



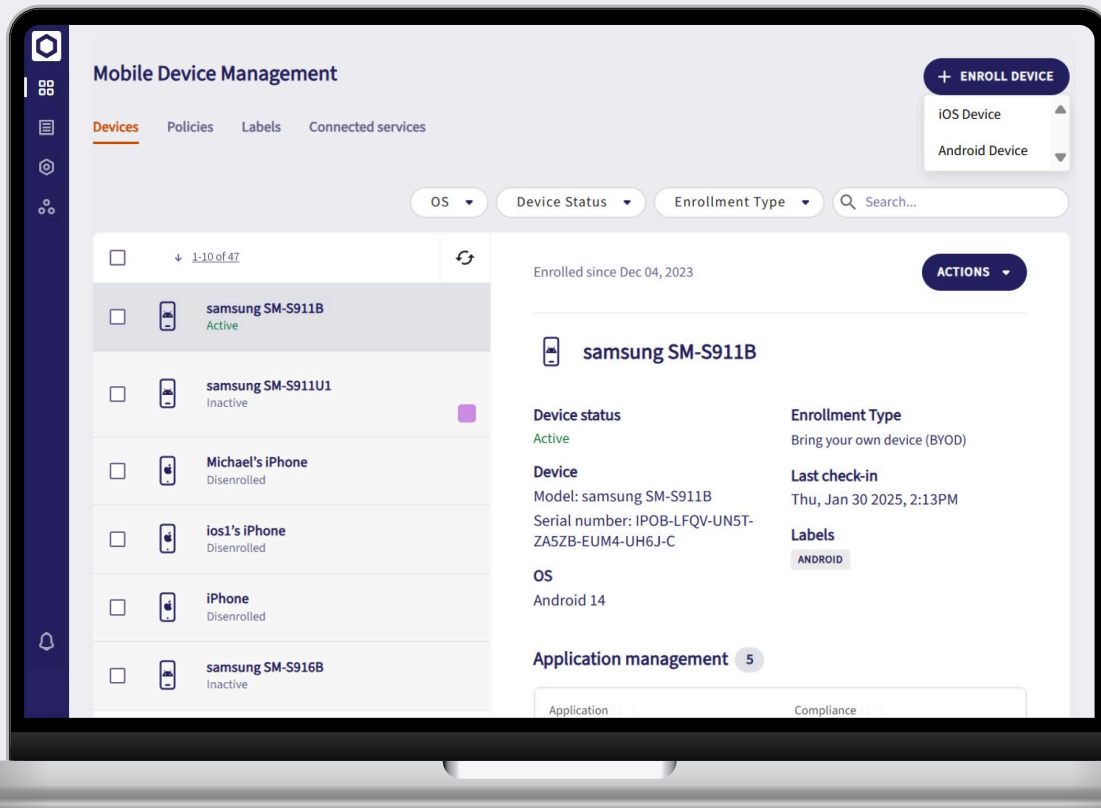
Mobile Device Management

Built for small teams with big responsibilities



Coro's Mobile Device Management (MDM) module simplifies the management and security of company-owned and Bring Your Own Device (BYOD) work-related mobile devices. It enables IT teams to enforce app policies, manage apps, and ensure company policy compliance. The module gives visibility into mobile devices, ensuring efficient device management across the organization.

Modular Cybersecurity











Coro's Mobile Device Management (MDM) module is part of a powerful modular cybersecurity platform.

Designed to evolve with your needs, a modular platform ensures effortless security across cloud apps, devices, data, and endpoints while sharing one endpoint agent, one dashboard, and one data engine. Adding modules is done at the click of a button. Chosen modules snap into place, immediately integrating with other modules.



Key Features

-  **iOS and iPadOS**
Device Enrollment
Enrolls devices via DEP with Coro as the MDM or through MAID for identity-driven enrollment using managed Apple IDs
-  **Device Labels**
Groups related mobile devices, enabling filtered searches and targeted policy management
-  **Supported Mobile Platforms**
iOS/iPadOS and Android
-  **Policy Management**
Enables admins to create policies based on allowed apps for work profiles (iOS supervised/Android) and compliant apps with compliance reporting for installed apps (iOS BYOD)
-  **Rich Application Search**
Allows admins to add apps to a device policy from the Coro console based on the app name
-  **Multilingual Support**
Provides support for Spanish and Italian on mobile apps
-  **Device Management**
Allows admins to add labels to enrolled devices for better categorization, wipe data remotely for enhanced security, mark devices for disenrollment to remove profiles and policies, and remove devices that are inactive or disenrolled
-  **Expiration Reminders**
Sends emails to admin users warning of the expiration of their installed Apple certificates for APNs and DEP

Why Coro?

-  **High Threat Detection and Protection Rate**
Achieved AAA rating from SE Labs
-  **Easy to Maintain**
95% of the workload offloaded from people to machines
-  **Quick Deployment**
Simple and quick installation, no hardware required
-  **Fast Learning Curve**
Minimal training, simplified onboarding, user-friendly interface
-  **High ROI**
No hardware costs, zero maintenance overhead, affordable pricing
-  **High Customer Satisfaction**
95% likelihood to recommend - as rated by G2

Thousands Of Customers in **Automotive, Education, Energy, Financial** and more.



Cybersecurity for small teams with big responsibilities

SCHEDULE A DEMO TODAY

START A FREE TRIAL

About Coro

Coro, the leading cybersecurity platform for small and mid-size businesses, empowers organizations to easily defend against malware, ransomware, phishing, data leakage, network threats, insider threats and email threats across devices, users, networks and cloud applications. Coro's platform automatically detects and remediates the many security threats that today's distributed businesses face, without IT teams having to worry, investigate, or fix issues themselves. Coro has been named a leader in G2-Grid for EDR/MDR, received Triple-A grading (AAA) from SE LABS, and was named on Deloitte's Fast 500.

