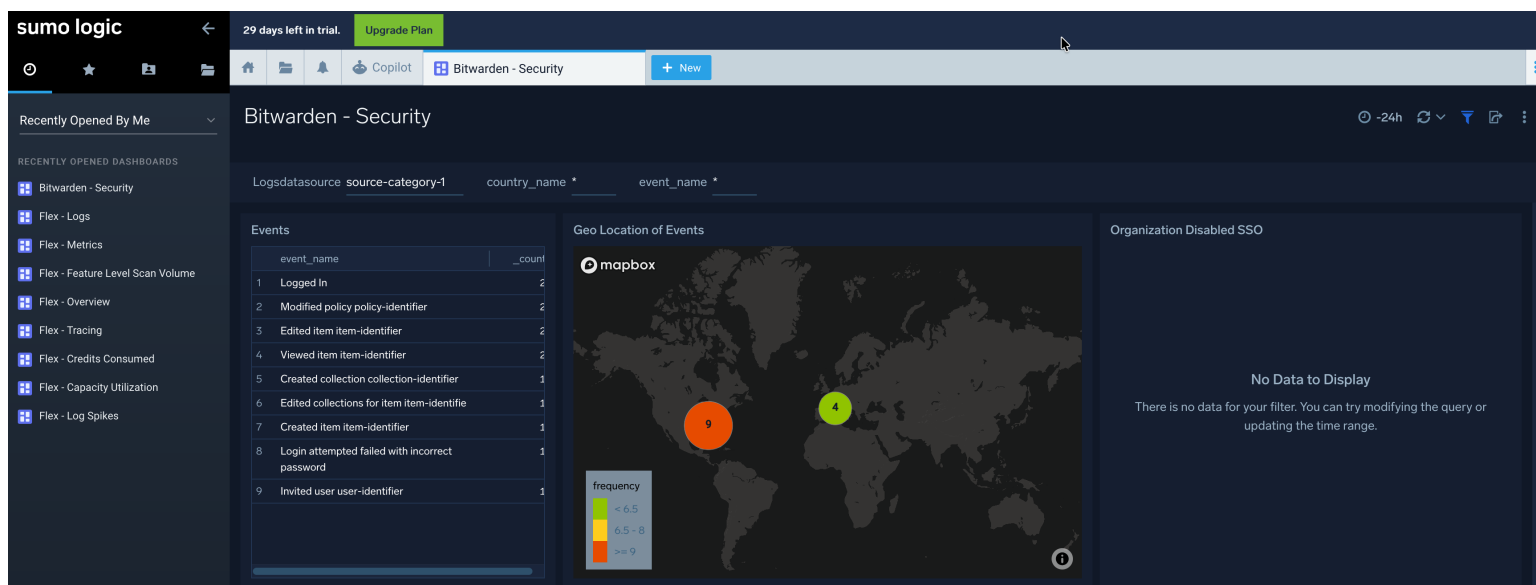
Save

Setup monitor

5. Select **Save** once you have configured the monitor.

Start monitoring data

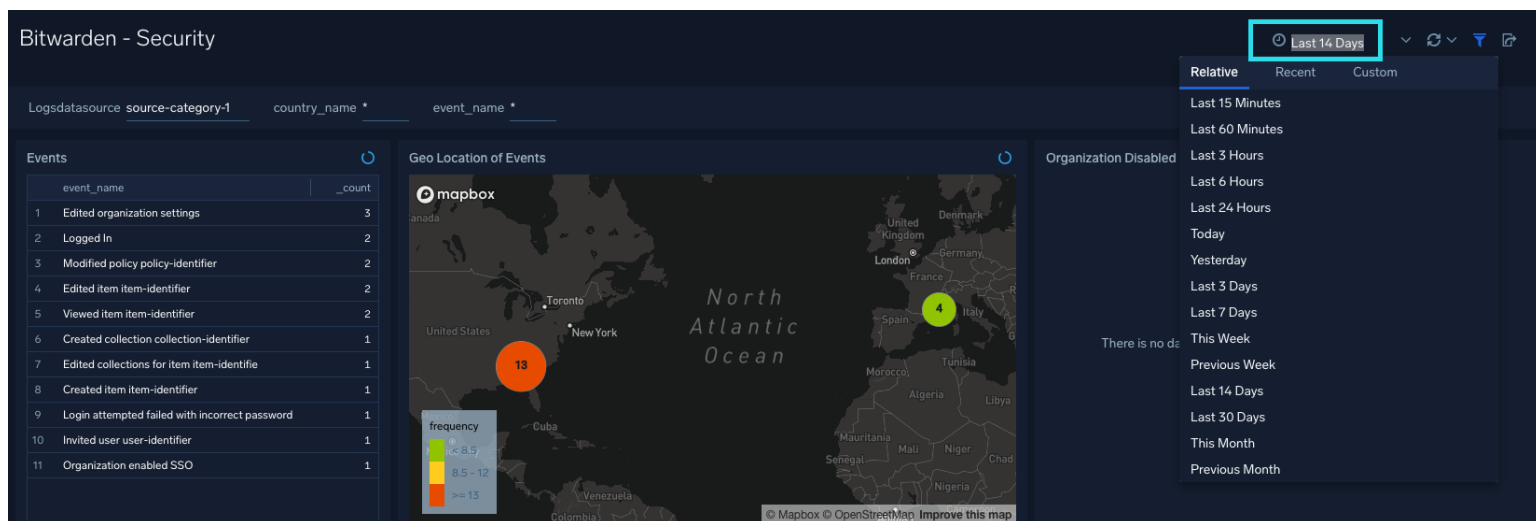
Once the app setup is complete, you may open the Sumo Logic dashboard and begin monitoring data. On Sumo Logic, select **Dashboards** and open the **Bitwarden - Security** dashboard. The security dashboard will allow you to visualize data gathered from Bitwarden event logs. A full list of Bitwarden event logs can be located [here](#).



Sumo Logic Bitwarden Dashboard

Timeframe

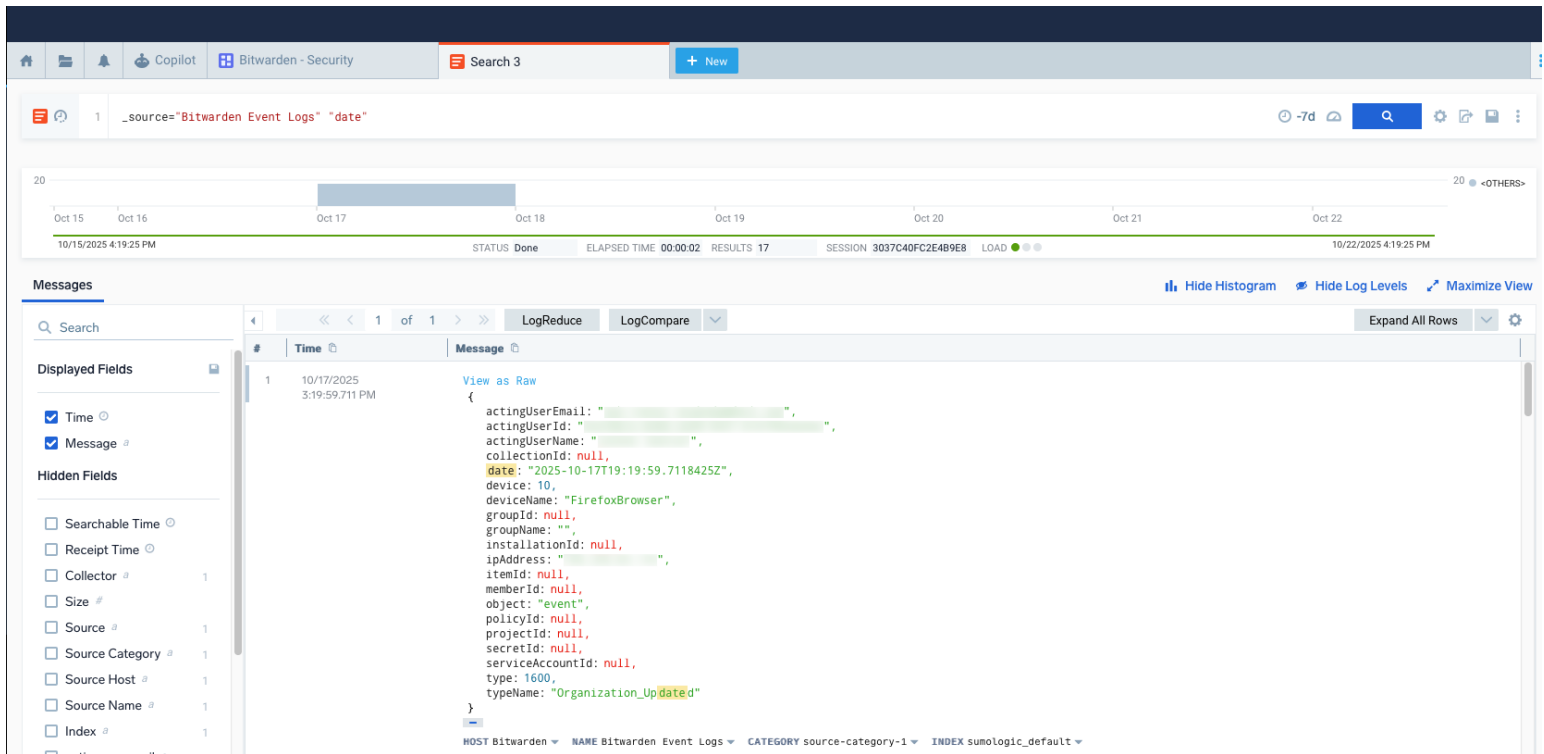
You may filter the dashboard results using the tool bar located at the top right of the dashboard. Select the to filter by timeframe:



2025-10-22 11:17:47

Sample query

You may query Bitwarden event logs on the sumo logic dashboard. Bitwarden events arrive in JSON format. An example event query may look like this:



The screenshot displays the Bitwarden Security interface with a Sumo Logic query results page. The query is `_source=Bitwarden Event Logs` with a filter on `date`. The results show a single event log entry for `Organization Updated` on 10/17/2025 at 3:19:59.711 PM. The interface includes a timeline view, a search bar, and a list of displayed and hidden fields.

Sumo Logic Simple Query

Sample query structure:

Plain Text

```
_sourceCategory=source-category-1
| json "actingUserName", "date", "object", "type", "typeName", "ipAddress", "deviceName", "actingUser
Email" as user_name, date, object, event_code, event_name, ip, device_name, user_email
| lookup event_name from source on event_code=event_code
| lookup latitude, longitude, country_name, country_code from geo://location on ip = ip
```

To learn more about advanced queries on Sumo Logic, please see the [Sumo Logic Query Language documentation](#).