Trellix

SOLUTION BRIEF

Protecting Sensitive Data in the Age of AI with Trellix® Data Security

Address data risk and accelerate secure AI adoption

Highlights

- **Identify interactions** with unsanctioned AI applications and web GPTs that have access to sensitive data.
- **Centralize AI risk tracking** and incident management with granular visibility and instant access to trends and incidents for remediation.
- **Prevent data leaks** by finding and blocking data leakage through common AI vectors, such as copy/paste and file uploads.
- **Protect databases** by identifying large data transfers or unusual activity, and detect and block prompt injection attacks.
- **Keep databases secure** and up to date with no downtime
- **Safeguard sensitive files** by protecting files and folders from AI ingestion.

AI and the growing risk to your data

AI and machine learning have helped drive efficiencies in enterprise technology for decades. The introduction of OpenAI's ChatGPT in late 2022 marked a new inflection point. Since then, the rapid rise of mainstream generative AI (GenAI) has transformed the technology landscape. According to a recent McKinsey study, 88% of businesses report implementing AI officially in at least one business function.[1]

The explosive growth of AI in the workplace has challenged organizations to strike a balance between adopting AI to drive productivity gains and protecting sensitive enterprise data. Risks such as data leakage, prompt injection attacks, and data ingestion by unauthorized tools have emerged as top concerns among business and security leaders. While growing regulatory actions around AI have introduced new compliance requirements that further necessitate AI data governance.

A framework for addressing insider risks and shadow AI

While blocking or restricting the use of AI tools in the workplace might provide some protection, it could drive employees to use "Shadow AI," the term for unsanctioned AI tools in the environment. Organizations that want to securely adopt AI to benefit from productivity advances while keeping sensitive data under their visibility and control can benefit from a secure adoption framework.

Secure AI adoption can be accelerated through a holistic approach that prioritizes protecting sensitive data. Technology solutions can help mitigate potential data loss, but an approach that encompasses organizational policy, user training, and real-time technology integration will offer stronger protection and enhance data security posture.

AI data risks - know your numbers

- **88%** of organizations reported GenAI use in at least one business function, **up from 74%** the year before.[1]
- Data privacy and security **(73%)**, legal compliance **(50%)**, and governance oversight **(46%)** are the primary AI risk concerns for organizations.[2]
- Only **20%** of organizations feel confident in their ability to secure generative AI models.[3]
- Security incidents involving shadow AI added an average of **$670,000** to the cost of a data breach.[4]

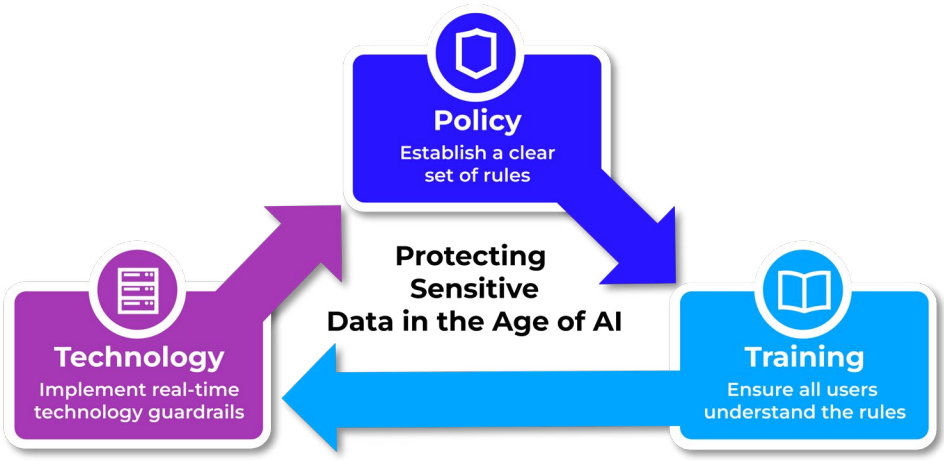

Figure 1. A three-part framework of policy, training, and technology accelerates secure AI adoption.

Three pillars for secure AI adoption

- **Policy:** Establish clear, actionable guidance on AI acceptable use, sensitive data handling, and expectations on compliance with global regulations. Policies should define boundaries while designating authorized use cases and tools.
- **Training:** Build an "AI-Aware Culture" organization-wide, ensuring all personnel (employees, contractors, third parties) understand acceptable use. Given the rapid pace of AI evolution, training should be an ongoing process with regular updates as technology changes.
- **Technology:** Implement technology to monitor AI usage, identify potential sensitive data loss to shadow AI, stop advanced attacks, and block data exfiltration. Technology should alert users instantly upon policy violations, providing "in-the-moment" reinforcement and guardrails.

Trellix services for protecting sensitive data in the age of AI

As GenAI expansion complicates the threat landscape, organizations may find internal teams lack the bandwidth or specialized skills to keep pace with policy development, training programs, and technology optimization. Trellix Professional Services bridges this critical gap, acting as a force multiplier for busy enterprise information governance, compliance, and security teams by aligning organizational strategy with emerging global regulations.

1 McKinsey, The state of AI in 2025: Agents, innovation, and transformation

2 Deloitte, The State of AI in the Enterprise

3 Accenture, State of Cybersecurity Resilience, 2025

4 IBM, Cost of a Data Breach Report, 2025

Trellix Professional Services: Trellix experts can help organizations align regulations and organizational objectives with specific security controls. Our experts provide guidance to develop robust AI acceptable-use policies and implement real-time user training, ensuring that your data governance program remains resilient even as AI technology continues to advance. Trellix experts can help deploy or fine tune Data Security technology solutions, support configurations to track AI-specific data leakage, and optimize the Trellix AI Data Risk Dashboard. Trellix experts are available worldwide and knowledgeable about local laws and regulations.

Trellix technology solutions for protecting sensitive data in the age of AI

Trellix provides a comprehensive suite of industry-proven data security technologies designed to monitor usage, stop advanced attacks, and block unauthorized data exfiltration so that organizations can harness the efficiency of AI while maintaining visibility and control over their most sensitive information

Trellix Data Loss Prevention (DLP): Trellix DLP monitors and blocks potential data exfiltration in real-time to prevent employees from sharing critical information, such as intellectual property or source code, with unauthorized GenAI tools. Customers can implement the AI Data Risk Dashboard, included at no extra charge, which offers visibility into over 400 predefined AI tools. Track authorized and unauthorized AI usage across the enterprise, provide real-time coaching to remediate risky behavior at the point of interaction, and remediate potential incidents swiftly from a single screen.

Trellix Database Security: Protect your most critical information from compromise or theft while maintaining the integrity of the data stores that feed AI models. Monitor for anomalous data transfers or unauthorized access by AI agents, enabling instant termination of suspicious sessions before proprietary data is exfiltrated or manipulated. Detect and block sophisticated, AI-automated SQL injection attacks to safeguard your enterprise from malware and poisoning while keeping databases patched and secure without downtime.

Trellix Data Encryption: Trellix File and Removable Media Protection (FRP) can establish a rigorous data boundary by rendering sensitive files unreadable to unauthorized AI scraping tools and autonomous agents. Ensure data remains encrypted at rest and in transit, preventing proprietary information from being inadvertently ingested or used for unauthorized model training without explicit consent.

Data security resilience for the AI-powered enterprise

The rapid evolution of generative AI presents opportunities and risks for today's enterprises. Organizations appreciate the potential opportunity for efficiency while simultaneously worrying about unprecedented new data risks. And the prevalence of AI has made blocking these tools nearly impossible. By implementing the Trellix framework of Policy, Training, and Technology, enterprises can move from a posture of restriction to one of secure enablement. Trellix's industry-proven Data Security Suite—bolstered by expert Professional Services—ensures that your critical intellectual property remains protected by intelligent guardrails.

To learn more about Trellix Data Security solutions for protecting sensitive data in the age of AI, please visit https://www.trellix.com/solutions/data-protection-for-ai-risk/