Executive Guide to Securing Data within Generative AI

Safeguard AI transformation and workforce productivity with Data Security Everywhere.

Introduction

Just like that morning cup of coffee, GenAI chat prompts have become essential to our workday. From marketing and finance to engineering and IT, AI is revolutionizing how departments in your business or government agency operate. It's like the digital shifts we've seen in the past – only on steroids. Integrating generative AI tools into daily workflows boosts productivity and drives growth. However, this newfound efficiency also opens the door to potentially exposing sensitive data online.

When users upload or paste confidential information into GenAI chats, the language models often store this data and learn from it. No matter how you slice it, that's a significant risk of data loss. AI's insatiable appetite for data, combined with threats like ransomware, makes protecting privacy and ensuring regulatory compliance a complex challenge.

To harness AI's potential without risking your business, you need the freedom to experiment safely. This is where a data-first security approach can be a competitive advantage. By unifying visibility and control, you can innovate securely.

This guide will help you navigate your AI transformation with confidence, offering recommendations and insights on key security capabilities and best practices. Additionally, we'll explore how Forcepoint's AI-powered platform can significantly reduce risks and prevent data loss across applications, making Zero Trust for AI a reality while simplifying compliance.

Of organizations are currently using or plan to use AI in in the next 12 months

Source: IDC Business Value of AI Survey, September 2023

Of organizations are adopting Generative AI at a very fast pace

Source: Deloitte: State of Generative AI in the Enterprise Quarter 2 Report, April 2024

ROI for every dollar invested in AI

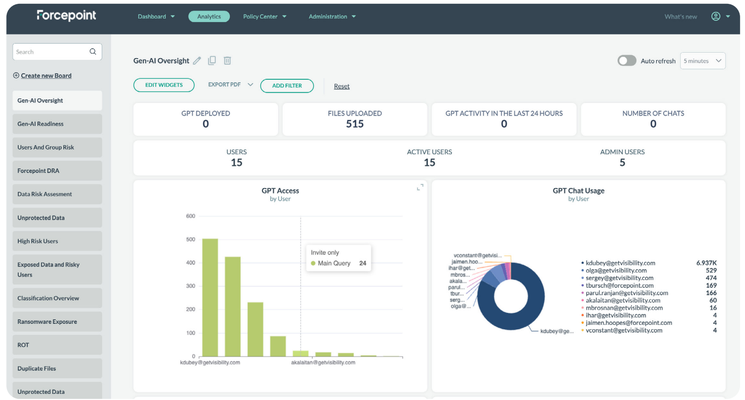
Source: IDC Business Value of AI Survey, September 2023

Gain Visibility of Sensitive Data

Imagine navigating a dense forest without a map. You'd have no idea where the dangers lurk or where the valuable resources are hidden. Gaining visibility in your AI environment is akin to creating a live, detailed map. You pinpoint where sensitive data is stored and understand who has access to it. Some AI security solutions also use rich data forensics and usage pattern tracking to identify vulnerabilities like compliance gaps. With this clarity, you can identify and mitigate risks before they escalate. Data discovery, classification and continuous monitoring serve as your compass and guide, ensuring you're always one step ahead of potential threats.

Forcepoint Advantages:

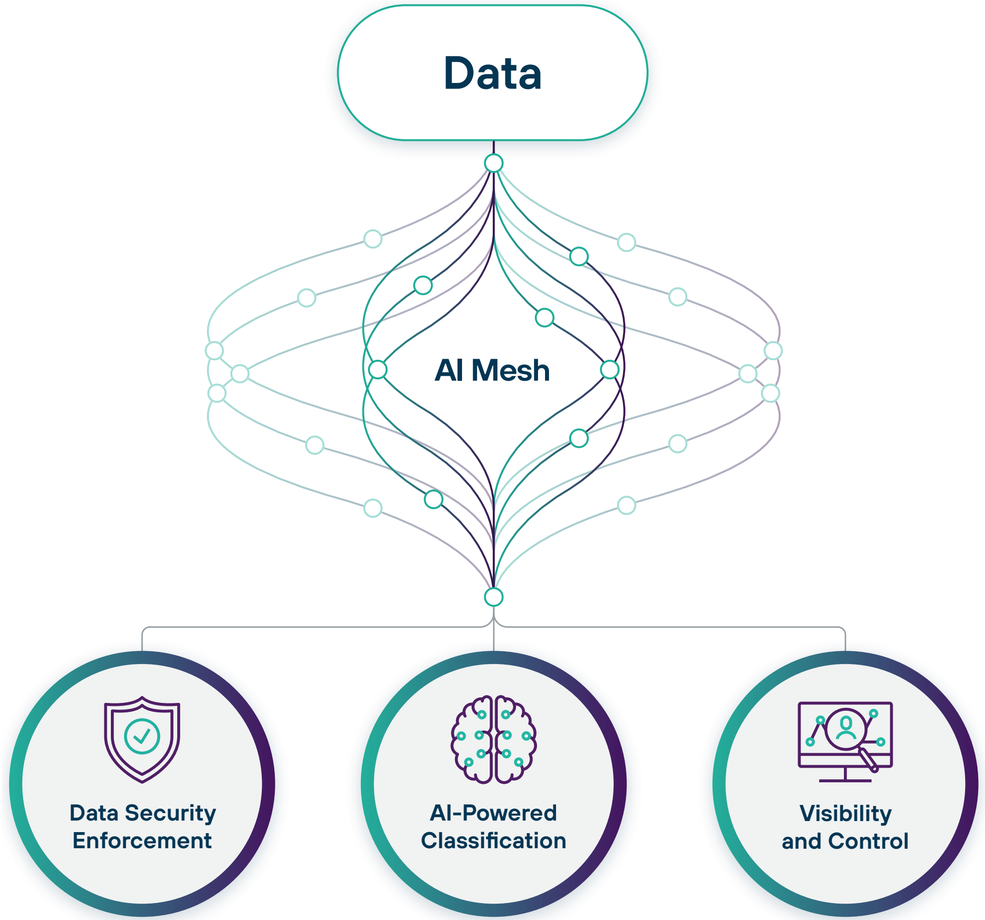
- **Data Security Posture Management (DSPM):** Powered by AI Mesh, DSPM enables proactive data risk management by uncovering vulnerabilities across networks, devices and clouds. It scans a million files an hour and uses AI Mesh to classify sensitive data accurately in nearly an instant, helping administrators reduce obsolete information, set proper permissions and move data to secure locations. For ChatGPT Enterprise, DSPM summarizes the usage of sensitive data in AI chats and flags security and privacy violations.
- **DLP with Risk-Adaptive Protection:** This solution continuously monitors data flow and user behavior, automatically adjusting protection levels based on real-time risk assessments. Users can unknowingly make mistakes that could lead to data leaks or loss; Forcepoint provides automatic coaching to guide safe AI usage, along with forensic reports on data loss attempts and user responses, helping admins refine coaching and training programs.
- **OpenAI API Integration:** Forcepoint is one of eight companies chosen by OpenAI as compliance and administrative tools for ChatGPT Enterprise. Forcepoint DSPM leverages OpenAI APIs to deliver clear dashboards that show who is using ChatGPT Enterprise, what files are being uploaded and the potential business risks. This comprehensive visibility into sensitive data usage makes it easier for you to create robust data security policies, which Forcepoint ONE SSE and DLP solutions enforce to prevent inappropriate data uploads.



Forcepoint provides risk assessment reports that help you visualize risk for any GenAI platform, including viewing user behavior and performing complete remediation within ChatGPT Enterprise.

Classify Data using AI Mesh

Forcepoint's AI Mesh combines language models, deep neural networks, data elements and machine learning to rapidly and accurately classify data in less than 200 milliseconds. It's highly customizable, so it can be tuned to their industry, regulatory or customer requirements for incredibly precise, low-maintenance data classification that significantly reduces the risk of sensitive data exposure.



Get Control Over Data on GenAI Chat

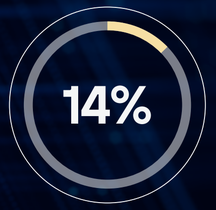
You've found where the critical resources (sensitive data) lie, but now you need to manage who holds the keys and how they're used. The next step is controlling access, usage and content sharing within AI applications, websites and tools. For this, you need a smart security system that not only grants access but also monitors every entry, adjusts permissions on the fly and at once addresses any breach attempts like pasting or uploading sensitive content into AI chats. That's what precise permissions and risk-based controls offer. By unifying the policy framework for various security capabilities like DLP, CASB, SWG and ZTNA, you streamline management, ensuring your proprietary and regulated data are safe.

Forcepoint Advantages:

- **Forcepoint DLP:** Keeps data secure by limiting or blocking access to sanctioned GenAI tools. Forcepoint enforces data security actions to prevent data loss through GenAI. Risk-Adaptive Protection capabilities help teams quickly and accurately implement automated remediation and risk-based access controls to enforce policies dynamically. We also use AI to identify data with highly accurate classification so that security policies are more effective.
- **Forcepoint ONE SSE (Web Traffic, SaaS Apps, Private Apps):** Ensures Zero Trust access to AI applications, websites and content by analyzing site risk and reputation, designating allowable site categories, restricting users and blocking or limiting activities involving sensitive information. Our cloud-managed platform isolates web content to prevent malware and sanitizes files to remove threats, protecting AI users and data without disrupting workflows.
- **Cloud-based, Unified Policy:** Streamlines policy enforcement for Forcepoint ONE Data Security and Forcepoint ONE SSE across multiple security domains including endpoints, email, networks, websites, cloud apps and private apps. With consistent, unified enforcement, security teams can manage a single security policy in the cloud or on-premises for all channels.

Deliver Increased Productivity and ROI

Now with clear routes and secured checkpoints helping you find all the hidden data paths, dangers and treasures, it's time to make the most of your AI transformation journey. A foundation based on unified management not only protects your data in AI interactions but also enhances productivity and reduces costs by consolidating tools and vendor relationships. Your organization can now enable employees to safely explore the innovative potential of AI and beyond, whether in cloud apps, websites, devices or email. Simplifying your security infrastructure with fewer tools and a single vendor makes implementing and sustaining comprehensive security easier. By securing all your data from one set of policies and location, you can save operational costs through automation and elimination of redundant processes.



Growth in Productivity for workers who access AI

Source: The National Bureau of Economic Research

Operational Costs Savings by streamlining DLP policy management

source: IDC

Considering Data Security Unification of multiple DLP products into a single interface

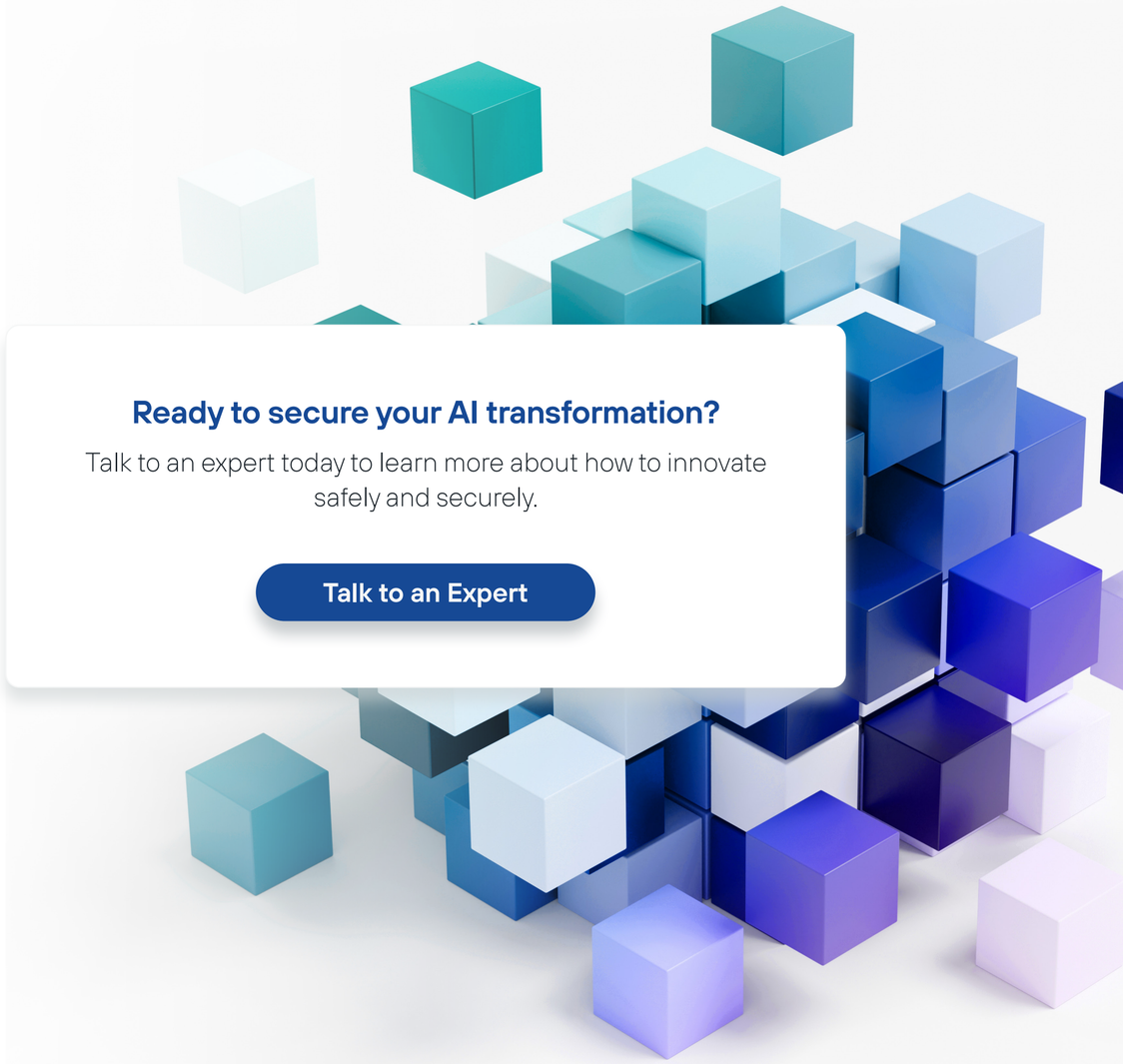
Source: IDC

Conclusion

In a world where AI is reshaping industries, how do you ensure your data stays secure? Forcepoint's AI ecosystem integration strategy and "Data Security Everywhere" capabilities empower you to confidently use AI systems and tools. Our multi-layered approach to AI security safeguards data assets regardless of the type or proficiency of AI user. Let's start the journey together to take control of your generative AI systems and workflows.

Next Steps:

- → **Assess your current AI security posture:** Understand your strengths and weaknesses.
- → **Identify key areas for improvement:** Spot vulnerabilities and opportunities.
- → **Implement a data-first security strategy:** Achieve unified visibility and control across your AI initiatives.



Ready to secure your AI transformation?

Talk to an expert today to learn more about how to innovate safely and securely.

Talk to an Expert

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Exec Guide to Securing Data within GenAI ebook-EN] 05Aug2024