Trusted Electronic Monitoring

Solution overview

Trusted Services

G-Cloud 15 customer-facing document

© Copyright 2026, Magellan. All rights reserved.

Introduction to Trusted Electronic Monitoring

Unifying the ecosystem for safer, smarter judicial supervision.

Monitor better, manage less

Electronic monitoring is a strategic lever for reconciling public safety, operational efficiency, and cost control. Devices and logistics can be fragmented, complex to manage, and difficult to adapt to local requirements.

A unified and adaptable platform

The platform unifies, simplifies, and secures the monitoring ecosystem while providing API-driven flexibility. It can integrate with device and logistics workflows, helping to remain agnostic to hardware providers and partners as policies evolve.

Configurable operational outcomes

An adaptable rules engine can be tailored to each organisation’s operations. The supplied functional scope states that equivalent outcomes can be achieved with half the staff compared with a traditional monitoring solution.

A centralising platform

A single control point for the entire electronic-monitoring ecosystem.

Multi-vendor by design

Aggregate and normalise data from diverse devices and technologies in a single platform. Coexist with multiple device generations and providers, evolve the device fleet without changing the software platform, and use a consistent interface for location, schedules, history, dashboards, and alerts.

From raw data to targeted action

Give agents a single place for technical events and the monitored individual's CRM context. The rules engine aggregates, correlates, and prioritises events without deleting data, helping to reduce noise while preserving integrity and enabling officers to focus on high-value cases.

Personalisation and compliance

Configuration aligned to local requirements

Each jurisdiction, administration, and territory can apply its own rules. Configure alert rules, severity, time windows, and geographic zones to match local laws and operational practice.

Integrated administration structure

Apply different settings by organisation, department, court, or service provider. Organise processing by agent groups, security providers, and authorised stakeholders; assign by territory, monitoring type, or authorised action; and route alerts to the right person with appropriate priority.

Control and data protection

Respect data-retention and protection obligations while retaining control over processes. Context-rich decision support can combine history, geolocation, and active measures to help users make prompt, accurate decisions.

Enhanced security and scalability

End-to-end confidentiality and traceability

Electronic-monitoring data is highly sensitive. The architecture supports dedicated or shared hosting options based on data security and capacity requirements, including isolated environments where required. It includes encryption of stored data, fine-grained role- and clearance-based access control, action logging, and enhanced audit capabilities.

Growth without disruption

Progressively add bracelets, home units, and mobile devices without performance degradation. Extend to new territories or jurisdictions with dedicated configurations, and increase the number of users and intervention teams by role and responsibility.

Functional evolvability

Adapt integration scenarios, measure categories, and processes to future legislative or organisational reforms. The objective is a future-proof platform that supports strategic decisions without major technical or budgetary reinvestment at every change.

Modular business architecture

Build the target solution around a core Trusted Electronic Monitoring engine and specialised functional components.

Composable components

Rather than a monolithic application, the platform is composed of business components that can be combined to reflect each administration's operational model and priorities. Modules can be activated when needed and extended over time.

Progressive evolution

Start with a core set of components and add capabilities such as supervision dashboards, logistics, or billing. Align the functional scope with the internal organisation, then adapt to reforms or process changes by reconfiguring or replacing components rather than redesigning the platform.

Monitoring and processing of alarms

A shared, prioritised workspace

Collect alarms in a central monitoring workspace. A common basket is updated in real time and sorted by severity, providing a shared view of workload. Agents create personal worklists by taking alarms from the basket, helping prevent duplicate work and enabling concurrent handling.

Configurable operational actions

For offender-related alarms, configure actions such as calling the offender, sending a message, adding a comment, drafting a report, closing an alarm, requesting technical support, or initiating an investigation. Display sentence and measure details, status, alarm history, and live device data in one interface.

Case consistency

Automatically link alarms to their related case so signals, operational decisions, and the legal context of the monitored person remain connected.

Rules engine: from raw events to meaningful alarms

Qualify what matters

An event is any message received from a monitoring device; an alarm is a qualified event defined by the relevant measures, schedule, history, risk, and business rules. The engine can combine and repeat events, detect gaps, and retain only the alarms with business value while logging other events for traceability.

Reduce noise without losing information

The supplied functional scope states that, even with continuous device and data streams, agent-visible alarms can be reduced by up to fourfold without losing information. Administrators can dynamically adjust parameters and scenarios without restarting the system.

Support timely intervention

Open cases, plan interventions, contact monitored individuals, and log follow-up activity from a consistent workspace. Contextual prioritisation helps users focus on the most relevant actions.

Proven at scale

Ministère de la Justice — domestic-violence electronic-monitoring programme.

Challenge

Implement electronic surveillance as an alternative to imprisonment while meeting public-safety, data-sensitivity, and French Code of Criminal Procedure requirements. In 2020, France introduced a domestic-violence electronic-monitoring programme designed to prevent offenders from approaching victims.

Delivered solution

The supplied material describes a specific, highly secured solution designed for customer requirements and French-law compliance. It references availability service levels of 99.97% and delivery of the domestic-violence monitoring programme in nine months.

Scale cited in the source

18,000 electronic tags deployed and 2,000 victim-protection units active 24/7.