



Securing AI: Comprehensive Data Protection Strategies in the AI Era

The risks, implications, and strategic approaches to securing AI and machine learning environments



The AI Revolution: Data Security Challenges

Artificial Intelligence (AI) has evolved from an emerging technology to a core business capability, reshaping industries through innovations like ChatGPT and DALL-E. These advancements enable breakthroughs in sales strategies, operational decision-making, and customer experience. However, AI's reliance on vast, sensitive datasets introduces significant data security challenges.

Unique Machine Learning Security Complexities

AI systems pose distinct security risks that traditional models cannot address effectively. The dynamic nature of datasets, which are continuously evolving, and the real-time adaptation of algorithms introduce complexities that demand a multifaceted approach to security. Furthermore, AI workflows operate within multi-layered processing environments, where adversarial attacks and data corruption pose significant threats to the integrity of machine learning systems. These risks highlight the urgent need for adaptive and robust security measures tailored to the unique requirements of AI.

Regulatory Requirements

Governments worldwide are intensifying data privacy and AI-specific regulations:

- **Global Privacy Frameworks:** GDPR, CPRA, and PDPA impose strict compliance mandates.
- **Emerging AI-Specific Laws:** The EU Artificial Intelligence Act introduces mandatory transparency and robust testing for AI data processing.



Multiple Risk Factors - Beyond Traditional Security Paradigms

AI environments introduce a new wave of vulnerabilities that go beyond traditional perimeter-based defenses. These systems, by design, are deeply interconnected with diverse technologies, creating a unique set of security challenges:

- **Data Manipulation Risks:** AI systems are only as reliable as the data they consume. If datasets are tampered with, the integrity of the AI's decision-making processes is compromised, leading to erroneous outcomes that could harm organizational operations.
- **Cloud Dependencies:** As AI solutions often rely on cloud infrastructure for data storage and processing, they become vulnerable to breaches and unauthorized access. Sensitive data housed in these systems, when inadequately protected, can become a prime target for cybercriminals.
- **Insider Threats:** Individuals such as system administrators and data scientists, who possess legitimate access to AI environments, may pose significant risks—either intentionally or inadvertently. Their elevated permissions can be exploited to misuse data or bypass existing security measures.

These interconnected risks emphasize the critical need for tailored security frameworks that address the distinct demands and complexities of AI systems, going beyond the reactive approaches of traditional IT security.

Potential Consequences of Data Compromise

The consequences of failing to secure data in AI environments can be severe and far-reaching, affecting both operational efficiency and public trust. Key outcomes include:

- **Predictive Inaccuracy:** Corrupted or compromised data undermines the reliability of machine learning models. This not only skews predictions but also disrupts decision-making processes, resulting in flawed business strategies and lost opportunities.
- **Financial Penalties:** Non-compliance with regulatory standards, such as EU-AI Act, GDPR or CPRA, often results in hefty fines. The financial strain from penalties and legal disputes can significantly impact an organization's bottom line.
- **Trust Erosion:** Security breaches diminish the confidence of customers, stakeholders, and partners. Trust, once lost, can be challenging to rebuild,

jeopardizing long-term relationships and potential collaborations. The negative publicity surrounding a breach and mishandling of sensitive data leads to reputation damage deterring the business and market position.

The stakes are high, and organizations must act decisively to mitigate these risks to preserve operational and reputational stability.

Strategic Imperatives for Secure AI

To safeguard the integrity and functionality of AI systems, organizations must focus on forward-thinking, adaptive security strategies. This involves a threefold approach:

- **Proactive Data Protection**
 - Develop comprehensive data protection strategies that encompass encryption, access controls, and robust monitoring capabilities specifically tailored to AI implementations.
 - Establish adaptive security frameworks designed to evolve alongside technological advancements, ensuring resilience against emerging threats.
- **Continuous Improvement**
 - Implement persistent monitoring mechanisms to identify and address vulnerabilities in real-time.
 - Invest in continuous security education for teams, fostering an organizational culture that prioritizes awareness and preparedness.
- **Balanced Innovation**
 - Strive for equilibrium between technological innovation and stringent security measures, avoiding trade-offs that compromise protection.
 - Cultivate an environment where developers and stakeholders integrate security considerations into every stage of AI development and deployment.

By embedding these strategies into their operational fabric, organizations can confidently leverage AI innovations while maintaining robust security and compliance.

SecuPi Data Security Platform: Advanced Protection Strategies

Traditional data-protection solutions do not offer the capabilities to address the full scope of business and technical requirements. Such tools further require extensive implementation effort, alongside high CAPEX and OPEX to maintain multiple technologies.

Access control is fundamental to securing data, but the complexity of on-premises, hybrid and cloud operations, volume of data, technologies and number of data users can cause it to quickly get out of hand as policies need to be defined and validated to be consistently enforced across **each and every user, different data-stores, classifications, technologies and so on.**

Adopting a data-centric security approach allows the externalization of data protection and control functions from the various applications, data-platforms, and other technologies and as such offers several key benefits to the organization:

- **Single pane-of-Glass across your data landscape:** consolidating telematics from multiple sources, correlating and aggregating it for a single, holistic view for all data activities is critical for real-time response to emerging risks.
- **Consistent data-protection, everywhere:** using a data-centric platform allows the organization to define data access and data security policies that support the organization's business strategy. Enabling data democracy while ensuring access on a need-to-know basis, regulates how data is being accessed or processed. Consistent policies will always apply.
- **From Classification to Remediation:** implementing a data centric security platform offers a superset of capabilities, traditionally procured from multiple vendors to address specific need. Such overarching set of capabilities enables ensuring nothing falls between the cracks.

The Capabilities of the SecuPi Data Security Platform

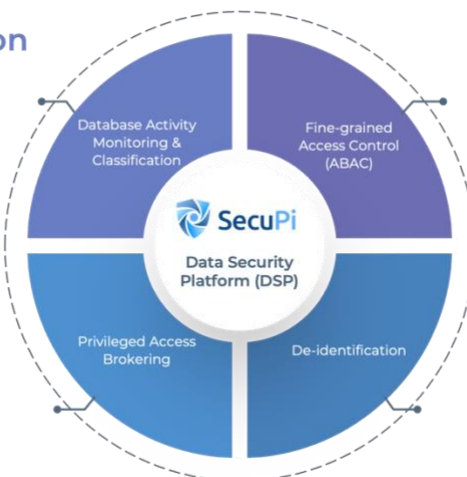
The SecuPi platform delivers end-to-end data protection with unparalleled capabilities:

Database Activity Monitoring & Classification

- > Real-time data access monitoring with classification, risk score presenting original identity & user behavior analytics
- > Data discovery and classification

Privileged Access Brokering

- > Controls privileged access using identity brokering, enforcing multi-factor authentication and credential vaulting
- > Enforce "least privilege" and Just-in-Time access to reduce attack surface



Fine-grained Access Control

- > Alert or block unauthorized access
- > Attribute Based Access Control (ABAC/PBAC)
- > Dynamic masking
- > Dynamic authorization "Self-service" data sets

De-identification

- > Format preserving encryption / tokenization, masking, and generalization
- > "Right of erasure" and consent-based retention management

a. Data Discovery and Classification

- **Application-Centric Classification:** Identifying sensitive data, such as PII and PHI, at the application layer.
- **Real-Time Monitoring:** Continuous visibility into data access and usage across the organization.

b. Advanced Access Control

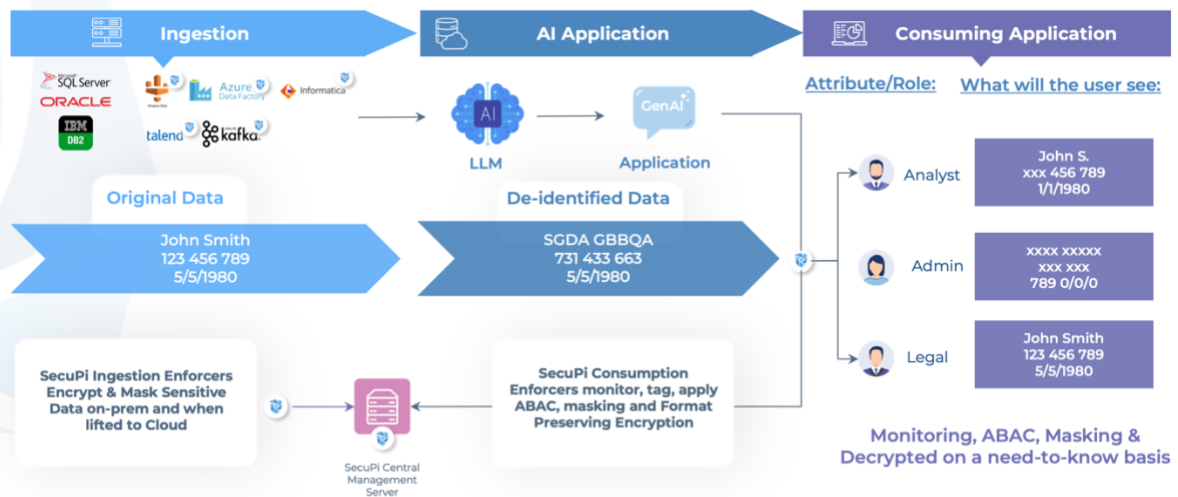
- **Attribute-Based Access Control (ABAC):** Policies enforced dynamically, ensuring access aligns with roles, context, and purpose.
- **Zero Trust Approach:** Prevent unauthorized access through fine-grained, context-driven controls.

c. Data De-Identification

- **Dynamic Masking:** Protect sensitive data during processing.
- **Client-Side Encryption:** Ensures data remains secure, even in cloud environments.

d. Unified View and Governance

- **Single Pane-of-Glass:** Consolidates data activities for a comprehensive security overview.
- **Policy Consistency:** Enforces universal data protection policies, reducing risk and complexity.



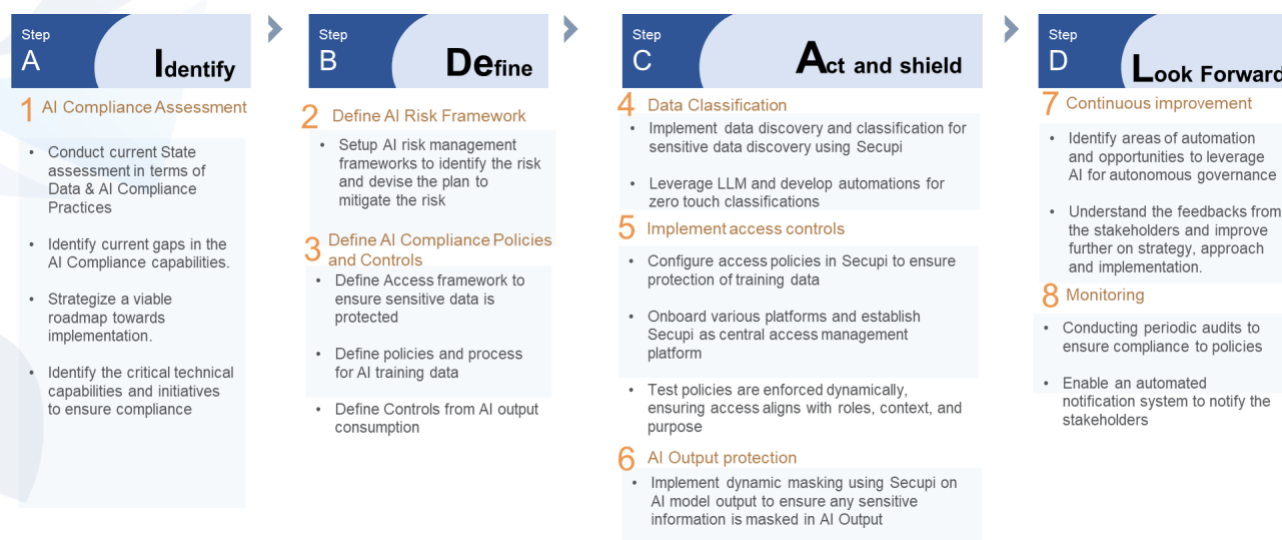
SecuPi Data Security Platform Outcomes



The SecuPi Data Security Platform delivers measurable outcomes for businesses by addressing critical data security, compliance, and cost-efficiency needs. It empowers organizations to securely harness data for initiatives like AI projects, data marketplaces, and marketing campaigns, while enabling data-centric Zero Trust through dynamic authorization, de-identification, and monitoring. By automating compliance with privacy & AI regulations and industry standards such as HIPAA and PCI-DSS V4, SecuPi simplifies reporting and reduces regulatory burdens. Its all-in-one, zero-code implementation optimizes cloud costs and seamlessly integrates with existing ecosystems, ensuring broad compatibility across diverse data platforms.

Infosys Implementation Approach

Infosys has developed IDeAL framework to manage the risk which comes from AI technologies. The below depicted approach has been adopted to showcase how AI compliance controls can be build leveraging SecuPi



About SecuPi

SecuPi's Data-Centric platform has been vetted by leading analysts (Gartner, Kuppingercole, Gigaom, SCMedia) as a market leader, providing a super-set of capabilities to address the application and analytical workload protection pillars as well as the Data security pillar with multi-facet, contextual, attribute-based access control (ABAC), sensitive data classification, real-time data usage monitoring, Dynamic Masking and Format Preserving Encryption.

About Infosys Topaz

Infosys Topaz is an AI-first set of services, solutions and platforms using generative AI technologies. It amplifies the potential of humans, enterprises and communities to create value. With a vast repository of AI assets, pre-trained AI models, 10+ AI platforms steered by AI-first specialists and data strategists, and 'responsibly by design' approach, Infosys Topaz helps enterprises accelerate growth, unlock efficiencies at scale and build connected ecosystems.

Authors

Saurabh Agarwal
Industry Principal
Infosys

Varun Khanna
Lead Consultant
Infosys

Avihai Segal
SecuPi