

AI Security Business Cases

Protect the Business from AI Threats, Without Slowing Innovation



Shadow AI Risk

Employees are increasingly using unapproved AI tools, many of which emerge rapidly and come from high-risk or unverified sources. These tools often operate outside IT's visibility, creating uncontrolled exposure. In some cases, they explicitly state that user data may be used to train their models or stored in foreign jurisdictions, raising serious concerns around data privacy, regulatory compliance, and national security.

Shadow AI Discovery and Control

Ovalix discovers Shadow AI across the organization, identifying unauthorized and unmonitored GenAI tools in use. It continuously monitors usage, performs risk assessments to highlight the most risky applications, and allows you to block high-risk AI tools directly from the platform, giving you full control and visibility to manage Shadow AI risk proactively.



Data Leakage Through Generative AI

AI tools rely on contextual input, which often causes employees to unintentionally share sensitive information with public GenAI applications that lack proper safeguards or data controls. Such sensitive information may include customer records, financial data, contracts, intellectual property, and other confidential business data.

GenAI Data Leakage Prevention

Ovalix continuously monitors interactions between users and GenAI applications to detect risky behavior and potential data exposures. It helps identify patterns of unsafe usage and policy violations, enabling real-time enforcement to prevent data leakage.



Policy Enforcement

Although most organizations establish written policies for AI tool usage, enforcement at scale is impossible without automation.

Real-Time AI Policy Enforcement

Ovalix enables real-time policy enforcement, reducing violations and ensuring employees follow organizational guidelines consistently, without relying on manual oversight.





Lack of AI Governance and Visibility

As AI adoption grows, organizations often struggle to gain visibility into how these tools are being used, where sensitive data is going, and whether proper governance is in place. The absence of unified oversight results in blind spots, inconsistent practices, and elevated risk.



Unified AI Governance and Oversight

Ovalix provides centralized oversight of all AI-related activity, enabling organizations to monitor usage, enforce policies, and uphold effective governance across departments and tools.



Exposure to AI-Specific Cyber Threats

Traditional cybersecurity tools do not detect or prevent threats such as prompt injection, jailbreaks, or adversarial inputs targeting GenAI applications. These emerging threats can lead to data compromise and loss of control over internal AI systems.



Detection and Mitigation of AI Threats

Ovalix continuously monitors for signs of adversarial activity in AI usage – such as prompt injections or jailbreak attempts – and flags and potential abuse or misuse that traditional security tools miss. It also mitigates these risks in real time, helping you stay ahead of emerging AI-specific threats.



Employee Training on Responsible AI Use

Even with policies and controls in place, employees often lack awareness of how their actions with AI tools can lead to risk. Ongoing education is essential to building a secure AI culture.



Continuous Employee Guidance and Education

Ovalix helps educate employees in real time through contextual pop-ups, messages, and guidance whenever violations occur, turning violations into learning opportunities. The platform also provides dashboards and insights to identify the most common violations, high-risk applications, and users with recurring issues, allowing organizations to tailor training efforts for maximum impact.

About Us

Ovalix is on the mission of empowering organizations to harness the full potential of AI by providing a robust security platform that ensures the security and integrity of AI systems. **Start your journey to secure AI adoption today!**