harmonic | Harmonic Protect

Harmonic Protect:

The control you need to unlock AI across your company

Uncover Shadow AI Use and Gain Control

Security teams want to find ways to safely enable Generative AI use while managing the associated data privacy risks.

Product Overview

Harmonic empowers security teams to fully understand how their organization uses GenAI, while safeguarding sensitive data from leaking into GenAI or GenAI-enabled SaaS. Our small language models are specialized for detecting structured and unstructured sensitive data. Harmonic then interacts with the end-user at the point of data loss, helping to avoid sensitive data leaking while coaching end users toward the secure use of AI.

Confidently Adopt GenAI

With Harmonic, security teams can confidently support the secure adoption of Generative AI and stay ahead of emerging compliance requirements. Harmonic is the “easy button” for GenAI data protection. There is no need for complicated regex rules. No need to train on customer data. No drowning in false positives.

Key Features

Continuously identify shadow AI, including employee use of GenAI-enabled SaaS.

Prevent sensitive data leakage in GenAI, including structured and unstructured data types.

Improve user awareness, by coaching users at the point of data loss.

Report on secure GenAI adoption, with Harmonic’s built-in insight pages.

Why People Love Harmonic

Catch data you actually care about. Go beyond PII-matching and regex to identify your real crown jewels.

Ditch the labels. Catch and identify sensitive data at the point of data loss, even if it isn’t categorized.

Easy to deploy & run. Simply roll out to all browsers within 30 minutes.

Wow end-users. Deliver an experience that will engage end-users, not drive them away.

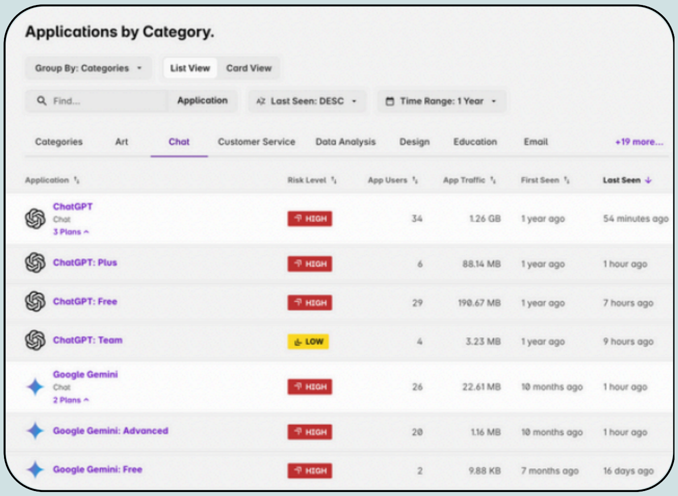
Insights in GenAI Usage

It's a challenge for organizations to gain true visibility into employee AI usage—not just *which* tools are being accessed, but *how* they're being used, what sensitive data is being exposed, and whether subscription plans allow that data to be used for training. This becomes critical as most SaaS tools now embed GenAI capabilities, while a growing number of compliance frameworks demand comprehensive 'AI Asset Inventories.

Strict approaches to ban or limit GenAI are met with resistance by end users, who go to extreme lengths to circumvent controls to get their hands on a variety of tools.

With Harmonic, you can:

- Pinpoint use of Shadow AI and unsanctioned apps;
- Detect high-risk apps training on your data;
- Get prompt-level visibility of *how* AI tools are being used



Application	Risk Level	App Users	App Traffic	First Seen	Last Seen
ChatGPT Chat 3 Plans	HIGH	34	1.26 GB	1 year ago	54 minutes ago
ChatGPT: Plus	HIGH	6	88.14 MB	1 year ago	1 hour ago
ChatGPT: Free	HIGH	29	190.67 MB	1 year ago	7 hours ago
ChatGPT: Team	LOW	4	3.23 MB	1 year ago	9 hours ago
Google Gemini Chat 2 Plans	HIGH	26	22.61 MB	10 months ago	1 hour ago
Google Gemini: Advanced	HIGH	20	1.16 MB	10 months ago	1 hour ago
Google Gemini: Free	HIGH	2	9.88 KB	7 months ago	16 days ago

Harmonic Category Detail Screen

Prevent Sensitive Data Leakage into GenAI

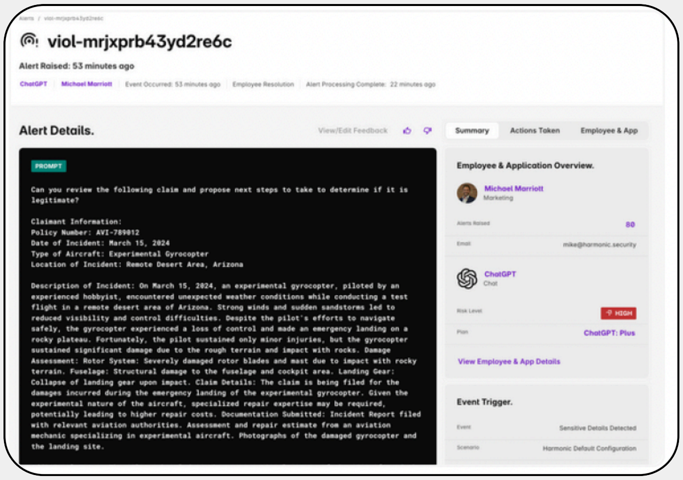
At the core of Harmonic's solution is a suite of small language models. These models can analyze sensitive data in structured, unstructured, and semi-structured datasets.

The models are capable of assessing far greater context than traditional tools, which means they can be far more accurate than writing regular expressions. With the context assessed, the models are capable of making human-like decisions about whether that data should be leaving the business.

These models are trained on Harmonic's unique set of publicly leaked data, which has been cleaned and anonymized. According to an independent analysis by ESG, the models have 96% fewer false positives when compared with traditional, regex-based approaches.

This accuracy and speed of these models enables security teams to engage directly with end users, significantly taking the load off the security team.

The full context of all activities is also available within the Harmonic portal, where we combine activity with context from your identity provider to provide a richer picture of user activity.



viol-mrjxprb43yd2re6c

Alert Raised: 53 minutes ago

ChatGPT | Michael Marriott | Event Occurred: 53 minutes ago | Employee Resolution | Alert Processing Complete: 22 minutes ago

```
Can you review the following claim and propose next steps to take to determine if it is
legitimate?

Claimant Information:
Policy Number: AVI-789012
Date of Incident: March 15, 2024
Type of Aircraft: Experimental Gyrocopter
Location of Incident: Remote Desert Area, Arizona

Description of Incident: On March 15, 2024, an experimental gyrocopter, piloted by an
experienced hobbyist, encountered unexpected weather conditions while conducting a test
flight in a remote desert area of Arizona. Strong winds and sudden sandstorms led to
reduced visibility and control difficulties. Despite the pilot's efforts to navigate
safely, the gyrocopter experienced a loss of control and made an emergency landing on a
rocky plateau. Fortunately, the pilot sustained only minor injuries, but the gyrocopter
sustained significant damage due to the rough terrain and impact with rocks. Damage
Assessment: Rotor System: Severely damaged rotor blades and mast due to impact with rocky
terrain. Fuselage: Structural damage to the fuselage and cockpit area. Landing Gear:
Collapse of landing gear upon impact. Claim Details: The claim is being filed for the
damages incurred during the emergency landing of the experimental gyrocopter. Given the
experimental nature of the aircraft, specialized repair expertise may be required,
potentially leading to higher repair costs. Documentation Submitted: Incident Report filed
with relevant aviation authorities. Assessment and repair estimate from an aviation
mechanic specializing in experimental aircraft. Photographs of the damaged gyrocopter and
the landing site.
```

Employee & Application Overview.

Michael Marriott
Marketing

Alerts Raised: 80

Email: mike@harmonic.security

ChatGPT
Chat

Risk Level: HIGH

Plan: ChatGPT: Plus

Event Trigger.

Event: Sensitive Details Detected

Scenario: Harmonic Default Configuration

Harmonic Alert Detail Screen

Coach Users at the Point of Data Loss

Security teams are realizing that blocking GenAI tools is not enough; employees will use these tools regardless. By enabling end users to use these tools while nudging them against exposing sensitive data, security teams have a way to enable the business' AI use.

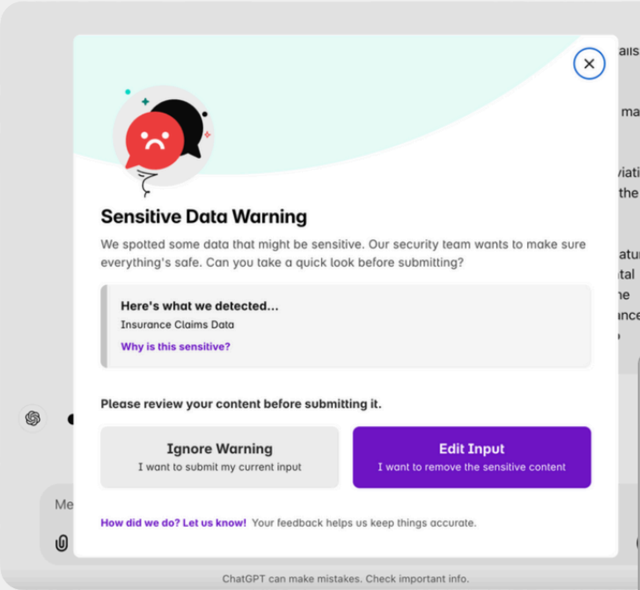
Harmonic's models are exceptionally fast, making accurate assessments within 200 milliseconds. This is 300 times quicker than if you were to use an LLM like ChatGPT.

When we detect sensitive data, we intercept the prompt before it is exposed and give the end user context to understand what is sensitive and how they can remove the sensitive data.

The intervention model is fully customizable in how end users may be nudged:

- Prompt user to edit, block, ignore, or redirect;
- Link to internal policies or documents;
- Define which users can upload sensitive data types to specific GenAI apps;
- Customize text, colors, and logo.

This helps to engage with users where they are at, minimizing friction and encouraging secure adoption of GenAI.



Sensitive Data Warning

We spotted some data that might be sensitive. Our security team wants to make sure everything's safe. Can you take a quick look before submitting?

Here's what we detected...
Insurance Claims Data
Why is this sensitive?

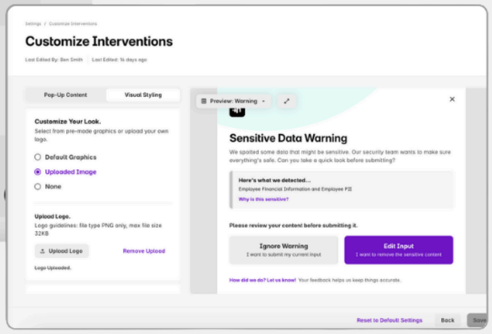
Please review your content before submitting it.

Ignore Warning
I want to submit my current input
Edit Input
I want to remove the sensitive content

How did we do? Let us know! Your feedback helps us keep things accurate.

ChatGPT can make mistakes. Check important info.

Customizable Model Displayed to End Users



Customize Interventions

Last Edited By: Ben Smith | Last Edited: 16 days ago

Customize Your Look.
Select from pre-made graphics or upload your own logo.

○ Default Graphics
● Uploaded Image
○ None

Upload Logo.
Logo guidelines: file type PNG only, max file size 32KB

Logo Uploaded.

Sensitive Data Warning

We spotted some data that might be sensitive. Our security team wants to make sure everything's safe. Can you take a quick look before submitting?

Here's what we detected...
Employee Financial Information and Employee PII
Why is this sensitive?

Please review your content before submitting it.

Ignore Warning
I want to submit my current input
Edit Input
I want to remove the sensitive content

How did we do? Let us know! Your feedback helps us keep things accurate.

Customize Interventions and Nudges

Why Harmonic?

Harmonic Protect empowers security teams to safeguard sensitive data without the need for extensive data labeling or complex rule-setting.

Your data in your hands
Our models do not need to store or train on client data. Instead, we use our unique sets of public, anonymized data.

Recognized for innovation
Harmonic was named Gartner Cool Vendor and RSA Innovation Sandbox finalist.

Scale the security team
Minimal false positives and end-user coaching minimize security team effort with our “zero-touch” approach.

> While we did understand what people were using — because we had that visibility — we didn't know how they were using it, and the data leakage was definitely a big one. ...
>
> That's when we went looking for outside help. ... It's literally hours to seconds. If we deploy a tool and it's covered by Harmonic, we have insight right away.
>
> **Mike Janielis Principal Information Security Architect**
> **Advisor360**

Getting Started with Harmonic

Getting started with Harmonic is quick and easy. Simply install the Harmonic browser extension to start gaining insights in GenAI usage and secure your sensitive data.

Within 30 minutes, the extension may be rolled out to your entire organization with Group Policy Object (GPO), Microsoft Intune, JAMF, or Kandji.

Get Started >

harmonic.security sales@harmonic.security

As every employee adopts AI in their work, organizations need control and visibility. Harmonic delivers AI Governance and Control (AIGC), the intelligent control layer that secures and enables the AI-First workforce. By understanding user intent and data context in real time, Harmonic gives security leaders all they need to help their companies innovate at pace.