

White Paper Executive Summary

Licensing and Security for the IoT

Believe the IoT Hype and Be Prepared to Protect It

Nations around the world have come to consider the technological potential opened up by the IoT as their future and are investing heavily into research in the field, making IoT an integral component of their long-term strategy.

IoT applications are developed with devices and services in various sectors: Information technology, automation and manufacturing, the aerospace industry, maritime and naval applications, rail transport, car makers and their suppliers, energy providers, agricultural businesses, medical technology, and building automation. These many and diverse areas share certain industrial-grade standards in terms of a technology's lifecycle, reliability, robustness in harsh environments, or reliable, long-term availability.

With its many promises and great prospects, the IoT warrants much stronger protection than the closed systems of the past. IoT systems rely on public networks which, by definition, are not safe environments. Hackers are always looking for backdoors and exploits to execute their criminal plans, and attackers are trying to tamper with data to cause untold damage.

Because of these threats, security by design needs to be the goal for all components. This places a priority on industrial grade design, the footprint of hardware and software, development support, and cross-brand cooperation as well as complete protection from the very first software layer.

This white paper explores the various trends emerging in the IoT and the key strategies for success, which depend not only on superior products, creative marketing, or aggressive sales activities, but security, integrity, and reliable licensing as well.

It also outlines the standards that must be addressed and long-term considerations that will impact security, like integration in devices and software, upgrades and updates, secure boot, licensing models tailored to the IoT, license management, access rights and certificates, scalable safeguards, and data integrity protections.

The white paper concludes with an overview of Wibu-Systems' CodeMeter protection, licensing, and security platform and how it provides the makers of IoT applications and embedded systems with the mechanisms to comply with all the standards and requirements necessary to achieve the highest level of protection and security. With safeguards against reverse engineering and manipulation along the entire design chain – from the hardware to the individual application – to fine-grained licensing options, CodeMeter technology is available in IoT-ready and scalable security products in robust, industry-grade versions. Equipped in this manner for the connected future, companies can look forward to lasting success in the new world of the Internet of Things.