Data Sheet

THALES
Building a future we can all trust

CYBERSECURITY

Securing your GenAI

Protect Your Data, Brand, and Business Continuity.

cpl.thalesgroup.com

THALES
Building a future we can all trust

CYBERSECURITY

Overview:
What is AI Application Security?

AI Application Security is a purpose-built security solution designed to protect homegrown applications that use Large Language Models (LLMs) or GenAI at the backend. A statistic that currently sits at 67% of all organizations globally adopting and using such technology. AI Application Security acts as a dedicated, intelligent shield in front of enterprise AI-powered interfaces such as chatbots, virtual assistants, and API-driven business automation - defending them from the rapidly escalating risks and vulnerabilities unique to AI and LLM ecosystems. Imperva's AI Application Security directly addresses threats in the 2025 OWASP Top 10 for LLM and GenAI, offering a level of protection that traditional web application firewalls (WAFs), endpoint, or network security tools simply cannot match.

What AI Application Security Does

AI Application Security is designed specifically to safeguard interactions and outputs between your homegrown business applications and their underlying AI models, providing real-time protection by:

- Blocking Prompt Injection: Dynamically detects and neutralizes user inputs intended to manipulate AI behavior, ensuring the LLM acts only as intended.
- Preventing Data Leakage: Analyzes model outputs to block and alert on accidental exposure of private, regulated, or proprietary data.
- Securing System Prompts: Prevents the leakage of internal instructions, keeping operational logic and security controls invisible—even from determined attackers.
- Enabling Safe Output Handling: Reviews AI responses before they reach users, applying customizable policies to stop unsafe, unverified, or harmful information from being released.
- Controlling Resource Consumption: Detects and prevents abuse, such as recursive or excessive API calls, protecting against runaway AI costs.

Why It Matters

AI is reshaping industries more than we know - improving efficiency, automating customer interactions, and enabling new digital experiences. As AI becomes part of mission-critical business operations, the stakes for security are dramatically higher:

Prompt injection attacks can trick AI models into unsafe or undesirable actions, bypassing business rules or outputting harmful content.

Sensitive data leakage can expose PII, proprietary information, or confidential business data, leading to reputational damage and legal risk. Real-world incidents—such as airline chatbots making legally binding offers—demonstrate the real cost of unprotected AI.

Legacy security tools do not understand LLM logic, nor can they intercept the new classes of risks introduced by AI integration.

Threats We Prevent

- Prompt Injection
- Secure Information Disclosure
- Improper Output Handling
- System Prompt Leakage
- Unbounded Consumption

Without dedicated protection for AI-powered apps, organizations are exposed to:

- Unintentional or malicious data leaks (PII, business secrets, IP)
- Internal prompt leakage that reveals system-level logic or access
- Misinformation, toxic, or erroneous outputs trusted as fact
- Exploding infrastructure costs from unbounded API/model consumption
- Brand-damaging, embarrassing, or even legally binding AI mistakes

Primary Use Cases

- Securing public-facing and internal enterprise chatbots (e.g., HR assistants, customer support bots)
- Establishing safe AI-driven workflow automation in business processes
- Protecting proprietary APIs enhanced by AI
- Enabling AI innovation while maintaining compliance and trust

How Imperva's AI Application Security Is Different

AI Application Security does not protect traditional web applications, endpoints, or network perimeters and it does not replace your existing security stack. It is not simply a "WAF powered by AI"; but rather fills the security gap at the application's AI interface that legacy tools cannot address. Purpose built and focused on defending the LLM or GenAI powering your homegrown business applications, not generic SaaS or consumer AI interactions. It is specifically engineered for business applications with an AI backend that you build, deploy, and own.

Solution Architecture

More signals to filter increase security efficacy and enable better protection against LLM threats

How AI Application Security Works

The Imperva AI Application Security sits between your applications and the large language models (LLMs) they rely on, analyzing all inputs sent to the models and all outputs they produce—while preserving application performance. Every interaction is evaluated against multiple security guardrails, including protections for prompt injection, sensitive data exposure, and other emerging AI-specific threats. An adaptive risk scoring system continuously assesses and prioritizes potential issues for more accurate detection. By inspecting data after application-level modifications, the AI Application Security has a unique vantage point for identifying malicious or noncompliant behavior with greater precision. Depending on policy and risk severity, the Firewall can take automated actions such as alerting, masking sensitive information, or blocking malicious requests—ensuring organizations can safely deploy AI at scale without sacrificing performance, compliance, or innovation.

What AI Application Security Is NOT

- Not a general WAF, endpoint, or network security solution
- Not an "AI-powered" generic security tool
- Not designed for protecting SaaS apps, employee use of public AI models, or model training environments
- Not a replacement for your perimeter security, but an essential new control for the modern AI attack surface

Business Value

Imperva AI Application Security delivers a simplified, purpose-built approach to securing GenAI applications by providing out-of-the-box protection against AI-specific threats without adding operational complexity. Supporting any major LLM provider, whether third-party or self-hosted, it ensures flexible, environment-agnostic deployment and minimal integration effort. As part of Imperva's unified WAAP platform, it consolidates AI threat protection with proven web application, API, and bot defenses, enabling single-pane-of-glass visibility and policy management.

Backed by enterprise-grade guardrails, tailored policies, and 20+ years of application security expertise, it safeguards innovation while meeting compliance obligations. Recognized by industry analysts for best-in-class security efficacy and efficiency, Imperva AI Application Security gives organizations the confidence to adopt AI at scale—knowing unique LLM risks are fully locked down.

By adopting AI Application Security, you can:

- Deploy AI-driven apps to users and customers with confidence
- Proactively prevent costly, public, and reputationally damaging AI errors
- Accelerate innovation while maintaining compliance and user trust
- Focus on business growth, knowing unique LLM threats are managed

Beta Program

- Early access to product
- Influence direction of roadmap and product
- Direct access to product and engineering team for support
- Early access is complimentary

Beta Partner

- Deploy in test and production environments
- Provide regular feedback every other week
- Willingness to partner with Imperva to harden the product

Contact us today to secure your spot and shape the future of AI Application Security.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us