

^{管理者コンソール > レポート} Microsoft Sentinel SIEM

ヘルプセンターで表示: https://bitwarden.com/help/microsoft-sentinel-siem/

Microsoft Sentinel SIEM

Microsoft Sentinel is a security information and event management (SIEM) platform that can be used to monitor Bitwarden organizations. Organizations can monitor event activity with the Bitwarden Event Logs app on Microsoft Sentinel.

Setup

To setup the Bitwarden integration, an active Azure account with access to a Microsoft Sentinel Workspace is required. Additionally, a Bitwarden API key, which can only be retrieved by organization owners.

Install the Bitwarden app to your Microsoft Sentinel dashboard

The Bitwarden Event Logs application can be located in the Microsoft Azure Marketplace. To add the new application to your Workspace:

1. Choose the Bitwarden Event Logs plan from the dropdown menu and select Create.

Microsoft Azure

Home > Marketplace >

Bitwarden Event Logs >> ...

Bitwarden Inc.

Bitwarden Inc. | Azure Application

Plan

Bitwarden Event Logs >> (Create)

2. Complete the required fields and select the Workspace that will be monitoring Bitwarden organization data.

3. Once complete, select Review + create.

Connect your Bitwarden Organization

Once the Bitwarden Event Logs app has been added to your Microsoft Sentinel Workspace, you can connect your Bitwarden organization using your Bitwarden API key.

1. Return to the **Data connectors** screen and select the Bitwarden Event Logs app. Select **Open connector page**. If the Bitwarden Event Logs app is not visible, you may be required to select *C* **Refresh**.

Microsoft Sentinel Selected workspace: "bw-event-logs"	Data con	nectors				×
	🕐 Refresh	<section-header> Guides & Feedback</section-header>				
✓ General	1	47 0	More content at			
Overview (Preview)	Connectors	•	Content hub			
₽ Logs						3
🌰 News & guides	Search I	by name or provider	Providers : Bitwarden Inc Data Types : All Status	Bitwarde	n Event Logs	
	y- search	by name of provider				
arsigma Threat management	Status	Connector name 1		- Status	Sitwarden Inc Provider	Contraction
Incidents	Status					
2 Workbooks		Bitwarden Event Logs Bitwarden Inc		 Description This connector prov	vides insight into activ	vity of your
Hunting		bitwarden nic		Bitwarden organiza	tion such as user's act 2fa, etc.), cipher activ	tivity (logged in,
Notebooks					hared, etc.), collection	
Entity behavior				-	y, and more.	
Threat intelligence				Last data received		
MITRE ATT&CK					Manalaa	
(Preview)				Content source () Bitwarden	Version 1.0.0	
SOC optimization				Author	Supported	l hu
✓ Content management				Bitwarden	Bitwarden	
Content hub				Related content		
 Repositories (Preview) 					↔ 0 ▲ 0	
s Community						rtics rules templates
\vee Configuration						
Workspace manager (Preview)				Data received		Go to log analytics
Data connectors				3-		
Analytics				2-		
Summary rules (Preview)						
Watchlist				Open connecto	r page	
		M	icrosoft Sontinal Pitwardon Evant Lago ann			

Microsoft Sentinel Bitwarden Event Logs app

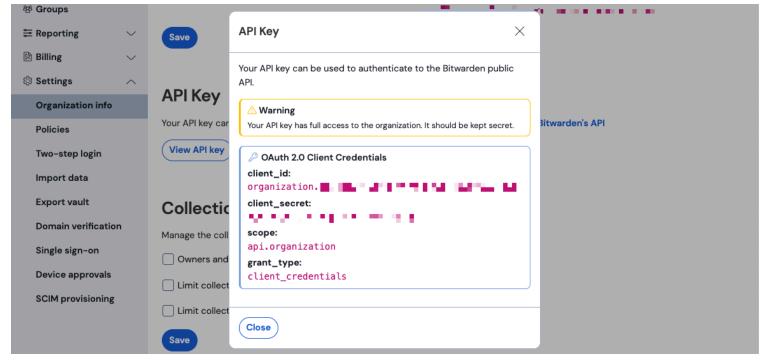
2. Keep this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:

D Password Manager	All vaults			New >> 🐯	BW
🗇 Vaults	FILTERS 🕜		Name	Owner	:
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	AZIV	Company Credit Card Visa, *4242	My Organiz	:
æ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	A My vault My Organiz :	0 6	myusername	Me	:
	 Teams Org : + New organization 		Secure Note	Me	:
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 	0 Ø	Shared Login sharedusername	My Organiz	÷
 Password Manager Secrets Manager 	 Folders No folder Collections Default collections 				
	Default colle				
🖉 Admin Console	🖻 Trash				
🖞 Toggle Width					

- *製品-スイッチャー*
- 3. 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.

Secure and trusted open source password manager for business

D bit warden



組織API情報

4. Return to the Microsoft Sentinel tab. On the **Configuration** page, complete the following fields:

Field	Value
Bitwarden Identity URL	For Bitwarden cloud users, the default URL will be https://identity.bitwarden.com or https://ident ity.bitwarden.eu. For self-hosted Bitwarden users, input your self-hosted URL. For example, https:// <self-hosted-url>/i dentity. Be sure that the URL does not include any trailing forward slashes at the end of the URL "/".</self-hosted-url>
Bitwarden API URL	For Bitwarden cloud users, the default URL will be https://api.bitwarden.com or https://api.bitwarden.eu. For self-hosted Bitwarden users, input your self-hosted URL. For example, https:// <self-hosted-url>/a pi. Be sure that the URL does not include any trailing forward slashes at the end of the URL "/".</self-hosted-url>
Client ID	Input the value for client_id from the Bitwarden organization API key window.
Client Secret	Input the value for client_secret from the Bitwarden organization API key window.

Select **Connect** once the required fields have been completed.

(i) Note

あなたの組織のAPIキー情報は、機密データです。これらの値を非セキュアな場所で共有しないでください。

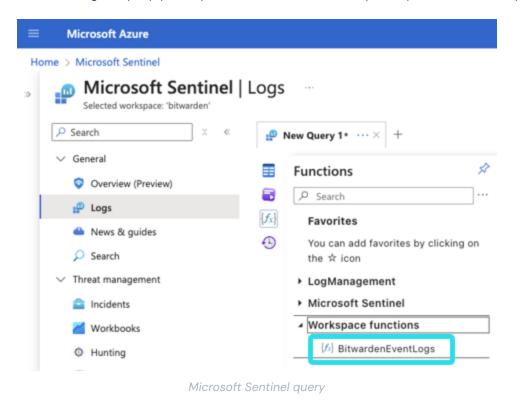
Start monitoring event logs

(i) Note

Historic event data is not available for the Bitwarden Event Logs app on Microsoft Sentinel at this time. Additionally, it may take up to 1 hour for the first events to appear in Microsoft Sentinel.

Bitwarden organization event logs can be viewed in Microsoft Sentinel using the BitwardenEventLogs query function.

- 1. From Microsoft Sentinel, select Logs. A New Query tab will be created. On the left hand navigation, select Functions → Workspace functions → BitwardenEventLogs.
- 2. Before running the query, you may select time frame and add specific parameters to the query. To being the query, select Run.



Queries can be saved for future use.

Microsoft Sentinel	Logs										
Selected workspace: 'bitwarden'	LOGS										
♀ Search × ≪	: ⁰ New Query 1* ···· × +									🗟 Save 🗸 🏥 Share 🗸 \cdots	ST Over
 General 	ip New Query I* ···· × +										
 Overview (Preview) 	E Run Time range : L	ast 7 days Limit : 1000	0								KQL mode
	BitwardenEventLogs										
₽ Logs	{A}										
News & guides	-										
🔎 Search											
 Threat management 											
Incidents											
🞽 Workbooks											
Hunting	Results Chart 🕅 Add bo										
Notebooks	□ TimeGenerated [UTC] [↑] ↓	eventType	itemId	groupId	actingUserId	device	ipAddress	Туре	deviceName	eventTypeName	actin
🥜 Entity behavior	> 10/9/2024, 1:41:34.313 PM	1402				9		BitwardenEventLogs_CL	Chrome Browser	Group_Deleted	
Threat intelligence	> 10/9/2024, 1:41:30.397 PM	1401				9		BitwardenEventLogs_CL	Chrome Browser	Group_Updated	
MITRE ATT&CK (Preview)	> 10/9/2024, 1:41:12.765 PM	1107				9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
SOC optimization	> 10/9/2024, 1:41:11.466 PM > 10/9/2024, 1:41:08.698 PM	1101		-	1 A A A A	9	1 A 40	BitwardenEventLogs_CL BitwardenEventLogs_CL	Chrome Browser Chrome Browser	Cipher_Updated Cipher_ClientViewed	1.1
 Content management 	> 10/9/2024, 1:41:08:698 PM	1000		-		9		BitwardenEventLogs_CL	Chrome Browser	User_LoggedIn	
Content hub	> 10/8/2024, 1:40:37:288 PM					9		BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
-	> 10/8/2024, 12:58:45.879 PM					9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
 Repositories (Preview) 	> 10/8/2024, 12:56:02.933 PM					9	-	BitwardenEventLogs_CL	Chrome Browser	Cipher_Updated	
4 Community	> 10/8/2024, 12:55:59.947 PM					9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
 Configuration 	> 10/8/2024, 12:55:57.232 PM		11 11 1			9		BitwardenEventLogs_CL	Chrome Browser	Cipher_ClientViewed	
Workspace manager (Preview)	0			_			_				
Data connectors											
Analytics											
Summary rules (Preview)											
🔄 Watchlist											
🍪 Automation											
Settings											

Microsoft Sentinel query result

Monitor using Workbooks

Workbooks can be used to review event logs and visualize data. Additionally, templates are included in the Bitwarden Event Logs Workbook for a pre-configured overview of available data.

To access Workbooks, select **Workbooks** from the navigation and then **Templates**.

Home > Microsoft Sentinel

♀ Search × «	🖒 Refresh 🕂 Add	Workbook 🛛 🛜 Guid	es & Feedback						
✓ General	0	<i>#</i> 3	① 0	More content at					
Overview	My workbooks	Templates	Updates	Content hub					
₽ Logs									
🜰 News & guides	My workbooks Ter	nplates				🞽 Bitwarden Orga	nization Events		
🔎 Search	🔎 Search		√ Add filter			<u> </u>			
✓ Threat management	Name			Status	Source name				
Incidents						Description This workbook provides insights on Bitwarden Organiz			
🞽 Workbooks	Bitwarden Authen				Bitwarden	Event Logs.			
Hunting	Bitwarden Organiz				Bitwarden	Content source () Bitwarden	Template version 1.0.0		
Notebooks	Bitwarden Vault Ite	ems Events			Bitwarden				
🔗 Entity behavior						Author Bitwarden	Supported by Bitwarden Inc Email		
Threat intelligence									
MITRE ATT&CK (Preview)									
SOC optimization (Preview)									
 Content management 									

Workbook templates

The Bitwarden Event Logs app will have three templates included by default. Select one of the templates and choose **View Template** to begin monitoring data.

My workbooks	Templates			
🔎 Search		√ Add filter		
Name			Status	Source name
Bitwarden Au	uthentication Events			Bitwarden
Bitwarden O	rganization Events			Bitwarden
Bitwarden Va	ult Items Events			Bitwarden

Included templates

The dashboards include visualized data:



Time: Last 14 days ∨ Successful Log In Attempts by Country



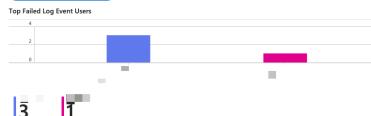
Polan 2 1

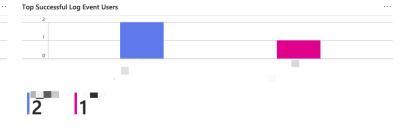


Microsoft Sentinel dashboard view

Continue scrolling the overview page for additional event log data:

Top Users By: User Name ∨





Latest Authentication Events

3

TimeGenerated	↑↓ eventType↑↓ itemId ↑↓	↓ collectionId ↑↓ groupId ↑↓ p	oolicyId ↑↓ memberId↑↓ actingUserId	↑↓ installation	ld ↑↓ device↑↓	ipA ↑↓	TenantId	
5/19/2024, 11:36:30.951 PM	1006				2			
5/19/2024, 11:36:16.556 PM	1006		10 M 10 M 10 M		2			
5/16/2024, 2:03:05.447 PM	1000		10 M 10 M 10 M		9		10 M	
5/16/2024, 2:03:55.748 PM	1005		10 M		9		10 M	
5/16/2024, 6:00:29.614 PM	1000		10 M		9		10 M	
5/17/2024, 9:11:59.709 PM	1005		100.00		1		10 M	
5/21/2024, 9:34:05.581 PM	1000		1000		2			

Bitwarden even log view