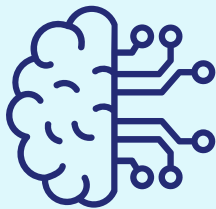


Safeguarding Enterprise AI: Securing Data and Models for the Future

Protecting AI Investments with Confidence and Agility



As AI and machine learning adoption accelerates, protecting AI data and models is critical. A strong security strategy safeguards sensitive assets across the AI lifecycle, enabling organizations to leverage AI confidently and securely.

Customer Challenges	Customer Outcomes
<ul style="list-style-type: none"> • Indirect prompt injection, data poisoning, and unauthorized access to sensitive information, • Preventing data leaks, intellectual property theft, and unauthorized access to AI/ML models across training, inference, and RAG in hybrid environments. • Meeting evolving privacy and digital sovereignty regulations while maintaining compliance globally. • Enforcing robust security controls without sacrificing operational efficiency. 	<ul style="list-style-type: none"> • Adopt AI securely to foster innovation • Maintain control and visibility over sensitive AI and ML assets • Show compliance and build trust with transparent data protection • Minimize disruptions and ensure resilient AI operations.
Why Thales?	Customer Benefits
<ul style="list-style-type: none"> • Unified security platform for AI/ML data and models across hybrid multicloud • Automated threat detection for rapid response to anomalies • External sovereignty controls and integration with existing security tools • Secure, cloud-agnostic workload migration with consistent policy enforcement 	<ul style="list-style-type: none"> • 70% reduction in encryption and key management effort, resulting in significant operational efficiency* • 221% return on investment over 3 years* • Reduced impact of a breach with an associated benefit of \$5.6 million over 3 years*

Next Steps:

Let's assess your current **AI security posture** and map a path to resilient, compliant operations.

Contact a Thales Security Expert