eSENTIRE

DATA SHEET

eSentire MDR for GenAI Visibility

Get metric-driven visibility into your company's Generative AI (GenAI) workforce insights and application usage and monitor risks before they become business critical events.

Improve visibility and support policy development and governance

Track unauthorized use of GenAI applications and policy adherence by getting comprehensive view of your employees' GenAI use.

Understand workforce GenAI insights and identify potential risks in user interaction

Monitor GenAI application user activity, applications, user prompts, and shared files over time to observe usage surges and identify risky user interactions.

Stay updated with latest GenAI-focused threat intelligence

Understand emerging security concerns and GenAI trends so you can develop policies that promote responsible AI usage.

Your Challenges

Generative AI (GenAI) technologies are revolutionizing every aspect of modern business operations. While your organization may have defenses in place to fight against today's threats, many are unprepared for GenAI-based threats. However, inappropriate or unauthorized usage can lead to the amplification of existing cyber risks as well. For example, employees using GenAI applications can unknowingly share confidential data with the application itself, leading to potential sensitive data and intellectual property (IP) leaks.

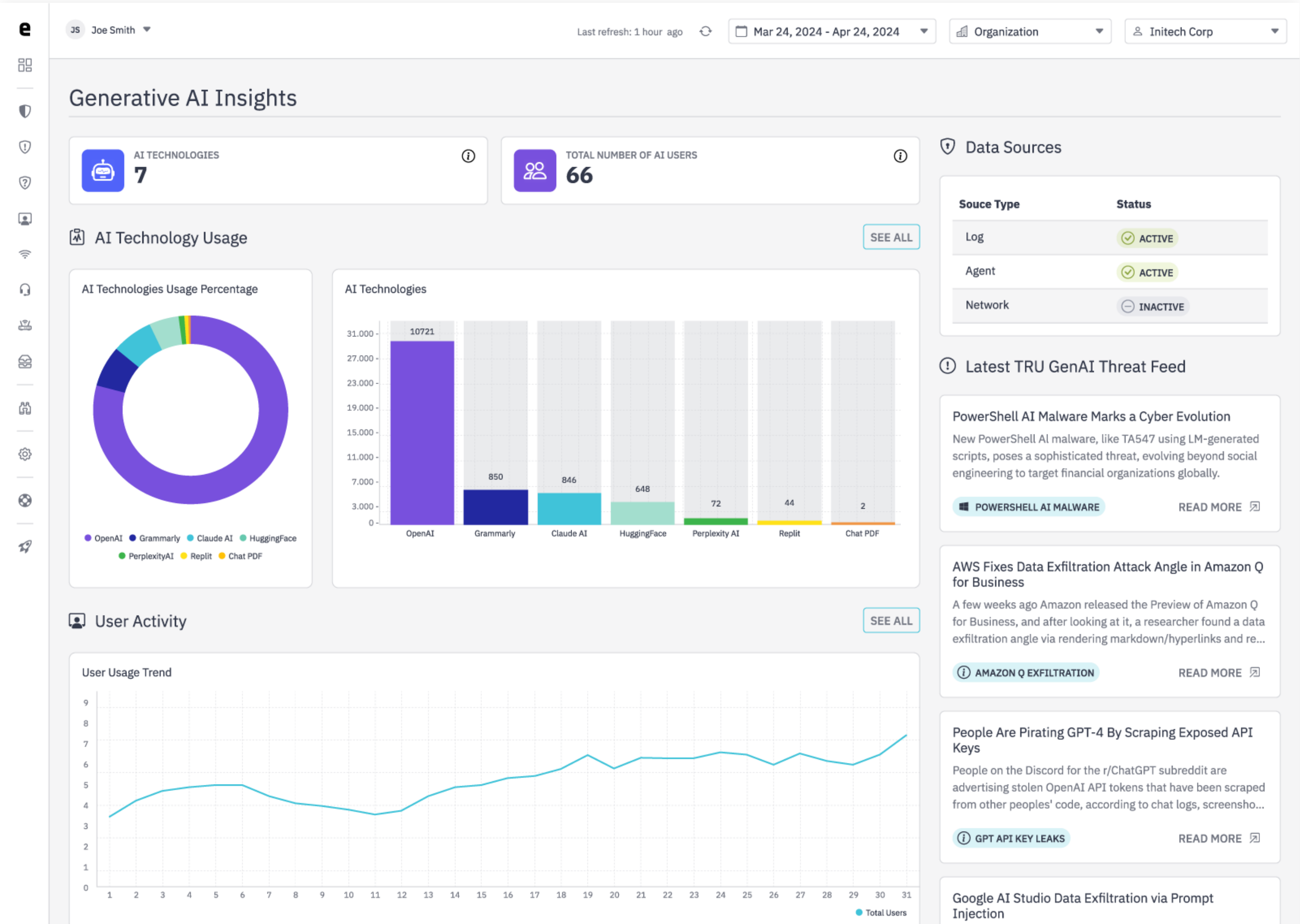
Unfortunately, many organizations don't have monitoring to put appropriate governance, risk and compliance policies in place around GenAI utilization. This lack of visibility can also lead to creating ill-informed policies and making governance decisions on GenAI usage based more around assumptions rather than data. To address these challenges, you must understand how your employees are using GenAI and have complete visibility over their user interactions.

Our Solution

eSentire MDR for GenAI Visibility provides metric-driven, comprehensive visibility into your organization’s GenAI usage, including applications, prompts, file share, trends, and more to determine potential risks. This visibility into GenAI usage offers early warnings of employees sharing sensitive information or noncompliance to corporate policies, helping monitor risks before they become business critical events.

How We Help	Your Outcomes
✓ Reduce GenAI blind spots with visibility into AI technology usage and general trends ✓ Centralize user activities to create a link between AI tools and workforce insights ✓ Know what information is being shared externally with visibility into prompts and files shared ✓ Compare workforce trends, and monitor relevant landscape developments to understand risks	✓ Protection against GenAI and LLM related threats ✓ Ability to reinforce policies and govern usage ✓ Monitor IP and data security risks to prevent sharing sensitive customer information ✓ Address ethical and legal concerns including content creation that infringes on copyright laws or perpetuates bias ✓ Understand if there is oversharing with GenAI applications to prevent compromising intellectual property and Data Loss Prevention (DLP) risks ✓ Reduce risk of publishing confidential, copyrighted, or biased information

eSentire MDR for GenAI Visibility Dashboard



Generative AI Insights

AI TECHNOLOGIES 7

TOTAL NUMBER OF AI USERS 66

AI Technology Usage

AI Technologies Usage Percentage

AI Technologies

User Activity

User Usage Trend

Data Sources

Souce Type	Status
Log	ACTIVE
Agent	ACTIVE
Network	INACTIVE

Latest TRU GenAI Threat Feed

PowerShell AI Malware Marks a Cyber Evolution

New PowerShell Al malware, like TA547 using LM-generated scripts, poses a sophisticated threat, evolving beyond social engineering to target financial organizations globally.

POWERSHELL AI MALWARE READ MORE

AWS Fixes Data Exfiltration Attack Angle in Amazon Q for Business

A few weeks ago Amazon released the Preview of Amazon Q for Business, and after looking at it, a researcher found a data exfiltration angle via rendering markdown/hyperlinks and re...

AMAZON Q EXFILTRATION READ MORE

People Are Pirating GPT-4 By Scraping Exposed API Keys

People on the Discord for the r/ChatGPT subreddit are advertising stolen OpenAI API tokens that have been scraped from other peoples' code, according to chat logs, screensho...

GPT API KEY LEAKS READ MORE

Google AI Studio Data Exfiltration via Prompt Injection

Why Choose eSentire MDR for GenAI Visibility

- ✓ **Leader in MDR:** Secure your GenAI usage by partnering with a Proven MDR provider and benefit from the real-world experience of our security experts who provide 24/7 threat detection and response and proactive, hypothesis-driven threat hunting across your entire attack surface including endpoint, network, and log data sources.

- ✓ **Pioneer in GenAI Security:** We leverage Generative AI to improve our SOC efficiency and have introduced the eSentire AI Investigator for SOC and customer use cases so you can query your security data in natural language. Now we're first to market in bringing unparalleled visibility in GenAI workforce insights to eSentire customers.

- ✓ **Reporting Flexibility:** Workforce insights are refreshed every 24hrs with latest information on your corporate GenAI usage. Reports accessible in CSV and PDF formats.

- ✓ **All-In-One MDR Solution:** Combine multiple security technologies into a single platform and get a unified view of your entire attack surface. eSentire MDR for GenAI Visibility consolidates your organization's GenAI footprint by leveraging your managed security telemetry across network, endpoint and log sources.

- ✓ **Available Through Our Customer Portal:** The eSentire MDR for GenAI Visibility dashboard is accessible through the eSentire Insight Portal.

Ready to get started?

Connect with an eSentire Security Specialist to learn how we can help you build a more resilient security operation and prevent disruption.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US ☎ 1-866-579-2200

eSENTIRE