Microsoft Sentinel × **Am I Being Pwned**

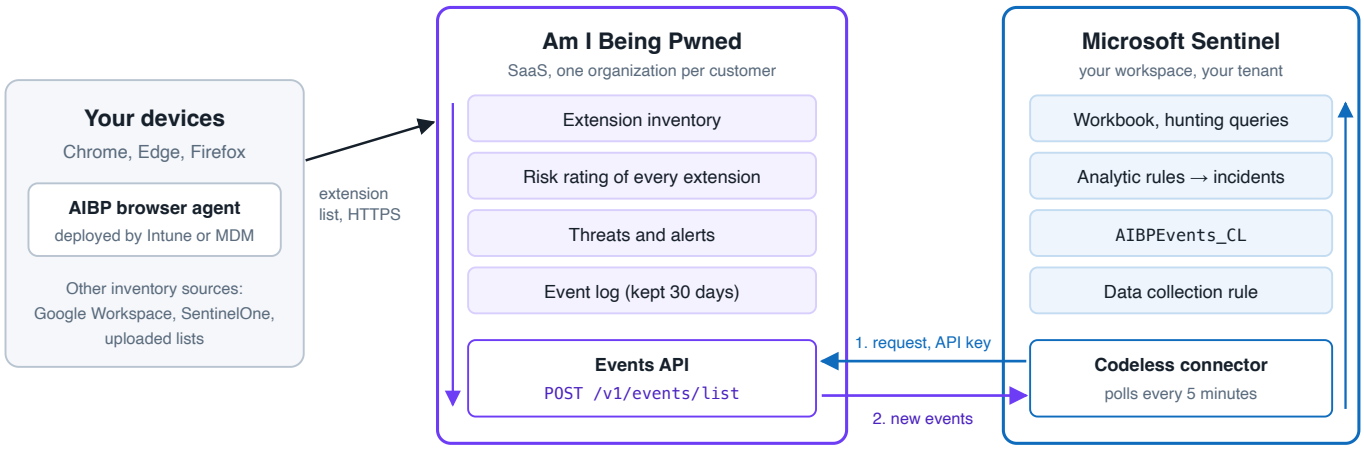
How the integration works

What flows between the two products, who starts each call, and what each side can do.

v1 · November 2026
amibeingpwned.com

The gap. Browser extensions run with access to every page a user opens, including sign-in pages, and most endpoint tools do not see them. Am I Being Pwned (AIBP) inventories the extensions on your devices, rates each one, and raises an alert when one turns risky or malicious. The Sentinel solution brings those alerts into your workspace, where they become incidents next to the rest of your security data.

1. System map



Sentinel starts every call. AIBP never connects to your workspace and holds no Azure credentials.

2. What arrives in Sentinel

Each event is one row in `AIBPEvents_CL`. The data collection rule pulls the fields you filter on into columns (extension, severity, device, user) and keeps the full event in `Data`.

EVENT	WHEN IT FIRES	RULE SHIPPED WITH THE SOLUTION
`alert.raised`	An extension in your fleet needs attention. Tier: urgent, action or blocked.	**Urgent extension alert**: High, one incident per alert, checked every 15 minutes.
`threat.detected`	A malicious extension is found on your devices.	**Malicious extension on many devices**: High, when it is on 10 or more.
`threat.resolved`	A threat closed in AIBP: no device still runs the extension, or someone closed it.	None. The workbook and hunting queries use it.
`device.uninstalled`	The AIBP browser agent was removed from a device, so that browser is no longer watched.	**Browser agent removed**: Medium, mapped to the user (Account) and the computer (Host).

Access and data.

- The connector uses one AIBP API key with a single, read-only scope, `events:read`. It can read your org's events and nothing else. Revoke it on the API tab at any time.
- Events carry extension details, alert reasons and, for agent removals, the device id, computer name and user email. Events carry no browsing history or page content.
- All traffic is HTTPS. AIBP keeps events for 30 days; Sentinel keeps them for your workspace's retention period.

3. Working with the data

ALERT TIERS

`urgent`	An extension that can steal logins or run remote code is running, and nothing has stopped it.
`action`	Someone needs to do something, for example a block that is not taking effect.
`blocked`	AIBP blocked an extension. Users may notice it is gone.

OTHER COLUMNS

`AlertReason`	why it is at that tier
`StealsLogins, RemoteCode`	what the extension can do
`IssueState`	running, block_sent, stopped
`InstallCount`	installs across your fleet
`IdentityEmail, MachineName`	who and where, on agent removals

STARTER QUERIES `KQL`

Extensions that can steal logins or run code

```
AIBPEvents_CL
| where TimeGenerated > ago(30d)
| where EventType == "alert.raised"
| where StealsLogins or RemoteCode
| summarize Installs = max(InstallCount),
    LastAlert = max(TimeGenerated)
    by ExtensionId, ExtensionName
| sort by Installs desc
```

Users whose agent was removed more than once

```
AIBPEvents_CL
| where EventType == "device.uninstalled"
| summarize Removals = dcount(EventId),
    Machines = make_set(MachineName)
    by IdentityEmail
| where Removals > 1
```

4. Responding to an extension incident

1 · SENTINEL
Incident opens
It names the extension, why it fired and how many installs there are.

→

2 · AIBP
Investigate
See what the extension does and which devices and users run it.

→

3 · AIBP
Block it
The block goes out through Intune, Google Workspace or your MDM.

→

4 · AIBP
Threat closes
Once no device still runs it. A stuck block raises a new alert.

> **Agent removed?** Check with the user (`IdentityEmail`) whether the device (`MachineName`) was retired or reimaged. If not, redeploy the agent: until it is back, AIBP cannot see that browser's extensions.

5. Getting started

1. In AIBP, an org admin opens **Integrations**, **Microsoft Sentinel** and selects **Create key**. The key can only read events.
2. In Sentinel, install **Am I Being Pwned** from the **Content hub**.
3. Open **Data connectors**, paste the key, select **Connect**.
4. Under **Analytics**, enable the rule templates named "AIBP".

GOOD TO KNOW

- Events arrive within about 10 minutes. There is no backfill.
- One row per alert, detection or agent removal, never per page view, so ingestion stays small.

BUYING THROUGH THE SECURITY STORE

- Priced per device, billed by Microsoft. Change the count in the Microsoft 365 admin center.
- 30 days' grace for devices over your count. Cancel and you keep your data on the Free plan.

Questions: support@amibeingpwned.com