Artificial Intelligence: Protection and Licensing

Production-Ready Solutions and Ongoing Research at Wibu-Systems

Nicolai Ruhnau
WIBU-SYSTEMS AG



WIBU SYSTEMS

Content

Introduction 2

AI Assets and Attack Surfaces 3

Wibu-Systems AI Protection and Licensing Solutions 4

Outlook 6

Summary 6

About the Author

Nicolai Ruhnau studied at the Munich University of Applied Sciences (B. Sc.) where he focused on distributed information systems and won an award for his Bachelor's thesis. At the Ludwig Maximilian University of Munich, he completed his studies in natural language processing (M. Sc.).

Since 2015, he has been gaining experience as a software engineer in various distinctive application areas at businesses in Munich and Karlsruhe. In 2023, he joined WIBU-SYSTEMS AG, where he is committed to cutting-edge research projects in the field of artificial intelligence.

Introduction

Artificial intelligence (AI) technologies like computer vision have moved from labs to real-world applications as industry reports like the current Gartner Hype Cycle from August 2023 illustrate.

It is useful to distinguish between protection from AI, protection with AI, and the protection of AI. As a global leader in innovative security technology, Wibu-Systems has many connection points to these topics. On the one hand, AI can be used to enhance license management, license binding, or code protection. On the other hand, AI itself can be protected and licensed. This document focuses on the latter topic.

In recent years, Wibu-Systems has gathered considerable expertise in this field, highlighted by several publications on protecting the machine learning (ML) lifecycle.

Our customers use various forms of machine learning; prominent use cases include medical diagnostics and quality control in factories. These applications usually have vastly different requirements than those of ChatGPT or other cloud providers.

How do you ensure protection of intellectual property in AI models and the deployed applications, possibly in environments accessible to attackers? And what are the ways to deal with specific licensing, marketing, and update considerations e.g., role-based access in a machine without Internet access? AI model serving poses new challenges and opportunities for licensing as well.

Furthermore, it is important to understand machine learning has its own lifecycle particularities. Making models production-ready covers deployment, monitoring, and ongoing maintenance. These issues are often described as Model Operations or ML-Ops.

Solutions to these protection and licensing requirements are still in their infancy, as described by Gartner in 2023.

Incidentally, the forthcoming EU AI Act will set the regulatory landscape for the upcoming years, emphasizing ethical and safety standards. Companies who act now and strategically design their machine learning operations will enjoy synergies with the new industry-wide compliance requirements.

AI Assets and Attack Surfaces

Assets

The illustrated ML architecture of figure 1 shows a range of assets and objectives a company might want to protect or license. The intellectual property might lie in the model itself,

the data used to train, and the way data gets extracted and entered into the pipeline by preprocessing based on experience and expert knowledge.

A variety of use cases can be enabled by smart licensing solutions:

- The model can be sold online on a pay-per-use basis or be embedded as part of a larger machine that stays offline. Access can be based on roles, location, and time.
- Another challenging requirement is combining the logistics of the artificial intelligence model protection at the customer's site with convenient and flexible licensing mechanisms.

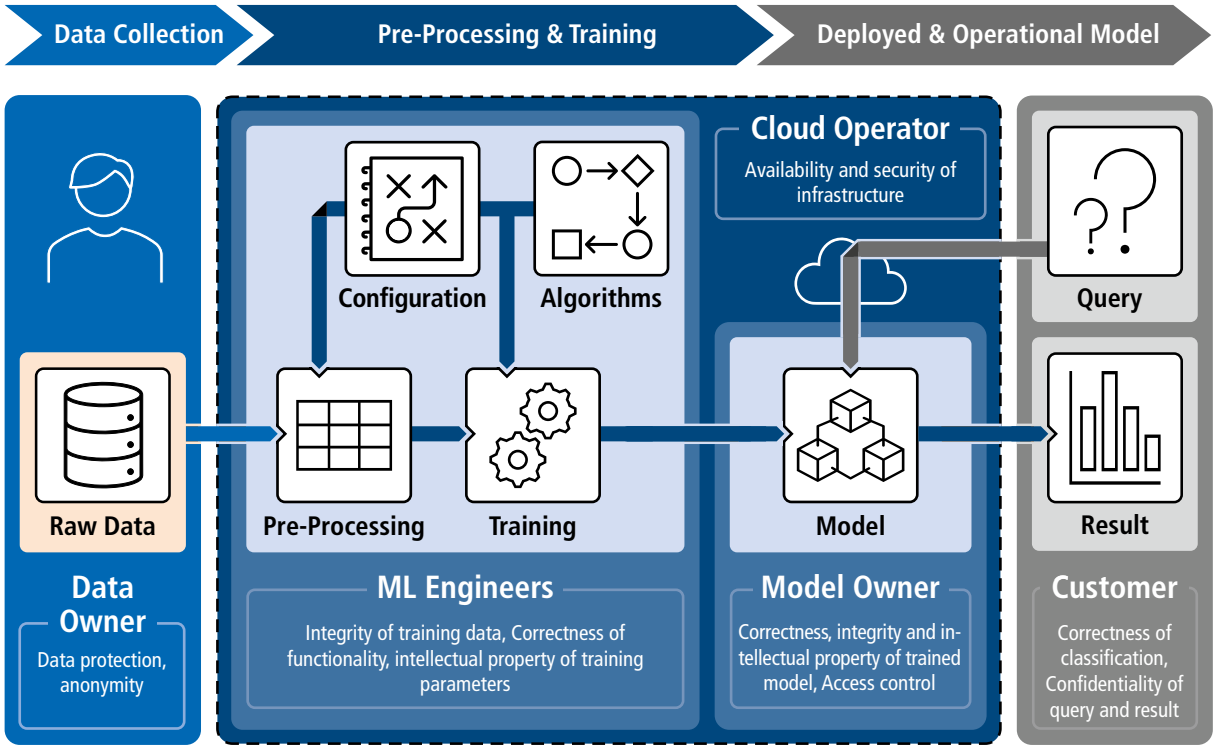


Figure 1: Protecting the machine learning lifecycle.

Attack Surfaces

The machine learning lifecycle is vulnerable to a variety of attacks, affecting all stages of development and operation. Unauthorized access to and modification of the original training data should be prevented to ensure that the final prediction is safe and authenticated.

The dynamic and data-intensive nature of the machine learning lifecycle poses unique challenges, such as preventing the reverse engineering of underlying data and models, and managing update processes.

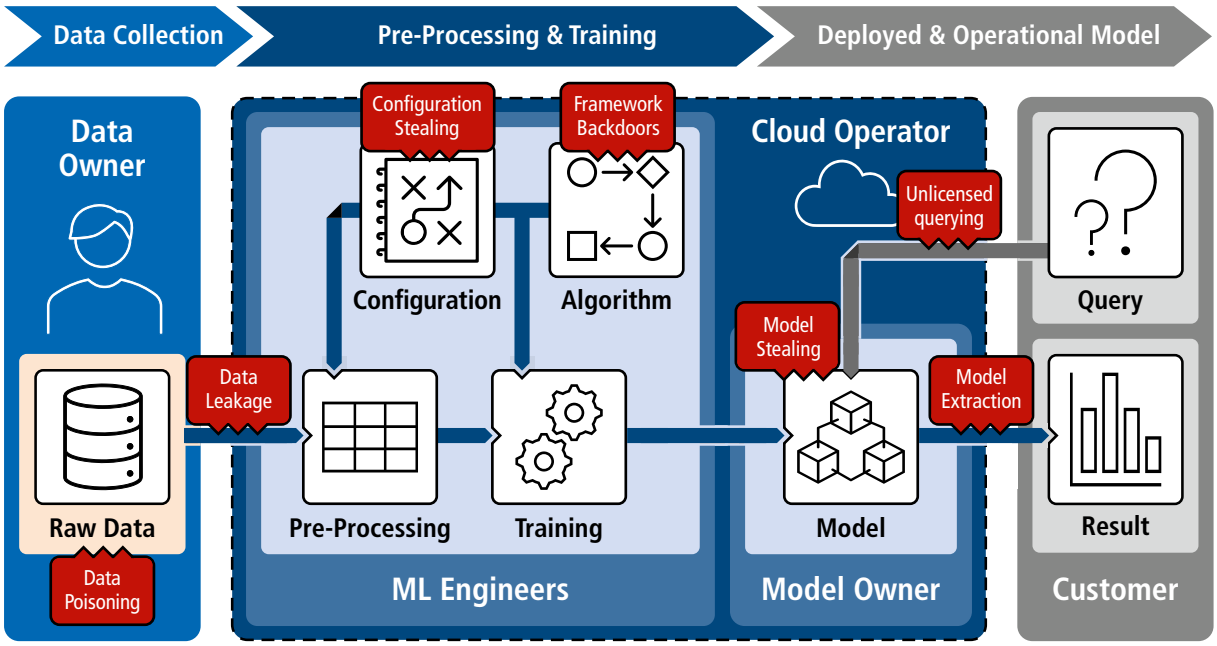


Figure 2: Attack surface of the machine learning lifecycle.

Wibu-Systems AI Protection and Licensing Solutions

CodeMeter and AxProtector

Wibu-Systems offers the solution to many of the above protection and licensing requirements in the form of CodeMeter and AxProtector.

With these solutions, a flexible and robust protective layer can be applied to arbitrary machine learning libraries and programs written in languages such as C++ and Python.

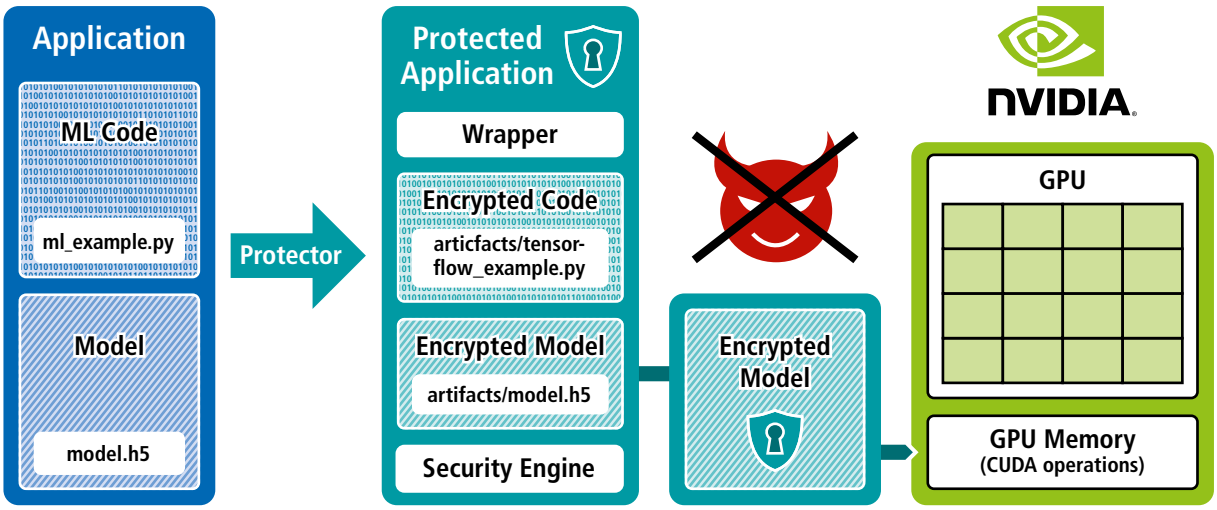


Figure 3: Model and code are encrypted, limiting reading and executing the contents to authenticated users.

Wibu-Systems Licensing Solutions

A variety of use cases can be enabled by smart licensing solutions:

- Selling the model online on a pay-per-use basis
- Embedding the artificial intelligence as part of a larger machine
- Using role-based access

Other examples include specific requirements, such as location or time-based access.

The logistics of protecting artificial intelligence models on customer premises add to the challenges of licensing solutions.

Wibu-Systems offers integrated licensing solutions that can be leveraged to enable and improve business processes.

For a Python application, for example, Wibu-Systems CodeMeter and AxProtector with the AxProtector Python license are simply installed on the operation system of choice (Windows, Linux, macOS etc.), creating a structured JSON configuration tailored to the specific licensing requirements of the business and running the encryption command.

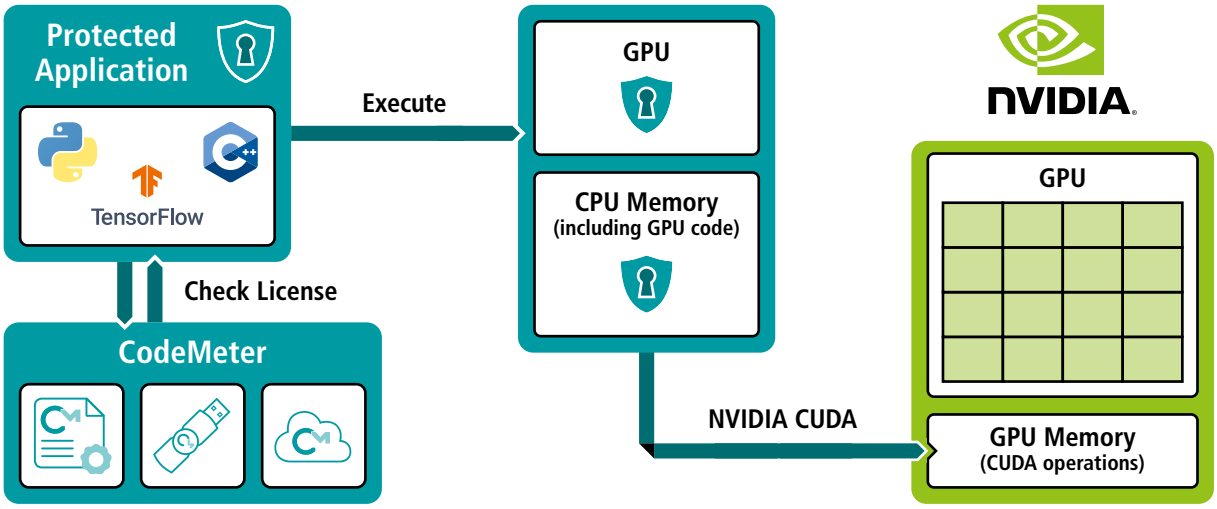


Figure 4: CodeMeter runtime checks the authorization. The operations inside the CPU including the CPU memory are protected, securing the program and machine learning model against runtime analysis, unauthorized access and reverse engineering

The AxProtector configuration is standard without the need for a machine learning addon or any other accessory. Business and use case requirements are customized according to specific requirements with CodeMeter, ensuring "Perfection in Protection, Licensing, and Security". Licenses can conveniently be managed on premises or in the cloud with CodeMeter License Central.

Only authenticated users will be able to execute the program. To further increase the security of the solution, secure hardware elements such as CodeMeter Dongles can be integrated.

With this simple installation, the machine learning licensing and protection process is complete.

Typically, NVIDIA GPUs are used, with NVIDIA CUDA interfaced with a machine learning library like Tensor-Flow. Given an ambitious attacker, instructions could possibly be read from the PCI bus or GPU memory, although this would still require considerable reverse-engineering expertise. The hacker would need to understand the memory-dumped instructions and the internal NVIDIA CUDA machine operations.

Outlook

In August 2023, Wibu-Systems kicked off the project SMILE4KMU, which is expected to end in July 2026. The central topics are the protection and licensing of the machine learning lifecycle, especially in the context of German small and medium-sized businesses. The cutting-edge research is subsidized by the German Ministry for Education.

The main goal is to develop secure and innovative protection and licensing solutions regarding the complete machine learning lifecycle.

WIBU-SYSTEMS AG coordinates the project, with the German machine learning startup preML GmbH developing the practical example use case as part of their vision-based quality control solution. Completing the SMILE4KMU project partnership, the University of Applied Sciences Offenburg is offering their renowned machine learning and IT security knowledge, research capabilities, and experience.

Wibu-Systems is working closely with the project partners and renowned German institutions to cover use cases of various industries, from mechanical or industrial engineering to web-based security services for the internet of things (IoT).

The results will consider the often-limited resources of small and medium-sized businesses while being applied to existing and novel business or industrial use cases. Benefitting from our cryptographic and licensing expertise and ecosystem, further competitive advantages to participating businesses shall be realized.

Regarding the importance of trustworthy execution environments and ensuring the integrity of AI models in the GPU context, techniques such as "NVIDIA Confidential Computing" enable secure data access and cryptographic applications at runtime. A promising approach for providing strong AI model protection could turn out to lie in combining these NVIDIA solutions with Wibu-Systems CodeMeter technology and integrating it with Wibu-Systems licensing solutions.



Image 1: Official image of the SMILE4KMU research project on the German Federal Ministry of Education and Research website.

Summary

As the use of artificial intelligence and machine learning becomes commonplace and vital to a company's success, the associated protection and licensing requirements, along with machine learning operations and lifecycle management, pose unique challenges, yet also offer opportunities for gaining competitive advantages.

How to license and protect these new assets? Wibu-Systems is adeptly addressing the surging demand with robust and adaptable solutions like AxProtector, CodeMeter, and License Central. This versatile license management solution effortlessly accommodates a broad range of complex requirements, with or without cloud integration. The EU AI Act and other compliance requirements will only add to the urgent need for trustworthy model protection and licensing.

Wibu-Systems is already working on extending its existing solutions to comprehensively cover various aspects of the machine learning lifecycle and operations. Cutting-edge research such as the SMILE4KMU project will enable innovators to license and profit from their machine learning solutions and leverage the power of "NVIDIA Confidential Computing".

5062-032-02 / 2026-11-02

About Wibu-Systems

Headquarters



WIBU-SYSTEMS AG
Zimmerstrasse 5
76137 Karlsruhe, Germany
Phone: +49 721 93172-0
sales@wibu.com | www.wibu.com

Wibu-Systems is a global leader in cutting-edge cybersecurity and software license lifecycle management. We are committed to delivering unparalleled, award-winning, and internationally patented security solutions that protect the intellectual property embedded in digital assets and amplify the monetization opportunities of technical know-how. Catering to software publishers and intelligent device manufacturers, the interoperable hardware and software modules of our comprehensive CodeMeter suite safeguard against piracy, reverse engineering, tampering, sabotage, and cyberattacks across mainstream platforms and diverse industries.

Wibu-Systems Branch Offices

WIBU-SYSTEMS USA, Inc.
USA +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai +86 21 5566 1791
Beijing +86 10 8296 1560
info@wibu.com.cn

WIBU-SYSTEMS K.K.
Japan
+81 45 565 9710
info@wibu.jp

WIBU-SYSTEMS Korea Ltd.
Republic of Korea
+82 2 6206 9490
sales@wibu.co.kr

WIBU-SYSTEMS India Pvt. Ltd.
India
+91 9632423407
info@wibu.in

WIBU-SYSTEMS BV
The Netherlands +31 74 750 14 95
Belgium +32 2 808 6739
sales@wibu.systems

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.systems

WIBU-SYSTEMS SARL
France
+33 1 86 26 61 29
sales@wibu.systems

WIBU-SYSTEMS
Spain | Portugal
+34 91 123 0762
sales@wibu.systems

WIBU-SYSTEMS
Scandinavia | Baltics
+46 8 5250 7048
sales@wibu.systems

Wibu-Systems expressly reserves the right to change its programs or this documentation without prior notice.

© 2026 WIBU-SYSTEMS AG – Blurry Box®, CmReady®, CodeMeter®, SmartBind®, SmartShelter®, and Wibu-Systems® are registered trademarks of WIBU-SYSTEMS AG. All other brand names and product names used in this documentation are trade names, service marks, trademarks, or registered trademarks of their respective owners.

WIBU SYSTEMS

SECURITY
LICENSING
PERFECTION IN PROTECTION

www.wibu.com