CUCo
Central Unit Control

FIRMWARE SECURITY

CUCo Firmware Security is an anti-theft technology based on secure protocols embedded on x86 UEFI BIOS or deep in Android kernel, a firmware solution oriented to computers, tablets and smartphones. The innovative patented technology was developed in cooperation with EU sponsored university researchers, leaders in digital systems security.

learn more

PROTECTION AND SECURITY

Through the autonomous operation based on predefined rules, *CUCo Firmware Security* ensures an intelligent and effective protection of devices, preventing them from being used in the event of a non-compliance with a contract, such as in a situation of loss or theft. By ensuring effective deterring against theft, *CUCo Firmware Security* contributes in a unique way to the protection and abuse of the end-user, especially in scenarios where the device represents an asset of substantial value to the end-user, such as in public education projects. **Firmware device lock is the most effective solution to protect children from theft abuse.**

CUCo leverages the security model of the underlying firmware and, regardless of OS or internet connections, allows a secure and self-acting lock by the device firmware.

CUCo is globally compatible with most devices and brands that support the UEFI x86 standard. Low level access allows CUCo to provide special functions to MDM programs and its management platform can be deployed in the cloud or on premises for especially large projects.

inforlandia

CUCO
Central Unit Control

OBJECTIVES

The main purpose of the *CUCo Firmware Security* solution is to enable a computing device to perform a contractual self-compliance check, based on predefined rules, allowing the protection against theft and abuse of the user and device through an auto firmware lock and remote unlocking of the device, independently of the connectivity status of the device.

DaaS
(Device as a Service)

CUCo Firmware Security can be implemented in several scenarios, valid for a wide range of owners, with different scopes, from government entities, educational institutions (public or private), military or security forces, telecom operators or leasing and renting companies. Any entity that owns and is responsible for the management of a fleet of heterogeneous devices will find in *CUCo Firmware Security* the solution to ensure effective control of their devices, in accordance with their contract terms.

inforlandia

CUCO
Central Unit Control

MAIN FEATURES

•Allows locking by the firmware before operating system boot or startup, being OS agnostic;

•Does not require proprietary chipset security features, being UEFI and TPM compatible;

•After lock event, device can be unlocked remotely after owner permission;

•Auto locks in case of non-access to the internet for a rules-based predefined period of time;

•Compatible and validated with the majority of PC manufacturers. Optimized for Intel® x86 platforms.

•Resists attempts to attacks on ROM vulnerabilities, preventing its removal by hackers or unauthorized agents; Supports updates with signed binaries;

•Keeps functioning even if the Operating System or the disk storage is replaced;

•Compatible with Windows, Linux, Android, Chrome, etc. Optimized for Microsoft® Windows.

•Allows permanent deactivation of the CUCo system (ex: at the end of leasing period);

•Encryption hash follows ISO/IEC 10118-3:2004 and UEFI module ISO/IEC 19678:2015 standards;

•No access to any data beyond its own variables, a warrant of no-access to device end-user contents;

•GDPR compliant; Third-party MDM can use CUCo for remotely auto wipe & reinstall OS;

•Cloud based management console (Azure compatible) or installed on premises;

•API support for third-party management solutions; Allows lock commands from other platforms;

•Low level functions support for MDM such as InTune, RxArt, c.MDM, h.MDM;

MILESTONES

1 million devices protected with CUCo in Portugal “Escola Digital” project (2020-22);

•240.000 devices in 4 Argentina Education projects (2019-22);

•Total 1.4 million devices active*;

•4 multinational device brands licensed*;

•7 companies licensed “private label” versions based on CUCo technology*.

(*) (as of March 2022)

PRIVATE LABEL

Specific needs in many countries and scenarios incentivized the creation of a private label program to allow the development of project or country specific needs. This program, by fully addressing the needs of some projects, such as in security forces or public safety organizations, has allowed an exceptional success degree among our private label partners.
Contact us for further information.

Inforlandia

CUCO
Central Unit Control

COMPETITIVE ANALYSIS

CUCo vs Main competitors:

	CUCo	C1	C2	C3
Open Platform, UEFI standards based, compatible with multiple brands of devices (open license to ODM's)	✓		x	x
Single purpose Firmware level remote-lock, device auto-control, rules-based pre-OS boot lock	✓	x	✓	
No access to user data on device by platform manager (RGPD compliant)	✓	x	✓	
Remotely reactivate device after lock event (non-software dependent, but solely hardware/firmware lock)	✓		x	✓
Self-protection against hacking attempts to deactivate security on device	✓	✓	x	
Low bandwidth and no-connectivity regular functioning for defined period	✓	x	x	
Multiple OS support, including Windows, Linux, Android. Lock by firmware survives OS changes. Software agnostic	✓	x	x	x
Focus on "hardware only" security. Data and content agnostic.	✓	x	✓	x
Remote permanent freedom command to permanently deactivate security mechanism	✓		x	

inforlandia

CUCo
Central Unit Control

GET IN TOUCH

If you'd like a quote or need more details,
please provide your information, and we'll be in touch

Contacts

Email

inforlandia

CUC
Central Unit Control