THALES

CYBERSECURITY

imperva

How AI-Driven Applications Are Prioritizing Bot Protection and API Security in 2025

Advanced Bot Attacks on AI Models

AI-driven applications are vulnerable to bot-driven data scraping, fraud, and automated decision manipulation.

API Abuse in AI Applications

Effective API security addresses risks outlined in the API Security OWASP Top 10, such as broken object-level authorization and excessive data exposure.

LLM Manipulation Through Prompt Injection

Organizations increasingly deploy LLMs in customer-facing applications, where prompt injections could lead to reputational harm or compliance failures.

Privacy Violations and Data Exposure

By controlling bot access to AI models and APIs, organizations can prevent unauthorized data scraping, automated manipulation, and other abuses that could lead to regulatory breaches.

Protect From Business Logic Abuse

Attackers are finding creative ways to disrupt online transactions, content delivery, and user authentication — undermining your business operations.

THALES

CYBERSECURITY

Get the Insights You Need to Defend Against Bots, API Breaches, AI Attacks, and Business Logic Abuse

Learn More

imperva