RESOURCE CENTER

Monitor Bitwarden events using Splunk for SIEM Management

Learn how Bitwarden and Splunk integrate together to provide security information and event management (SIEM) for defense against malicious attacks and network breaches.

Get the full interactive view at https://bitwarden.com/sv-se/resources/monitor-bitwarden-events-using-splunk-for-siem-management/

bitwarden

Splunk is a security and observability tool used to provide visibility on large amounts of data for multi-cloud and on-premise deployments. The solution delivers insights on critical metrics such as uptime, anomalies, outages, suspicious activity, and more. With these cloud observability insights, Splunk can detect malicious activity and notify IT, DevOps, and SRE teams when a data security event occurs.

Bitwarden and Splunk integrate together to provide security information and event management (SIEM) for defense against malicious attacks and network breaches. SIEM technology identifies potential threats to online applications, while also providing compliance and security management for cloud infrastructure data in near real-time. This is achieved by logging a collection of detailed events that occur across various data sources.

With Bitwarden and Splunk, detailed information on activity across password management activity can be gathered and displayed in visual dashboards for easy monitoring. Together, the two integrate to provide valuable insights into a given Bitwarden organization, including information such as user activity, password changes, shared passwords, and more. Combined with monitoring of other infrastructure, apps, and networking, Splunk provides a holistic view of company security.

Table of Contents

The benefits of Bitwarden and Splunk together

Integration Details: The official Bitwarden Splunk app

The benefits of Bitwarden and Splunk together include

- Alerts for suspicious activity and detailed reports from Bitwarden logs
- Expands SIEM oversight to website and application credentials
- Visual dashboards and event search macros for easy monitoring
- Records of specific credential access by users
- Insights into user adoption of company security tools
- Offboarding reports that list credentials a former employee had access to, ensuring tighter security and access control

Did you know?

Bitwarden records more than 60 types of events that are logged in perpetuity and can be passed to Splunk for analysis and integration into existing security systems.

Integration Details: The official Bitwarden Splunk app

Bitwarden integrates easily into Splunk Enterprise self-hosted, Splunk Cloud Classic, and Splunk Cloud Victoria installations through the official Bitwarden Event Logs app available in the user interface. The app entry can also be found on Splunkbase**.** Follow the steps in the Splunk SIEM integration documentation from the Bitwarden Help Center. Once your Bitwarden organization is connected to Splunk, three pre-built dashboards will populate: Authentication Events, Vault Item Events, and Organization Events. Other custom dashboards can be built to make use of this data.

Alternatively, use Bitwarden API integration to set up SIEM functionality by exporting event data from your organization. The Public API can provide information about your organization and users. The Vault Management API provides access to information about encrypted data and is hosted within the Bitwarden CLI client using the `serve` command on an owned endpoint. Combined, these two APIs will provide a full view of your organization and vault.

Additional Resources

- Using Splunk with Bitwarden
- Event Logs
- Event Logs in Onboarding and Succession
- Splunk SIEM
- Bitwarden Public API
- Bitwarden Vault Management API