Fortanix

Solution Brief

Transforming AI Security and Trust:

Integration of Bosch AIShield with Fortanix Confidential AI

We are proud to present an important new security solution for artificial intelligence and machine learning (AI/ML) workloads, created through the collaboration between Fortanix and Bosch AIShield. This integrated offering combines the strengths of both companies to provide businesses with, unparalleled, secure and trustworthy AI models.

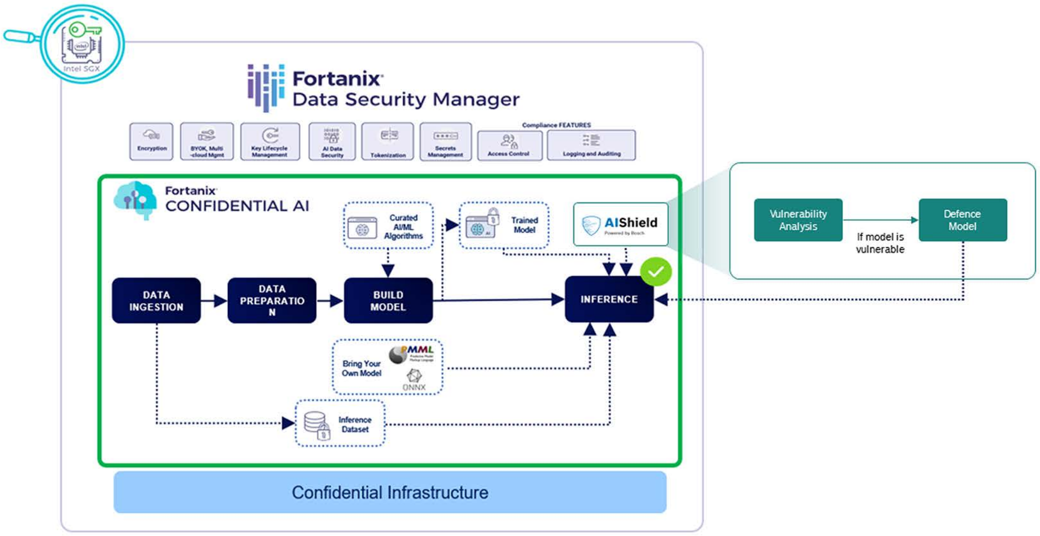
In this brief, we will explain how this innovative solution works, outline its key benefits, and conclude with the advantages it brings to customers across various industries.

How the Solution Works :

The Fortanix Confidential AI solution now incorporates Bosch AIShield advanced AI-driven threat analysis and detection capabilities.

The Fortanix Confidential AI service ensures the secure processing of AI models and sensitive data in trusted execution environments (TEEs). Powered by scalable infrastructure, the solution supports a broad range of AI/ML models and frameworks, provides hardware-backed proof of execution reporting, and delivers data security and confidentiality for AI/ML workloads.

The Fortanix Confidential AI integration of model-level defense against adversarial attacks that is provided by Bosch AIShield technology extends the capabilities of this secure AI service to deliver trustworthy AI deployments.



Key Benefits :

Secure and Trustworthy AI

Unprecedented AI security and trust for businesses by combining the power of Confidential Computing in Fortanix Confidential AI with Bosch AIShield's AI-driven threat detection.

Comprehensive Data Protection

Securing data across all stages of the MLOps pipeline – at rest, in motion, and in use – to ensure auditable data privacy and regulatory compliance.

Streamlined User Experience

Seamless integration of Bosch AIShield technology within the Fortanix Confidential AI service.

Expert Support and Guidance

Exceptional support and guidance for customers through the combined expertise of Fortanix and Bosch AIShield.

Conclusion :

Integration of Bosch AIShield technology within the Fortanix Confidential AI service is a groundbreaking offering that promises to transform the AI security landscape. By combining the expertise of two industry leaders, this solution provides unparalleled levels of security and trust for AI developers and system users. With its comprehensive protection, streamlined user experience, and relevance to industry use-cases involving regulated and sensitive data, this innovative collaboration is poised to empower organizations to harness the full potential of AI while protecting training and inference data in line with regulatory obligations and organizational policy.