Enterprise Strategy Group™

BRIEF

AUGUST 2025

Addressing the Challenges of Securing GenAI Adoption With Harmonic Security

Todd Thiemann, Principal Analyst

Abstract: Enterprises want to embrace AI but are reluctant to deploy AI apps due to the potential for data loss. Harmonic Security helps enterprises safely deploy AI apps with controls designed to deliver precise protection against data loss.

Key Highlights

- 62% of enterprises intend to deploy a new DLP tool for a specific use case, according to Enterprise Strategy Group research.[1]
- Harmonic Security increased its GenAI tool coverage by 30x and now provides tailored responses for personal accounts, a prime data loss vector.
- Enterprises can deploy AI apps with confidence by controlling against potential data loss while avoiding DLP alert noise.

Gen AI Application Deployments Inhibited by Data Loss Risk

Enterprises are embracing generative AI (Gen AI) to streamline operations and increase revenue by letting AI perform manual, tedious tasks. However, the potential for data loss hinders many deployments. Organizations are concerned about their key intellectual property and sensitive data being inadvertently disclosed. GenAI-based apps were a top data loss vector, with 43% of enterprises having experienced a data loss event via a GenAI-based application.

Existing data loss prevention (DLP) tools are based heavily on regular expression (regex) logic that functions well with known, structured data types like personally identifiable information (PII). However, the regex approach does not lend itself to GenAI applications where intellectual property and other unstructured data are commonplace. Conventional solutions being redeployed for GenAI applications can be a burden to configure and administer and also tend to generate significant false positive alert noise that burdens security teams. GenAI applications are a different beast that benefits from a new DLP approach.

GenAI applications are also being rapidly adopted, frequently without oversight from security teams. It is easy for employees to fire up their browsers and visit ChatGPT, Claude, or Perplexity to complete their tasks. Such tools may be unauthorized or risky AI applications, and security teams frequently lack visibility and control over AI apps.

Any solution needs to overcome the traditional DLP challenges of minimizing administrative overhead and reducing alert noise. While existing solutions might solve that challenge for existing data loss vectors like email and endpoints, GenAI applications pose different risks to sensitive information. Enterprises need to have an adequate inventory of AI assets, identify and assess shadow AI, enforce AI policies, and continuously guide end users to avoid inadvertent data leakage. GenAI is different in that solutions need to prevent leakage of unstructured sensitive data like intellectual property and source code. Compliance requirements mean that solutions also need to detect personally identifiable information (PII) and cardholder information affected by Payment Card Industry Data Security Standard (PCI-DSS) mandates.

[1] Source: Enterprise Strategy Group Research Report, *Reinventing Data Loss Prevention: Adapting Data Security to the Generative AI Era*, May 2025. All Enterprise Strategy Group research references in this brief have been taken from this report.

Harmonic: Expanding AI Coverage and Key Data Loss Vectors

Harmonic Security has continued its rapid drumbeat of innovation to help security teams facilitate adoption of GenAI applications while controlling against data loss. In April 2025, the company announced they had expanded AI tool coverage by 30x, expanded file type coverage, and enhanced Harmonic's ability to distinguish between sanctioned AI usage and personal account usage for AI tools that may violate policy.

Analyst Insight

The potential for data loss can bring a halt to GenAI initiatives. Existing DLP approaches have struggled to protect against the loss of unstructured sensitive data like intellectual property and source code. Security teams need to facilitate secure deployments rather than being a "department of no" that stops projects due to security concerns.

Market Insight

71% of enterprises are concerned or very concerned about the loss of sensitive data via AI or LLM applications.

Harmonic Security achieves its results with an approach that lends itself to detecting and blocking unstructured data while avoiding alert noise. While AI is helping improve security solutions, large language models (LLMs) can be imprecise and incur latency that results in a poor user experience. The small language models used as part of the Harmonic solution provide precision as well as low latency to facilitate inline blocking where appropriate.

With the new version of its tool, Harmonic claims to increase AI tool coverage by 30x to solve for the expanding AI tool ecosystem. As new AI tools crop up that may be sanctioned or risky, Harmonic provides visibility so security leaders can make optimal policy decisions.

Harmonic has led the industry in addressing GenAI data loss concerns and continues to do so with the addition of features like the ability to address key file types and the ability to understand the accounts being used. For example, a sanctioned work account on ChatGPT Enterprise may be fine, but using a personal Gmail with an unapproved tool may violate policy. Harmonic allows users to shape their response based on the context.

Conclusion

Enterprises are embracing GenAI but need to ensure sensitive data does not leak via an AI application. It creates a new data loss vector that lends itself to new DLP tools focused on GenAI-based DLP problems. Technology providers that can control against data loss via GenAI apps while avoiding alert noise and administrative burdens should be on the short list when considering how to safely deploy GenAI apps that touch sensitive data.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com