
WAVESTONE
CYBER SOLUTIONS
FOR A TRUSTWORTHY AI
Radar 2024

Why is AI security different?

AI systems are fundamentally different to traditional IT systems

AI systems base their decision-making on statistics as opposed to deterministic algorithm-based IT systems

In addition to usual cybersecurity methods and practices, securing AI systems require new methods and means as the threats and the relevant regulations are specific to this intrinsic difference

AI-specific threats: *Poisoning* *Oracle* *Evasion*

New rules and regulations for AI security: *Especially the EU AI Act but not only*

Even typical cybersecurity threats must be analyzed differently in an AI context:

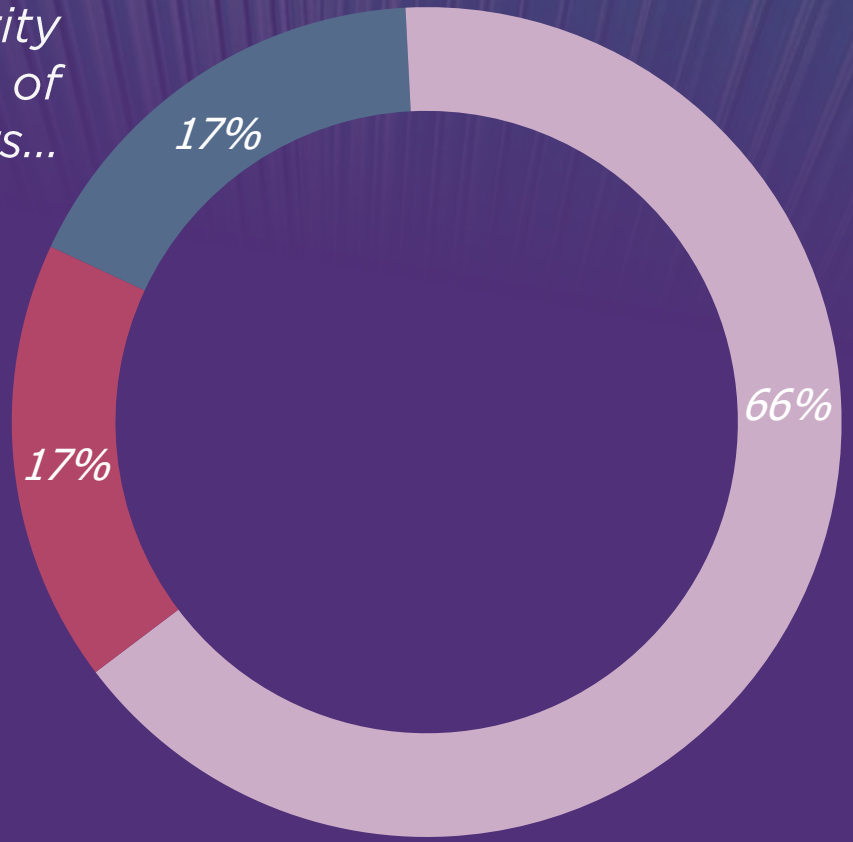
Data leaks

Attacks on the model

We need new security measures, built internally when possible or relying on new market solutions!

A market that Wavestone analyzed over the last 6 months scouting and meeting with suppliers globally

Suppliers bringing a security feature to an AI company's list of offers...

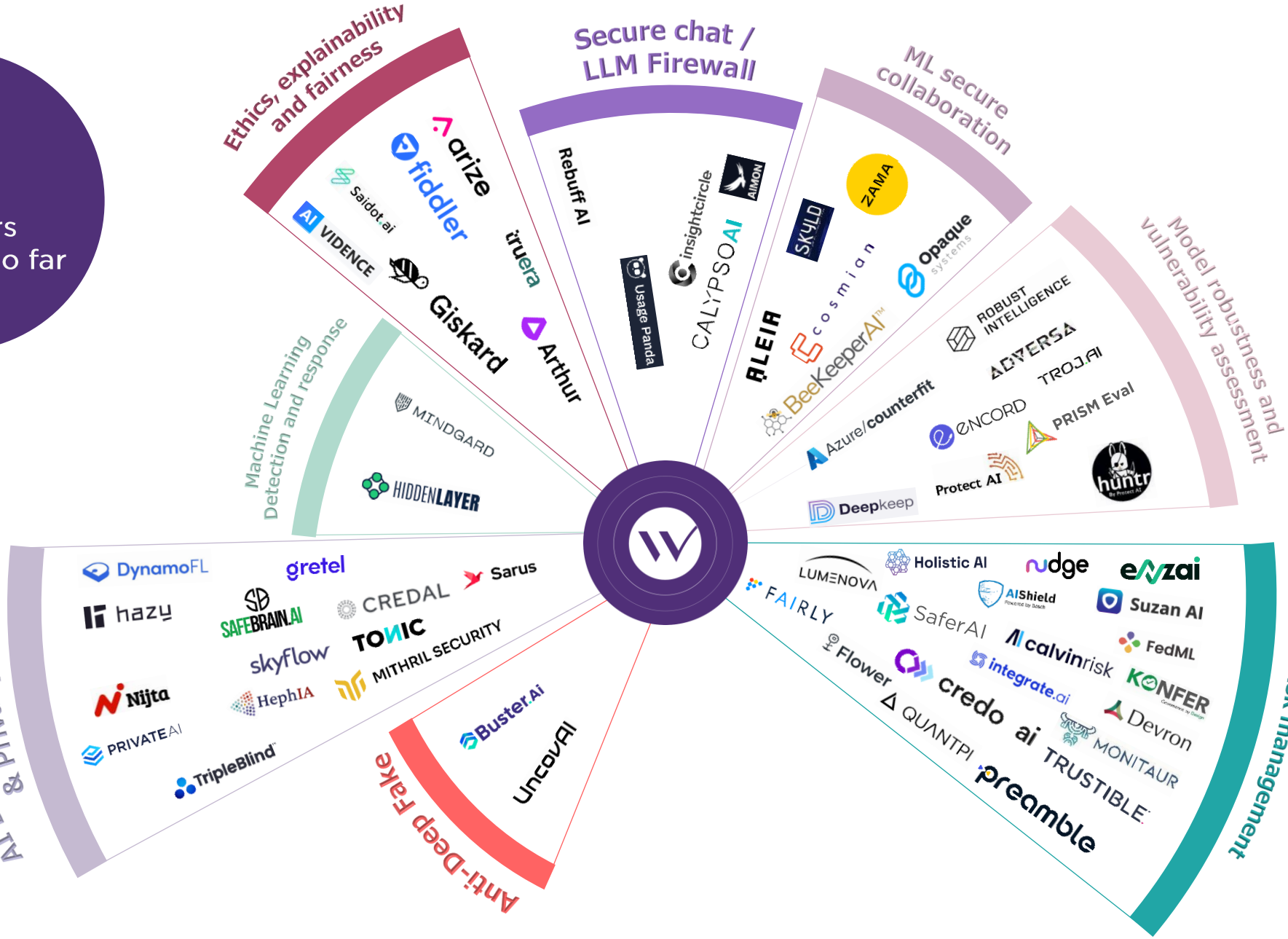


Suppliers entering the market as a pure player.

Suppliers adapting an existing offer to AI (e.g., DSPM to securing training data)...

Introducing the AI Security Radar:

63
providers
identified so far



Some companies have offers covering more than one category: our decision was to limit their presence to a single category on the radar.
This is the first version of our AI Security Radar: we kindly encourage all other companies to contact us to present their offer.

Today's Most Available Tooling: Governance and Compliance solutions

Companies urgently need to meet increasing regulations and want clear oversight of AI-related risks. They are turning to compliance and governance tools with limited R&D requirements, leading to rapid market growth.

Ethics, explainability and fairness

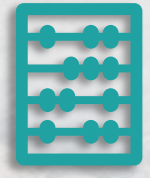
7 providers

Ensure that models are and remain fair, transparent, and effective

AI Data Protection & Privacy

13 providers

Ensure compliance and keep all concerned data used or produced by AI systems private



AI risk management

19 providers

Ensure full governance and visibility over risks

Next in Line: Securing Chatbot and ML Collaborative Systems

Chatbots and third-party systems have been two of the faster-expanding aspects of AI adoption by businesses. These technologies often expose AI systems many users or involve sharing data or models with external partners, raising the need for security. Yet, at this stage, many companies are still using basic security measures they set up themselves, rather than seeking more comprehensive solutions from the market.

Future Needs: Awaiting AI Maturity

Some categories are technically challenging. However, they will become more critical as companies gain in maturity in their AI security practices and policies.

Machine Learning Detection and Response

MLDR is set to become an all-encompassing defense solution that includes advanced capabilities to detect model and dataset drifting

2 providers

Anti-Deep Fake

Deep Fakes are a growing societal concern and will have an increasingly negative business impact on companies, countering them will become a major need

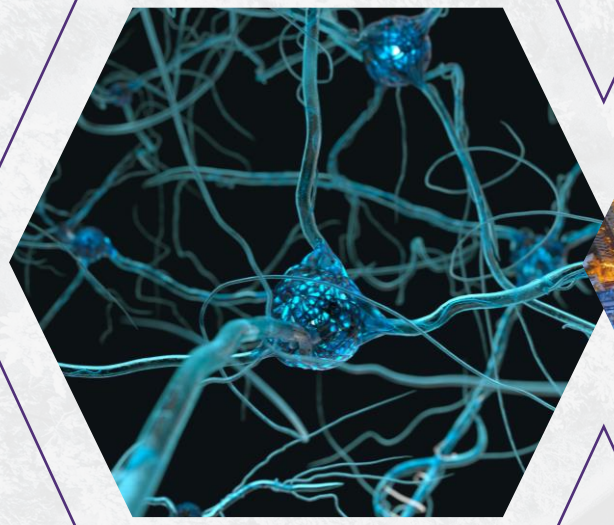
2 providers

Model robustness and vulnerability assessment

AI models rely on very complex inputs implying such a diversity of exploitable vulnerabilities that may require an AI to provide the assessment

9 providers

Market evolution: AI security's Path to Maturity and Standardization



Fundraising and partnerships
between AI security companies and with research labs will help bridge across multiple offers and create more mature security solutions

Customer maturity
will drive AI security providers to tailor and enhance their solutions

Standards
rooted in current regulations will guide the market towards uniformity, offering clearer insights into its trajectory

The priority today is building trustworthy AI

Amidst the rush to adopt AI, the paramount question is ensuring the reliability and integrity of these systems

The time is just right for AI Security

While AI's use for security may not yet be mature, securing AI infrastructures is critical now more than ever, as their business application scales up

While keeping in mind that the market will move sharply

We recommend tailored investments on a project-by-project basis, rather than broad commitments to a single platform. Keep in mind that the AI security sector is expected to undergo rapid changes with new entrants, mergers, and collaborations.

AI Security Radar: Navigating a Dynamic Future

This is just the beginning! This tool is designed to adapt and grow alongside the ever-evolving market of AI Security.

DO NOT HESITATE TO CONTACT US if you want to have your solution evaluated and added to the radar.
Contact: henri.du-perier@wavestone.com

Disclaimer: analysis done between October 2023 and March 2024. Based on identification of several suppliers using open source or closed community discussions. A majority of companies were met by our teams to analyze their offer.

Coming soon: Dive deeper into all 8 categories and how they support their offer technically