Press Release – 28 October 2026

Wibu-Systems Wins Embedded Security Award for CodeMeter

- **Cyber Defense Magazine names Wibu-Systems "Most Innovative" in Embedded Security in its Top InfoSec Innovators Awards 2026.**
- **CodeMeter combines protection against software extraction and tampering with controls over authorized use, including in offline and air-gapped deployments.**
- **The Black Unicorn Report 2026 puts trust in executable code and software supply chain integrity among the priorities facing security leaders.**

Recognition brings attention to the challenge of protecting embedded software after devices leave the manufacturer's control

Karlsruhe, Germany – **Wibu-Systems, a specialist in software protection, licensing, and cybersecurity, has won the Most Innovative Embedded Security award in Cyber Defense Magazine's Top InfoSec Innovators Awards 2026. The recognition puts a practical challenge for device manufacturers in focus: how to protect proprietary software and control its use after equipment has been delivered, integrated into other systems, and placed in service for years.**

CodeMeter, Wibu-Systems' modular software protection and licensing platform, addresses this challenge by combining protection against reverse engineering and tampering with cryptographically secured license checks. Manufacturers can use these mechanisms to protect the algorithms that differentiate their products and determine which software functions a device is authorized to run, including where a permanent Internet connection is unavailable.

Trust in code becomes an operational question

The Black Unicorn Report 2026, published by Cyber Defense Magazine, lists Wibu-Systems among this year's winners. Its editorial analysis also provides a broader perspective on the problem. In his discussion of cybersecurity architecture, publisher Gary S. Miliefsky identifies code as a distinct security domain and asks whether it can

be trusted before execution. His outlook for 2027 highlights the need to establish whether software components have been tampered with and how quickly compromised components can be replaced.

For embedded manufacturers, those questions follow the product into the field. A proprietary algorithm may reside in a controller installed at a customer site, pass through an integrator's hands, or become accessible during maintenance. Restricting network access alone does not address extraction of that algorithm from the application binary or unauthorized changes to the application. Protection has to reach the software itself and remain workable under the device's operating constraints.

> *"A manufacturer may deliver a machine once, but its software will face changing users, service interventions, and new attempts to extract its know-how for years," said Marcellus Buchheit, President & CEO of Wibu-Systems USA. "The engineering challenge is to keep protection effective through those changes while allowing legitimate customers to use, maintain, and upgrade their equipment. That is where software protection and licensing need to work together."*

Protection that fits the device

Different embedded architectures require different implementations. On supported platforms, AxProtector CTP applies protection during compilation, including control-flow encryption and integrity checks, to make reverse engineering and unauthorized code modification more difficult. Where selected sensitive functions require additional isolation, CodeMoving can move their execution into a secure environment in a hardware- or cloud-based CodeMeter license container.

For equipment that must operate offline, hardware-based license containers can provide a local cryptographic trust anchor. CmASIC integrates that capability directly into the device, while CmDongles provide a removable hardware option. Manufacturers select the protection and licensing components appropriate to their target platform, connectivity, and physical design.

At the smallest end of the spectrum, implementation size becomes decisive. A compact microcontroller-focused library and optimized license format reduce licensing to essential license and signature verification for targets with only a few kilobytes of memory available. This allows constrained devices to participate in the broader CodeMeter ecosystem without assuming that they can run the full protection stack used by larger systems.

The connection between protection and licensing also gives manufacturers a way to manage product evolution. Authorized functionality can be differentiated and licensed as requirements change, while protection mechanisms help defend the underlying implementation against extraction and tampering. For long-lived equipment, the objective is to preserve the manufacturer's intellectual property and the customer's ability to use the software legitimately throughout updates, maintenance, and modernization.



Cyber Defense Magazine's Top InfoSec Innovators 2026 winner badge marks Wibu-Systems' recognition in the Most Innovative Embedded Security category.

Additional Dedicated Resources

- Award winners: https://cyberdefenseawards.com/top-infosec-innovators-for-2026/
- Wibu-Systems Awards and Recognition: https://www.wibu.com/innovation-journey/awards.html
- Licensing for low-memory microcontrollers: https://www.wibu.com/magazine/keynote-articles/article/detail/licensing-for-low-memory-microcontrollers.html
- Press release as audio file: https://www.wibu.com/fileadmin/Audiofiles/press_releases/WIBU-PR_InfoSec-Innovator-Awards-Winner_EN.mp3
- Press release images for download ready for print and online publications: https://wibu.sharefile.com/public/share/web-s0fe94609988642b0a8a787b2c3baf29c

About Cyber Defense Awards

This is Cyber Defense Magazine's 14th year of honoring cybersecurity innovators on our Cyber Defense Awards platform. In this competition, judges for these and other prestigious awards includes cybersecurity industry veterans, trailblazers and market makers Ron Gula of Gula Tech Adventures, Gary Miliefsky of CDMG, Dr. Lindsey Polley de Lopez of VentureScope, Katie Gray of In-Q-Tel, Robert R. Ackerman Jr. of DataTribe, Ira Winkler from CruiseCon, Dino Boukouris of AltitudeCyber and with much appreciation to emeritus judges Robert Herjavec of Cyderes, Dr. Peter Stephenson of CDMG and David DeWalt of NightDragon. Top InfoSec Innovators for 2026 is found here: https://cyberdefenseawards.com/top-infosec-innovators-for-2026/ and download The Black Unicorn Report for 2026: https://cyberdefenseawards.com/the-black-unicorn-report-for-2026/ and Top Global CISOs Winners for 2026, here: https://cyberdefenseawards.com/top-global-cisos-winners-for-2026/.

About Cyber Defense Magazine

Cyber Defense Magazine was founded in 2012 by Gary S. Miliefsky, globally recognized cyber security thought leader, inventor and entrepreneur and continues to be the premier source of IT Security information. We are managed and published by and for ethical, honest, passionate information security professionals. Our mission is to share cutting-edge knowledge, real-world stories and awards on the best ideas, products and services in the information technology industry. We deliver electronic magazines every month online for free, and limited special editions exclusively for the RSAC, BlackHat and Cyber Defense Conferences. Learn more about us at https://www.cyberdefensemagazine.com. Cyber Defense Magazine is a proud member of the Cyber Defense Media Group.

About Wibu-Systems

Daniela Previtali, Global Marketing Director
Phone +49 721 9317235 / +39 035 0667070
daniela.previtali@wibu.com
https://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.

Blurry Box®, CmReady®, CodeMeter®, SmartBind®, SmartShelter®, and Wibu-Systems® are registered trademarks of WIBU-SYSTEMS AG.

Media graphic resources available at: https://www.wibu.com/media-library.html.

© Copyright 2026, WIBU-SYSTEMS AG. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective organizations and companies.